УЧЕБНОЕ ПОСОБИЕ

А.В. Новоструев, В.М. Солодовников,
А.А. Терентьева

ТЕЗАУРУС В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курганский
государственный
университет

редакционно-издательский
центр
41-71-07

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Курганский государственный университет»

А.В.НОВОСТРУЕВ, В.М. СОЛОДОВНИКОВ, А.А.ТЕРЕНТЬЕВА

ТЕЗАУРУС В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Курган 2014

УДК 004
ББК 32.973.202
Н

Р е ц е н з е н т ы

кафедра «Безопасность информационных систем» федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Южно-Уральский государственный университет"

начальник Центра информационных технологий, связи и защиты информации Управления Министерства внутренних дел по Курганской области, полковник полиции О.Ю.Родионов.

Печатается по решению методического совета Курганского государственного университета.

Научный редактор – канд. техн. наук Д.И.Дик

Новоструев, А.В., Солодовников, В.М., Терентьева, А.А. Тезаурус в сфере информационной безопасности [Текст]/ А.В. Новоструев, В.М. Солодвников, А.А. Терентьева : Учебное пособие. – Курган: Изд-во Курганского гос. Ун-та, 2014. – 471 с.

В учебном пособии собраны официальные (стандартизированны) определения понятий, используемых в области информационной безопасности и защиты информации. Данное учебное пособие позволяет пользователям находить определения терминов, содержащиеся в отечественных и зарубежных нормативных документах, стандартах, научной литературе, периодике по информационной безопасности, словарях и других изданиях.

Для каждого термина есть ссылка на источник, из которого взято определение.

В тезаурусе указаны семантические отношения (связи) между терминами.

Тезаурус может быть полезен как авторам текстов, связанных с информационной безопасностью, так и их читателям. Первым он позволит более точно применять термины информационной безопасности с учетом нюансов их значения в контексте различных документов и областей применения. Вторым – поможет глубже понять специфику профессиональных текстов. А в целом будет способствовать формированию единой терминологии по информационной безопасности и более полному взаимопониманию между специалистами.

Предназначено для студентов вузов, обучающихся по направлениям и специальностям в области информационной безопасности.

УДК 004
ББК 32.973.202

ISBN……..

©Курганский государственный университет, 2014
©Новоструев А.В.,Солодовников В.М., Терентьева А.А.,2014

Абонент [abonent, subsriber, user] —

1. Пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации. *[Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004*]

2. Пользователь, имеющий право доступа к системе обработки или передачи информации. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*

Выше: Пользователь услугами связи

См. также: Абонент сети, Услуга связи

Абонент сети —

Лицо, являющееся сотрудником учреждения (предприятия), имеющее соответствующим образом оформленное разрешение и технические возможности на подключение и взаимодействие с сетями. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»*]

См. также: Информационные сети общего пользования, Услуги сети

Абонентский пункт —

Средства вычислительной техники учреждения (предприятия), подключаемые к сетям с помощью коммуникационного оборудования. АП могут быть в виде автономных персональных электронно-вычислительных машин (ПЭВМ) с модемом и не иметь физических каналов связи с другими средствами вычислительной техники (СВТ) предприятия, а также в виде одной или нескольких объединенных локальных вычислительных сетей (ЛВС) с рабочими станциями и серверами, соединенных с сетями через коммуникационное оборудование (модемы, мосты, шлюзы, маршрутизаторы-роутеры, мультиплексоры, коммуникационные серверы и т.п.). *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*

См. также: Локальная вычислительная сеть

Абузоустойчивый хостинг [bulletproof hosting] —

Хостинг, который не будет закрыт в случае размещения на нем незаконных материалов (детской порнографии и т.д.), ресурсов, связанных с мошенничеством или спамерскими рассылками. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*

См. также: Спам

Автозагрузка программ —

Механизм операционной системы, позволяющий автоматически запускать определенный набор программ при каждой загрузке операционной системы (при включении компьютера или его перезагрузке).

Большинство современных вредоносных программ используют механизм автозагрузки для скрытого от пользователя запуска себя на зараженных компьютерах.

Наиболее популярная в настоящее время операционная система Windows XP использует набор ключей системного реестра и папок на жестком диске для определения автоматически загружаемых программ.

Ключи системного реестра:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]

Папки на жестких дисках:

%systemdrive%\Documents and Settings\All Users\Start Menu\Programs\Startup

%systemdrive%\Documents and Settings\%username%\Start Menu\Programs\Startup

%windir%\Profiles\All Users\Start Menu\Programs\Startup

%windir%\Profiles\%username%\Start Menu\Programs\Startup

В путях используются следующие переменные:

%systemdrive% - логический диск, с которого осуществляется загрузка операционной системы;

%username% - текущий пользователь операционной системы (определяется в момент ввода логина и пароля);

%windir% - папка, в которую установлена ОС Windows.

Папки, начинающиеся с "%windir%\Profiles", присутствуют, если операционная система Windows XP устанавливалась поверх операционной системы Windows NT 4.0.

Присутствие подозрительных ключей или ярлыков в любом из указанных источников автоматически загружаемых при старте операционной системы программ может свидетельствовать о наличии на машине той или иной активной вредоносной программы. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*

См. также: Компьютерный вирус

Автоматизированная банковская система —

Автоматизированная система, реализующая технологию выполнения функций организации банковской системы Российской Федерации. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*

Выше: Автоматизированная система

Ниже: Комплекс средств автоматизации автоматизированной банковской системы

Автоматизированная информационная система (АИС) [Automated Information System (AIS)] —

1. Информационная система, реализованная с использованием средств вычислительной техники, связи и передачи данных. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996.]*

2. Совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*

Выше: Информационная система

Ниже: Защищаемая автоматизированная информационная система

Автоматизированная обработка персональных данных [automated personal data processing] —

Обработка персональных данных с помощью средств вычислительной техники. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*

Выше: Обработка персональных данных

Автоматизированная система [automated system] —

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Примечания:

1. В зависимости от вида деятельности выделяют, например, следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др.

2. В зависимости от вида управляемого объекта (процесса) АСУ делят, например, на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*

Выше: Система

Ниже: Автоматизированная банковская система, Автоматизированная информационная система, Автоматизированная система в защищенном исполнении, Автоматизированное рабочее место, Защищенная автоматизированная система, Интегрированная автоматизированная система

См. также: Администратор АС, Информационное обеспечение автоматизированной системы, Методическое обеспечение автоматизированной системы, Организационное обеспечение автоматизированной системы, Правовое обеспечение автоматизированной системы, Программное

обеспечение автоматизированной системы, Техническое обеспечение автоматизированной системы, Класс защищенности автоматизированной системы, Штатные средства, предоставляемые средством вычислительной техники или автоматизированной системой

Автоматизированная система в защищенном исполнении —

Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или других нормативных документов по защите информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*

См. также: Аттестация автоматизированной системы в защищенном исполнении, Критерий качества функционирования автоматизированной системы в защищенном исполнении при испытаниях на устойчивость, Показатели устойчивости автоматизированной системы в защищенном исполнении, Устойчивость автоматизированной системы в защищенном исполнении к преднамеренному силовому электромагнитному воздействию

Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации —

Комплекс аппаратных и программных средств, информационных систем и информационно- телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам Российской Федерации, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*

См. также: Критическая информационная инфраструктура Российской Федерации, Критически важный объект информационной инфраструктуры (КВО)

Автоматизированное рабочее место (АРМ) [automated workplace] **—**

Программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Примечание. Видами АРМ, например, являются АРМ оператора-технолога, АРМ инженера, АРМ проектировщика, АРМ бухгалтера и др. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*

Выше: Автоматизированная система

Автономная система электронных платежей [off-line e-cash system] —

Система электронных платежей, в которой транзакцию платежа выполняют покупатель и продавец, без участия банка-эмитента. В такой системе требуется дополнительная транзакция депозита, с помощью которой продавец может положить полученные электронные деньги на свой счет в банке. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006.]*

Выше: Система (протокол) электронных платежей

Ниже: Транзакция (протокол) депозита

См. также: Конфиденциальный набор ключей, Проблема повторной траты электронных денег, Транзакция (протокол) депозита, Транзакция (протокол) платежа, Централизованная система электронных платежей

Автор результата интеллектуальной деятельности —

Гражданин, творческим трудом которого создан такой результат. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Авторские права, Объекты авторских прав, Соавторство

Авторизация [authorization] —

1. Санкционирование доступа — предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*. 2. Предоставление прав доступа. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*

Ниже: Единая авторизация

См. также: Права доступа

Авторские права —

Интеллектуальные права на произведения науки, литературы и искусства.

Автору произведения принадлежат следующие права:

1) исключительное право на произведение;

2) право авторства;

3) право автора на имя;

4) право на неприкосновенность произведения;

5) право на обнародование произведения.

В случаях, предусмотренных Гражданским Кодексом РФ, автору произведения наряду с правами, настоящей статьи, принадлежат другие права,

в том числе право на вознаграждение за использование служебного произведения, право на отзыв, право следования, право доступа к произведениям изобразительного искусства. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

Выше: Интелектуальные права

Ниже: Право автора на имя, Право авторства, Право доступа, раво на обнародование своего произведения

См. также: Знак охраны авторского права, Информация об авторском праве, Объекты авторских прав, Патентные права, Технические средства защиты авторских прав, Программное пиратство

Агент нарушителя —

Лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*

См. также: Нарушитель

Агрегирование риска [risk aggregation] —

Объединение нескольких рисков в один риск, направленное на более глубокое понимание совокупного риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Син. Объединение рисков

Адаптация программы для ЭВМ или базы данных —

Внесение изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: База данных, Программа для ЭВМ, Модификация (переработка) программы для ЭВМ или базы данных

Адаптивная атака [adaptive attack] —

Атака на криптосистему, при которой характер воздействия противника и/или нарушителя может изменяться во времени в зависимости от действий законных пользователей криптосистемы или от других условий. Например, противник может подбирать различные исходные данные для воздействия на криптосистему. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006.]*

Выше: Атака

Ниже: Адаптивная атака на основе подобранного открытого сообщения, Адаптивная атака на основе подобранного шифрованного сообщения

Адаптивная атака на основе подобранного открытого сообщения [adaptive chosen-plaintext attack] —

Адаптивная атака, при которой противник и/или нарушитель имеет возможность вынудить законного пользователя криптосистемы к обработке (зашифрованию) некоторого открытого сообщения, выбранного противником и/или нарушителем, и наблюдать соответствующее шифрованное сообщение. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006.]*.

Выше: Адаптивная атака

Син.: Адаптивная атака по выбранному сообщению

См. также: Адаптивная атака на основе подобранного шифрованного сообщения

Адаптивная атака на основе подобранного шифрованного сообщения [adaptive chosen-ciphertext attack] —

Адаптивная атака, при которой противник и/или нарушитель имеет возможность вынудить законного пользователя криптосистемы к обработке (расшифрованию) некоторого шифрованного сообщения, выбранного противником и/или нарушителем, и наблюдать соответствующее открытое сообщение. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006.]*

Выше: Адаптивная атака

См. также: Адаптивная атака на основе подобранного открытого сообщения

Адаптивная атака по выбранному сообщению [adaptive chosen-plaintext attack] —

См. Адаптивная атака на основе подобранного открытого сообщения.

Адвокатская тайна —

Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием. *[Федеральный закон от 31.05.2002 N 63-ФЗ “Об адвокатской деятельности и адвокатуре в Российской Федерации” (с изменениями на 2 июля 2013 года). Введен в действие: 01.07.2002]*.

Выше: Профессиональная тайна

Административное управление ключом —

Генерация, сохранение, распределение, удаление, каталогизирование и применение ключей в соответствии со стратегией защиты. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды механизмов защиты

См. также: Стратегия защиты

Административный регламент [administrative regulation] **—**

Соответствующий действующему законодательству нормативный документ организации, который определяет совокупность действий, необходимых для исполнения конкретной функции организации, порядок, сроки, участников, результаты и условия их выполнения *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009.]*

См. также: Технический регламент

Администратор АС —

Лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и. рекомендации по технической защите конфиденциальной информации»]*

См. также: Автоматизированная система, Администратор защиты

Администратор защиты [security administrator] **—**

Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)*.

См. также: Защита информации от несанкционированного доступа (ЗИ от НСД), Защита от несанкционированного доступа (Защита от НСД), Несанкционированный доступ к информации

Администратор межсетевого экрана —

Лицо, ответственное за сопровождение межсетевого экрана. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Дистанционное управление компонентами межсетевого экрана, Локальное (местное) управление компонентами межсетевого экрана, Централизованное управление компонентами межсетевого экрана

Администратор (руководящий орган) системы обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Физическое или юридическое лицо, ответственное за реализацию политики обеспечения информационной безопасности ВСС РФ *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Информация управления информационной безопасностью Взаимоувязанной сети связи Российской Федерации, Политика информационной безопасности Взаимоувязанной сети связи Российской

Федерации, Служба информационной безопасности Взаимоувязанной сети связи Российской Федерации

Адресная книга —

База данных особого формата, содержащая адреса электронной почты, а также прочую персональную информацию о ваших адресатах. Как правило, требует ручного добавления новой записи, то есть, автоматического сохранения адресов, по которым отсылались электронные письма, не предусматривает.

Адресные книги разных несовместимых форматов есть у большинства современных email-клиентов. Наиболее распространен формат адресной книги Windows (WAB, Windows Address Book). Этот формат используют самые популярные email-клиенты, такие как MS Outlook Express и MS Outlook.

Множество почтовых и сетевых червей используют записи в адресных книгах (особенно в адресной книге Windows) для поиска адресов, по которым затем производится несанкционированная пользователем рассылка зараженных писем. Зачастую именно так на компьютер пользователя проникают вредоносные программы - приходят в письме со знакомого email-адреса. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/].*

См. также: Сетевой червь, Электронная почта

Аккаунт [account] —

См. Учетная запись

Аккредитация [accreditation] —

1. Официальное признание органом по аккредитации компетентности физического или юридического лица выполнять работы в определенной области оценки соответствия. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003].*

2. Подтверждение соответствия третьей стороной, относящееся к органу по оценке соответствия, служащее официальным свидетельством его компетентности для выполнения конкретных задач по оценке соответствия. *[ГОСТ ИСО/МЭК 17011-2009 Оценка соответствия. Общие требования к органам по аккредитации, аккредитующим органы по оценке соответствия. Введен в действие: 01.07.2010].*

См. также: Орган по аккредитации, Маркировка

Аккредитация удостоверяющего центра —

Признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона. Аккредитация удостоверяющих центров осуществляется уполномоченным федеральным органом в отношении удостоверяющих центров, являющихся российскими или иностранными юридическими лицами. Аккредитация удостоверяющего центра осуществляется на добровольной основе. Аккредитация удостоверяющего центра осуществляется на срок пять лет, если более короткий срок не указан в заявлении удостоверяющего центра. Аккредитация удостоверяющего центра осуществляется при условии выполнения им следующих требований:1) стоимость чистых активов

удостоверяющего центра составляет не менее чем один миллион рублей; 2) наличие финансового обеспечения ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи, выданном таким удостоверяющим центром, или информации, содержащейся в реестре сертификатов, который ведет такой удостоверяющий центр, в сумме не менее чем полтора миллиона рублей; 3) наличие средств электронной подписи и средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности; 4) наличие в штате удостоверяющего центра не менее двух работников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей, имеющих высшее образование в области информационных технологий или информационной безопасности либо высшее образование или среднее профессиональное образование с последующим получением дополнительного профессионального образования по вопросам использования электронной подписи. Аккредитация удостоверяющего центра осуществляется на основании его заявления, подаваемого в уполномоченный федеральный орган. К заявлению прилагаются документы, подтверждающие соответствие удостоверяющего центра требованиям, установленным Федеральным законом N 63-ФЗ *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

См. также: Аккредитованный удостоверяющий центр, Уполномоченный федеральный орган

Аккредитованный удостоверяющий центр —

Удостоверяющий центр, получивший аккредитацию, является аккредитованным удостоверяющим центром. Аккредитованный удостоверяющий центр обязан хранить следующую информацию:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

Аккредитованный удостоверяющий центр должен хранить информацию, указанную в части 1 настоящей статьи, в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами

Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

Аккредитованный удостоверяющий центр обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к выданным этим удостоверяющим центром квалифицированным сертификатам и к актуальному списку аннулированных квалифицированных сертификатов в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Удостоверяющий центр

Актив [asset] —

1. Сущности, предположительно представляющие ценность для владельца объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Что-либо, что имеет ценность для организации.

Примечание. Имеются различные типы активов:

- информация;
- программное обеспечение;
- материальные активы, например компьютер;
- услуги;
- люди и их квалификация, навыки и опыт;
- нематериальные активы, такие как репутация и имидж. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

3. Все, что имеет ценность для организации в интересах достижения целей деятельности и находится в ее распоряжении.

Примечание. К активам организации могут относиться:

• информационные активы, в том числе различные виды информации, циркулирующие в информационной системе (служебная, управляющая, аналитическая, деловая и т.д.) на всех этапах жизненного цикла (генерация, хранение, обработка, передача, уничтожение);

• ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие);

• процессы (технологические, информационные и пр.);

• выпускаемая продукция и/или оказываемые услуги. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

4. Все, что имеет ценность для организации и находится в ее распоряжении.

Примечание. К активам организации могут относиться:

- вычислительные, телекоммуникационные и прочие ресурсы;

- информационные активы, в т.ч. различные виды информации на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;

- продукты и услуги, предоставляемые сторонним организациям. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

5. Все, что имеет ценность для организации. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

6. Все, что имеет ценность для организации банковской системы Российской Федерации и находится в ее распоряжении.

Примечание. К активам организации банковской системы Российской Федерации могут относиться:

• работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;

• различные виды банковской информации — платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;

• банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы);

• банковские продукты и услуги, предоставляемые клиентам. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Информационный актив

См. также: Ресурс, Информационная безопасность организации, Информационный процесс

Активная атака [active attack] —

Атака на криптосистему или на криптографический протокол, при которой противник и/или нарушитель может влиять на действия законного пользователя, например, подменять или удалять сообщения законного пользователя, создавать и передавать сообщения от его имени и т. п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Ниже: Имитация

См. также: Активный нарушитель, Криптографическая система, Криптографический протокол, Имитостойкость, Пассивная атака

Активная угроза [active threat] —

1. Угроза преднамеренного несанкционированного изменения состояния системы.

Примечания:

1) Примерами активных угроз, относящихся к защите информации, могут служить модификация сообщений, дублирование сообщений, вставка ложных сообщений, маскирование какого-либо логического объекта под санкционированный логический объект и отклонение услуги.

2) Активные угрозы системе означают изменение информации, содержащейся в системе, либо изменения состояния или работы системы. Примером активной угрозы служит умышленное изменение таблиц маршрутизации системы неполномочным пользователем. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Угроза, которая может быть реализована путем намеренного несанкционированного вмешательства в работу криптосистемы (криптографического протокола). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Угроза, Виды угроз

Активный аудит [active audit] —

Автоматизированный анализ данных аудита с целью своевременного выявления нарушений безопасности, оповещения о них администраторов и пользователей системы и принятия мер по защите. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Аудит

Активный нарушитель [active adversary] —

Нарушитель, который недопустимым образом влияет на ход выполнения криптографического протокола. Как правило, полный анализ всех результатов однократного выполнения криптографического протокола позволяет обнаружить присутствие активного нарушителя. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Нарушитель

См. также: Пассивный нарушитель, Криптографический протокол

Активный противник [active adversary] —

Противник, который вмешивается в ход выполнения криптографического протокола или работу криптографической системы. Как правило, полный анализ всех результатов однократного выполнения криптографического протокола позволяет обнаружить присутствие активного противника. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Противник

См. также: Пассивный противник, Криптографический протокол

Актуальные угрозы безопасности персональных данных —

Совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия. *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

См. также: Безопасность персональных данных

Алгоритм блочного шифрования [basic block encryption algorithm] —

Алгоритм зашифрования, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков открытого текста, имеющих фиксированную длину. Представляет собой алгоритм простой замены блоков текста фиксированной длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм шифрования

Син.: Базовый блочный алгоритм зашифрования

См. также: Блок данных, Блочная шифрсистема, Развертывание ключа

Алгоритм генерации цифровой подписи [signature generation algorithm] —

См. Алгоритм формирования цифровой подписи.

Алгоритм зашифрования [encryption algorithm] —

Криптографический алгоритм, реализующий функцию зашифрования. В случае блочных шифрсистем получается использованием базового блочного алгоритма зашифрования в конкретном режиме шифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм шифрования

Ниже: Поточный алгоритм зашифрования

См. также: Алгоритм блочного шифрования, Режим шифрования, Функция зашифрования, Уравнение зашифрования, Алгоритм расшифрования

Алгоритм имитозащищающего кодирования [integrity protection algorithm] —

Криптографический алгоритм преобразования информации, обеспечивающий контроль ее целостности (как правило за счет внесения избыточности). В отличие от алгоритма формирования цифровой подписи использует симметричные криптосистемы. Примерами алгоритма имитозащищающего кодирования являются код аутентификации, некоторые автоматные преобразования и алгоритмы шифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Система имитозащиты

Ниже: Код аутентификации, Алгоритм шифрования

Алгоритм проверки цифровой подписи [signature verification algorithm] —

Составная часть схемы цифровой подписи. Алгоритм, на вход которого подаются цифровая подпись, открытый ключ и другие открытые параметры

схемы цифровой подписи. В схемах цифровой подписи с восстановлением сообщения результатом работы алгоритма является заключение о корректности подписи и, если она корректна, — само сообщение, извлеченное из подписи. В остальных случаях сообщение является частью входных данных, и алгоритм проверки выдает лишь заключение о корректности подписи. В некоторых разновидностях схемы цифровой подписи при проверке подписи используется интерактивный протокол. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Схема цифровой подписи

См. также: Алгоритм формирования цифровой подписи, Интерактивный протокол, Процесс проверки подписи

Алгоритм расшифрования [decryption algorithm, deciphering] —

Криптографический алгоритм, обратный к алгоритму зашифрования и реализующий функцию расшифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм шифрования

См. также: Дешифрование, Функция расшифрования, Уравнение расшифрования, Алгоритм зашифрования

Алгоритм формирования цифровой подписи [signature generation algorithm] —

Составная часть схемы цифровой подписи. Алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое сообщение, секретный ключ, а также открытые параметры схемы цифровой подписи. Результатом работы алгоритма является цифровая подпись. В некоторых разновидностях схемы цифровой подписи при формировании подписи используется протокол *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Схема цифровой подписи Син.: Алгоритм генерации цифровой подписи.

См. также: Алгоритм проверки цифровой подписи, Групповой протокол подписи, Подделка цифровой подписи

Алгоритм хеширования [hashing algorithm] —

В криптографии — алгоритм, реализующий криптографическую хеш-функцию. В математике и программировании — алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале — от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

См. также: Криптографическая хеш-функция

Алгоритм шифрования [encryption algorithm] —

Под алгоритмом шифрования в зависимости от контекста понимается алгоритм зашифрования или алгоритм расшифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм имитозащищающего кодирования

Ниже: Алгоритм блочного шифрования, Алгоритм зашифрования, Алгоритм расшифрования, Алгоритм шифрования RSA, Инволютивный алгоритм шифрования, Итеративный алгоритм шифрования

Алгоритм шифрования RSA [RSA encryption algorithm] —

Алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения асимметричных шифрсистем. Основан на возведении в степень в кольце вычетов по модулю, являющемуся произведением двух больших простых чисел *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм шифрования

См. также: Шифрсистема RSA

Альтернативная площадка [alternative site] —

Альтернативное рабочее помещение, выбранное организацией для использования в случае, если после аварии обычные операции бизнеса не могут осуществляться в обычном помещении. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

Анализ процедур защиты —

Независимый просмотр и анализ системных записей и активностей с целью проверки их адекватности системным управляющим функциям для обеспечения соответствия с принятой стратегией защиты и операционными процедурами, обнаружения пробелов в защите и выдачи рекомендаций по любым указанным изменениям в управлении, стратегии и процедурах. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Данные трассировки защиты, Стратегия защиты

Анализ риска (информационного) [risk analysis] —

1. Процесс понимания природы риска и определения уровня риска. Примечание 1. Анализ риска обеспечивает основу для оценивания риска и решений, касающихся воздействия на риск. Примечание 2. Анализ риска включает определение степени риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Процесс изучения природы и характера риска и определения уровня риска.

Примечание 1 - Анализ риска обеспечивает базу для проведения сравнительной оценки риска и принятия решения об обработке риска.

Примечание 2 - Анализ риска включает в себя количественную оценку риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

3. Систематическое использование информации для определения источников риска и количественной оценки риска. *[ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен в действие: 01.02.2008]*.

4. Систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

5. Систематический процесс определения величины риска. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

6. Процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчетов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Задача анализа риска состоит в определении степени приемлемости того или иного риска в работе системы. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Допустимый риск, Оценка риска, Сравнительная оценка риска, Определение приемлемости уровня риска

Анализ трафика [traffic analysis] —

1. Заключение о состоянии информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота). *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Анализ совокупности шифрованных сообщений, передаваемых по системе связи, не приводящий к дешифрованию, но позволяющий противнику и/или нарушителю получить косвенную информацию о передаваемых открытых сообщениях и в целом о функционировании наблюдаемой системы связи. Анализ трафика использует особенности оформления шифрованных сообщений, их длину, время передачи, данные об отправителе и получателе и

т.п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Ниже: Сетевой анализатор пакетов, Сетевые анализаторы (снифферы)

См. также: Безопасность связи, Конфиденциальность трафика, Криптографические средства физического и канального уровня, Межсетевой экран (сетевой экран), Сетевой трафик

Аналоговый —

Определение, относящееся к данным, которые представлены непрерывными значениями какой-либо физической переменной. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Цифровой

Анонимайзер [anonymizer] —

Изначально средство для скрытия информации о компьютере или пользователе в сети. Может быть программой, устанавливаемой на компьютер (такой как прокси-сервер Tor), или специальным веб-сайтом (веб-прокси). На сегодняшний день веб-прокси наиболее популярны, так как не требуют каких-либо дополнительных настроек или программного обеспечения. Работает веб-анонимайзер следующим образом: пользователь заходит на веб-сайт предоставляющий услугу анонимайзера, вводит в адресную строку адрес веб-страницы, которую пользователь желает посетить анонимно. Анонимайзер загружает эту страницу себе, обрабатывает её, и передает пользователю от своего имени (имени сервера-анонимайзера). Сфера использования анонимайзеров сегодня сместилась от обеспечения конфиденциальности информации о пользователе в сторону предоставления доступа к запрещённым в локальной сети веб-сайтам. Необходимо отметить, что использование анонимайзера не только не обеспечивает конфиденциальности передаваемых данных между пользователем и целевым веб-сервером, но и является дополнительным звеном возможности утечки персональной информации. Не рекомендуется при работе через анонимайзер использовать сколько-нибудь значимые учётные записи, так как они могут быть легко скомпрометированы на сервере-анонимайзере. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Анонимная сеть TOR

Анонимная сеть I2P [anonymous network I2P] —

Анонимная сеть, работающая подобно TOR, но в отличие от TOR – это внутренняя сеть, она полностью децентрализована, не имеет постоянного списка серверов, не использует двунаправленных туннелей, что существенно затрудняет временную атаку, и поддерживает шифрование из конца в конец. Так как мы никогда не знаем, сохранены ли все соединения в логе данного конкретного узла или нет, то единственный способ реально быть уверенным в отсутствии таких записей заключается в создании собственного узла маршрутизации и смешении вашего трафика с трафиком других пользователей, которые не обязательно должны вам доверять, но которые будут смешивать

свой трафик с вашим трафиком в своих узлах. Таким образом, основная идея I2P – каждый узел направляет свой трафик всем другим и смешивает свой трафик с трафиком других, в то время как трафик любого узла также будет смешан с трафиком других и отправлен другим с помощью, так называемого, туннеля. Сеть высоко динамична и полностью децентрализована. Она состоит только из узлов, знающих о существовании вашего узла, так как кроме сторон, использующих ваш узел, не должно быть никакого другого трафика, смешиваемого с вашим. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Анонимная сеть TOR

Анонимная сеть TOR [TOR (The Onion Router)] —

Система, позволяющая устанавливать в режиме on-line анонимное сетевое соединение. Создана по заказу ВМС США, в 2002 году исходные коды были переданы независимым разработчикам, которые создали клиентское программное обеспечение со свободной лицензией, чтобы все желающие могли проверить его на отсутствие программных закладок. После установки его на компьютер пользователи могут сохранять анонимность при посещении сайтов, публикации материалов, отправке сообщений и при работе с другими приложениями, использующими протокол TCP. Программное обеспечение TOR работает на сетевом уровне, позволяя обеспечивать анонимные исходящие соединения и анонимные скрытые службы. Безопасность трафика обеспечивается за счёт использования распределённой сети прокси-серверов (нодов — «узлов»), называемых «многослойными маршрутизаторами» (onion routers). Каждый пакет, попадающий в систему, проходит через несколько различных узлов, которые выбираются случайным образом. Перед отправлением пакет последовательно шифруется ключами этих серверов: сначала для последнего узла, потом для предпоследнего, и, в конце концов, для первого. Когда каждый узел получает пакет, он расшифровывает пакет на своем ключе (аналогия с тем, как чистят луковицу) и узнает, куда отправить пакет дальше. На компьютере получателя должно быть установлено программное обеспечение сервера TOR. На последнем узле цепочки TOR исходное сообщение от клиента окончательно расшифровывается для передачи его серверу в первоначальном виде. В результате: первый узел цепочки знает настоящий адрес клиента; последний узел цепочки видит исходное сообщение от клиента, хотя и не знает истинного отправителя; сервер-адресат видит исходное сообщение от клиента, хотя и не знает истинного отправителя. Анонимная сеть TOR предназначена для сокрытия факта связи между клиентом и сервером, однако он принципиально не может обеспечить полное закрытие передаваемых данных, поскольку шифрование является лишь средством достижения анонимности. Для обеспечения конфиденциальности надо использовать шифрование из конца в конец. Кроме того, анонимная сеть TOR работает только по протоколу SOCKS, поддерживаемого не всеми приложениями, через которые может понадобиться вести анонимную

деятельность. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также Анонимайзер, Анонимная сеть I2P

Анонимность [anonymity] —

Понятие, родственное неотслеживаемости. Выражает предоставляемую участникам (протокола) возможность выполнять какое-либо действие анонимно, т. е. не идентифицируя себя. При этом, однако, участник обязан доказать свое право на выполнение этого действия. Анонимность бывает абсолютной и отзываемой. В последнем случае в системе есть выделенный участник, арбитр, который при определенных условиях может нарушать анонимность и идентифицировать участника, выполнившего данное конкретное действие. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Неотслеживаемость

Анти-антивирусный вирус —

Вредоносная программа, одной из функций которой является нарушение работы установленной на пораженном компьютере антивирусной защиты. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Компьютерный вирус

Антибот [anti bot] —

1. Программное обеспечение, предназначенное для обнаружения компьютеров, инфицированных в качестве узлов бот-сети, и предотвращения ущерба от воздействия вредоносного программного обеспечения путем блокирования скрытой передачи и приема управляющих команд. В основе работы лежит мониторинг действий выполняемых на компьютере приложений. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.
2. Программное обеспечение для автоматического обнаружения и удаления программ-роботов, шпионского программного обеспечения, потенциально нежелательных программ и других видов вредоносного программного обеспечения. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Бот, Бот-сеть (ботнет), Конфикер

Антивирус —

См. Антивирусная программа

Антивирусная защита —

Комплекс организационных, правовых, технических и технологических мер, применяемых для обеспечения защиты средств вычислительной техники и автоматизированной системы от воздействия программных вирусов. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Ниже: Антивирусная программа

См. также: Компьютерный вирус

Антивирусная защита по требованию —

Защита по требованию запускается самим пользователем и, как правило, заключается в полном или выборочном сканировании присутствующих на

жестких и сетевых дисках компьютера файлов. Защита по требованию производит однократную проверку оперативной памяти компьютера. В большинстве случаев антивирусные сканеры гораздо более требовательны к ресурсам компьютера, нежели постоянная антивирусная защита. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Антивирусная программа

Син.: Антивирусный сканер

См. также: Постоянная антивирусная защита

Антивирусная программа [antivirus] —

1. Программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

Многие современные антивирусы расширяют набор своих функций, позволяя обнаруживать и удалять также троянские и прочие вредоносные программы. Идёт и процесс интеграции антивирусных функций в другие программы — например, файрволы.

Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать сотни тысяч вирусов, но ни одна из них не даст 100% защиты. Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

3. Программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

В настоящее время большинство ведущих антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер). *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Антивирусная защита

Ниже: Постоянная антивирусная защита, Антивирусная защита по требованию

Син: Антивирус

Антивирусные базы данных —

Базы данных, содержащие сигнатуры огромного количества вредоносных программ. Одна запись в подобной базе может содержать алгоритмы детектирования как одной, так и сразу нескольких разновидностей вредоносных программ. Во втором случае записи присваивается версия ".gen", например, I-Worm.Bagle.gen.

С целью обеспечения надежной защиты пользователя от новых вредоносных программ набор сигнатурных записей в антивирусной базе данных необходимо регулярно обновлять.

С 1 августа 2004 года "Лаборатория Касперского", заслуженно являясь мировым лидером в скорости реакции на появление новых вредоносных программ, выпускает обновления антивирусной базы данных один раз в час. Вдобавок к этому в случае появления особенно опасной вредоносной программы производится выпуск срочного обновления, содержащего сигнатуры и алгоритмы детектирования данной вредоносной программы.

Понимая, что даже подобной частоты обновления антивирусных баз может быть недостаточно в случае эпидемии сетевых flash-червей (например, Worm.Win32.Lovesan.a и Worm.Win32.Sasser.a), молниеносно распространяющихся с одного компьютера на другой, используя прямое подключение через бреши в защите TCP/IP-портов операционной системы, эксперты компании постоянно совершенствуют эвристические алгоритмы проактивной поведенческой защиты.

Подобная проактивная защита, анализируя в реальном времени выполняемые программами действия, позволяет блокировать работу и дальнейшее размножение вредоносных программ еще до появления соответствующих обновлений антивирусной базы данных. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Син.: Эвристический анализатор, Поведенческий блокиратор, Проактивная защита

Антивирусный вирус —

Программа, одной из функций которой является поиск и удаление какой-либо другой вредоносной программы.

Не стоит заблуждаться: даже если подобные программы не осуществляют никаких очевидных деструктивных действий, они всё равно наносят вред пользователю, замедляя скорость подключения к интернету, снижая производительность компьютера и зачастую вызывая проблемы в работе операционной системы и других установленных на компьютере программ. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Компьютерный вирус

Антивирусный монитор —

См. Постоянная антивирусная защита

Антивирусный сканер —

См. Антивирусная защита по требованию

Антидебаггер —

Набор методов уклонения от дизассемблирования (разбора программы с целью анализа её функциональности и примененных при её создании алгоритмов), встроенных в код какой-либо программы.

Подобные методы присущи не только вредоносным программам. Зачастую антидебаггерами защищают вполне легальные программы, например, индустриальные системы защиты компакт-дисков от копирования. Более того, в большинстве лицензионных соглашений легальных коммерческих программных продуктов содержится пункт, запрещающий их дизассемблирование, поскольку в коде таких программ зачастую содержатся патентованные программные технологии. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Син.: Антидизассемблер

Антидизассемблер —

См. Антидебаггер

Антиспам-бот —

Одна из программ, защищающих пользователя от спама. Представляет собой систему автоответов, в которых получатель просит отправителя подтвердить, что тот является реальным лицом (пройдя по ссылке или написав письмо на другой почтовый ящик получателя*). [Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

См. также: Спам

Антифрод системы [Fraud Management System (FMS))] —

Системы выявления и предупреждения мошеннических действий в системах дистанционного банковского обслуживания, направленных на хищение денежных средств со счетов клиентов, а также, в более широком смысле, при использовании платных услуг. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*.

Син.: Фрод-мониторинг

См. также: Фрод, Дроппер, Инцидент в системе дистанционного банковского обслуживания (или инцидент, связанный с мошенничеством или покушением на совершение мошенничества в системе дистанционного банковского обслуживания), Преступное/мошенническое программное обеспечение

Аппаратная закладка [bug, hardware Trojan] —

1. Электронное устройство несанкционированно и замаскировано установленное в техническом средстве обработки информации или в выделенном помещении с целью обеспечения утечки защищаемой информации *[ОСТ В1 00464-82 Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. Введен в действие: 01.01.1998]*.

2. Электронное устройство, встраиваемое или подключаемое к элементам технических средств обработки информации в целях нарушения безопасности

информации при ее обработке техническими средствами. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

3. Устройство в электронной схеме, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу вычислительной системы. Результатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение её нормального функционирования, например несанкционированный доступ к информации, её изменение или блокирование.

Также аппаратной закладкой называется отдельная микросхема, подключаемая злоумышленниками к атакуемой системе для достижения тех же целей. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]* Син.: Специальное закладное электронное устройство. См. также: Закладочное устройство, Программная закладка, Специальная проверка

Аппаратное обеспечение [hardware] —

Любое физическое устройство, осуществляющее обработку данных.

Примечание. Примером является компьютер, периферийное оборудование. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Син.: Средства вычислительной техники

См. также: Аппаратные средства защиты информации, Класс защищенности средств вычислительной техники (автоматизированной системы), Обработка данных, Программное обеспечение

Аппаратное шифрование [hardware encryption] —

Шифрование, выполняемое с применением аппаратных криптографических средств. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Шифрование

См. также: Аппаратные криптографические средства

Аппаратные криптографические средства [cryptographic hardware (device, facility)] —

Криптографические средства, реализованные в виде специальных технических устройств. Реализуют одну или несколько криптографических функций или их частей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографические средства

Ниже: Криптографическое устройство

См. также: Аппаратное шифрование, Программные криптографические средства

Аппаратные средства защиты информации —

Механические, электротехнические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации

[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996].

Выше: Виды механизмов защиты

См. также: Технические средства защиты (информационной безопасности)

Арбитр [arbiter] —

Участник протокола с арбитром, выполняющий процедуру арбитража *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Арбитраж, Протокол с арбитром

Арбитраж [arbitration] —

Формализованная процедура разрешения споров о трактовке результатов выполнения криптографического протокола. Такая процедура необходима для многих прикладных криптографических протоколов, в т. ч. схем цифровой подписи, протоколов подписания контракта, платежей электронных систем и т. п., и должна рассматриваться как неотъемлемая часть этих протоколов. Для самой процедуры арбитража требуется либо алгоритм, выполняемый арбитром на входных данных, предоставленных ему заявителем (заявителями), либо специальный протокол с участием всех заинтересованных сторон. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Арбитр, Прикладной криптографический протокол

Архитектура [architecture] —

Базовая организация системы, воплощенная в ее компонентах, их отношениях между собой и с окружением, а также принципы, определяющие проектирование и развитие системы. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Архитектура вычислительной машины, Архитектура информационной безопасности Взаимоувязанной сети связи Российской Федерации

Архитектура вычислительной машины [computer architecture] —

Концептуальная структура вычислительной машины, определяющая проведение обработки информации и включающая методы преобразования информации в данные и принципы взаимодействия технических средств и программного обеспечения. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Архитектура

Архитектура информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Логическая структура и принципы обеспечения информационной безопасности ВСС РФ.

Примечание - логическая структура обеспечения информационной безопасности ВСС РФ - совокупность органов, служб, средств системы

обеспечения информационной безопасности ВСС РФ, объектов информационной безопасности ВСС РФ и процессов взаимодействия объектов информационной безопасности ВСС РФ между собой и с подсистемой управления системы обеспечения информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации

Асимметричная шифрсистема [public-key cryptosystem, asymmetric cryptosystem] —

Система шифрования, в которой асимметричным образом используются ключи двух видов — открытые ключи и секретные ключи. Открытый ключ участника протокола задает процесс зашифрования направляемых в его адрес сообщений и является общедоступным. Секретный ключ участника протокола задает процесс расшифрования направляемых в его адрес сообщений и хранится им в тайне. Криптографическая сойкость асимметричной шифрсистемы определяется трудоемкостью, с которой противник и/или нарушитель может вычислить секретный ключ, исходя из знания открытого ключа и другой дополнительной информации о шифрсистеме. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система шифрования

Ниже: Шифрсистема RSA

См. также: Симметричная шифрсистема, Закрытый ключ, Открытый ключ, Протокол (алгоритм) обмена ключами Диффи–Хеллмана

Атака [attack] —

1. Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Попытка преодоления системы защиты информационной системы.

Примечания - Степень "успеха" атаки зависит от уязвимости и эффективности системы защиты. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Ниже: Адаптивная атака, Атака (при применении информационных технологий), Атака блокировки доступа с целью получения выкупа, Атака компьютерной сети, Атака на криптографический протокол, Атака на криптосистему, Атака нулевого дня, Атака по алфавитному списку, Атаки методом подбора пароля, Инъекция SQL, Компьютерная атака, Мониторинговые атаки (объекта оценки), Сетевая атака

См. также: Вредоносное программное обеспечение, Компьютерный вирус, Хакер, Эксплойт

Атака (при применении информационных технологий) [attack] —

Действия, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Атака

См. также: Несанкционированный доступ к информации

Атака блокировки доступа с целью получения выкупа [ransomware attack] —

Обычно обнаруживает себя в виде неудаляемого всплывающего окна с сообщением о необходимости уплатить определенную сумму для разблокировки компьютера. В качестве прикрытия может использоваться, например, имя какой-либо официальной правоохранительной организации, обвиняющей пользователя в обращении к какому-либо нелегальному ресурсу или нарушении лицензионных условий. Несмотря на обещание, после полной уплаты указанной суммы разблокировки компьютера не происходит. С 2011 года широко применяется криминальными структурами для получения нелегальных доходов. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*

Выше: Атака

Атака «встреча посередине» [meet-in-the-middle attack] —

Атака на криптосистему, основанная на методе «встреча посередине». *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атака компьютерной сети [attack on computer network] —

Действия, направленные на манипуляцию, разрушение, блокирование, дезорганизацию или уничтожение информации в компьютерах и сетях компьютерных, или на сами компьютеры и сети непосредственно *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Выше: Атака

Атака мистификации [spoofing attack] —

См. Спуфинг.

Атака на криптографический протокол [attack on the protocol] —

Попытка проведения анализа сообщений протокола и/или выполнения не предусмотренных протоколом действий с целью нарушения работы протокола и/или получения информации, составляющей секрет его участников. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака

Ниже: Атака на протокол с повторной передачей, Атака «противник в середине»

См. также: Криптографический протокол

Атака на криптосистему [attack on the cryptosystem] —

Попытка противника и/или нарушителя понизить уровень безопасности конкретной криптографической системы на основе определенных методов криптоанализа и при некоторых предположениях криптоанализа. Разработчик, законный пользователь и противник при проведении криптографического анализа моделируют атаки на криптосистему. Совокупность различных атак постоянно расширяется за счет развития теоретических методов и возможностей техники. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака

Ниже: Активная атака, Атака на криптосистему на основе известного открытого текста, Атака на криптосистему на основе только шифрованного текста, Атака на основе эквивалентных ключей, Атака опробованием с использованием памяти, Атака последовательным опробованием, Атака протяжкой вероятного слова, Атака со словарем, Атака со словарем паролей, Атака «встреча посередине», Корреляционная атака, Линейная атака, Лобовая атака, Пассивная атака, Подмена, Разностная атака, Разностная атака на основе искажений, Разностно-линейная атака

См. также: Криптографическая стойкость

Атака на криптосистему на основе известного открытого текста [known plaintext attack] —

Атака на криптосистему, при которой противнику и/или нарушителю известен открытый текст. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атака на криптосистему на основе только шифрованного текста [ciphertext-only attack] —

Атака на криптосистему, при которой противнику и/или нарушителю известен шифрованный текст и не известен открытый текст. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атака на основе эквивалентных ключей [equivalent keys attack] —

Атака на криптосистему, основанная на методе эквивалентных ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

См. также: Эквивалентные ключи

Атака на отказ в обслуживании [Denial-of-Service attack (DoS attack)] —

1. Сетевая атака, приводящая к блокированию информационных процессов в автоматизированной системе. *[ГОСТ Р 53114-2008 Защита*

информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009].

2 Сетевая атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднен. Отказ системы может быть как самостоятельной целью, так и одним из шагов к проникновению в систему (в расчете на то, что во внештатной ситуации в системе появятся новые уязвимости), либо иметь целю затруднение обнаружения несанкционированных действий в системе. В качестве объектов атак на отказ в обслуживании могут выступать системы интернет-банкинга, платежные шлюзы кредитных карт, интернет-магазины и т. п. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/].*

Выше: Сетевая атака. Ниже: Ветвящаяся бомба, Распределенная атака на отказ в обслуживании, Непреднамеренная атака на отказ в обслуживании

См. также: Блокирование доступа (к информации)

Атака на протокол с повторной передачей [replay attack] —

Атака на криптографический протокол, при которой противник и/или нарушитель записывает все передаваемые сообщения и впоследствии повторно передает их от имени законного пользователя *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Атака на криптографический протокол

См. также: Функция-сервис аутентификации сторон

Атака нулевого дня [zero day attack] —

Термин, обозначающий вредоносные программы, против которых еще не разработаны защитные механизмы или уязвимости, которые не устранены. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Атака

См. также: Уязвимость нулевого дня

Атака опробованием с использованием памяти [memory using attack, memory-used search attack] —

Атака на криптосистему, основанная на методе, существенно использующем память. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Атака на криптосистему

Атака по алфавитному списку [dictionary attack] —

Рассылка сообщений на огромное количество автоматически сгенерированных адресов на некотором сервере из расчета, что какие-то из этих адресов окажутся действующими. Адреса генерируются по словарю, и атака по ним идет в алфавитном порядке. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/].*

Выше: Атака

Атака последовательным опробованием [sequential key search] —

Атака на криптосистему, основанная на методе последовательного опробования ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атака «противник в середине» [man-in-the-middle attack] —

1. В широком смысле — вид атаки, при котором противник имеет возможность полностью контролировать обмен сообщениями и управляющими командами в коммуникационном канале: перенаправлять их, модифицировать, подменять, блокировать или создавать новые. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*

2. Атака на криптографический протокол, в которой противник C выполняет этот протокол как с участником A, так и с участником B. Противник C выполняет сеанс с участником A от имени B, а с участником B от имени A. В процессе выполнения противник пересылает сообщения от A к B и обратно, возможно, подменяя их (отсюда название атаки). В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для B под именем A. Для осуществления атаки «противник в середине» необходимо обеспечивать синхронизацию двух сеансов протокола. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптографический протокол

Атака протяжкой вероятного слова [moving probable word attack] —

Атака на криптосистему, основанная на методе протяжки вероятного слова. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атака со словарем [dictionary attack] —

Атака на криптосистему, использующая словарь элементов открытого текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атака со словарем паролей [password attack] —

Атака на криптосистему, основанная на переборе значений пароля. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему

Атаки методом подбора пароля [brute force attacks] —

Так называемые атаки методом "грубой силы". Как правило, пользователи применяют простейшие пароли, например "123", "admin" и т.д. Этим и пользуются компьютерные злоумышленники, которые при помощи специальных троянских программ вычисляют необходимый для проникновения в сеть пароль методом подбора - на основании заложенного в эту программу

словаря паролей или генерируя случайные последовательности символов. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Атака

Атрибут безопасности [security attribute] —

1. Характеристика субъектов, пользователей (включая внешние продукты ИТ), объектов, информации, сеансов и/или ресурсов, которые используются при определении функциональных требований безопасности, и значения которых используются при осуществлении функциональных требований безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления политики безопасности объекта оценки. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Политика безопасности объекта оценки, Требование безопасности (объекта оценки)

Атрибуты файла —

Характеристики файла, наделяющие файл определенными свойствами. Для наиболее распространенных в настоящее время файловых систем FAT16, FAT32 и NTFS можно выделить следующие файловые атрибуты:

"Только для чтения" (Read-only) - означает, что файл доступен операционной системе только для чтения, т. е. в него нельзя вносить какие-либо исправления. В большинстве случаев это не означает, что исправления внести вовсе невозможно, просто при попытке изменить файл с данным атрибутом пользователю будет показано соответствующее предупреждение.

"Скрытый" (Hidden) - подразумевается, что файл с данным атрибутом не выводится при показе тех или иных списков файлов. В большинстве программ обработку этого атрибута можно настраивать. Например, стандартный "Проводник" Windows XP позволяет как прятать, так и показывать файлы с атрибутом "скрытый". Во втором случае иконка файла отображается полупрозрачной.

"Системный" (System) - файлы с атрибутом "системный" чаще всего относятся к критичным файлам операционной системы, которые нельзя удалять или изменять. В общем смысле, атрибут "системный" является "утяжеленным" вариантом атрибута "только для чтения", скомбинированным с атрибутом "скрытый". В стандартном "Проводнике" Windows XP атрибут "системный" отрабатывается аналогично атрибуту "скрытый" - подобные файлы по умолчанию спрятаны от пользователя, но можно и разрешить их показ.

"Архивный" (Archive) - в настоящее время по своему прямому назначению данный файловый атрибут FAT практически не используется. Изначально предполагалось, что этот атрибут будет указывать программам

архивации файлы, предназначенные для резервного копирования. Другими словами, программа, осуществляющая резервное копирование файла на жестком диске, должна была сбрасывать атрибут "архивный", а программы, вносящие в последующем в этот файл какие-либо изменения, наоборот, вновь его устанавливать. Таким образом, программа резервного копирования путем проверки данного файлового атрибута могла легко определить, изменялся ли данный файл на жестком диске с момента осуществления предыдущего резервного копирования.

В файловой системе NTFS, применяющейся в современных версиях ОС Windows, помимо уже приведенных атрибутов, в файловых атрибутах хранятся имена файлов, само содержимое файлов, а также множество другой информации. Более того, вдобавок к набору стандартных файловых атрибутов, файловая система NTFS позволяет разработчикам приложений создавать свои собственные атрибуты, с которыми затем могло бы работать их приложение. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/].*

Син.: Файловые атрибуты

Аттестационные испытания [evaluation test] **—**

Испытания, проводимые для оценки уровня качества продукции при ее аттестации по категориям качества. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011].*

Выше: Испытания

См. также: Аттестация, Контрольные испытания, Сертификационные испытания, Типовые испытания

Аттестация —

Определение квалификации, уровня знаний и умений чего-либо, а также соответствия требованиям (продукция, технические устройства, рабочие места); отзыв, характеристика. Полученный в результате аттестации документ называют аттестатом.

В обучении — установление уровня знаний, умений и навыков обучаемых по отношению к объёму и содержанию учебных дисциплин, представленных и утвержденных в учебных планах и учебных программах.

В аудите — проверка квалификации физических лиц, изъявивших желание заниматься аудиторской деятельностью, с выдачей кандидатам, успешно сдавшим необходимые квалификационные экзамены, квалификационного аттестата аудитора установленного образца.

В деятельности организации — проверка уровня подготовки, мастерства, квалификации работника. Непрохождение аттестации является одним из оснований для расторжения трудового договора по инициативе работодателя. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/].*

Ниже: Аттестация автоматизированной системы в защищенном исполнении, Аттестация испытательных организаций и подразделений, Аттестация методики испытаний, Аттестация объекта в защищенном исполнении, Аттестация объектов информатизации, Аттестация производства

См. также: Аттестационные испытания

Аттестация автоматизированной системы в защищенном исполнении —

Процесс комплексной проверки выполнения заданных функций защищаемой автоматизированной системы по обработке информации на соответствие требованиям стандартов и/или нормативных документов в области защиты информации и оформления документов о ее соответствии выполнять функции по обработке защищаемой информации на конкретном объекте информатизации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

Выше: Аттестация

См. также: Автоматизированная система в защищенном исполнении

Аттестация испытательных организаций и подразделений [certification of testing organizations and divisions] —

Удостоверение компетентности испытательных организаций и подразделений и их оснащенности, обеспечивающих проведение на должном техническом уровне всех предусмотренных нормативно-технической документацией испытаний закрепленных видов продукции и (или) видов испытаний. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

Выше: Аттестация

Аттестация методики испытаний [approval of test procedure] —

Определение обеспечиваемых методикой значений показателей точности, достоверности и (или) воспроизводимости результатов испытаний и их соответствия заданным требованиям. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

Выше: Аттестация

Аттестация объекта в защищенном исполнении —

Официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов и норм эффективности защиты информации. *[Положение о государственном лицензировании деятельности в области защиты информации (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. N 10)(с изменениями и дополнениями от 24 июня 1997 г. N 60)]*.

Выше: Аттестация, Норма эффективности защиты информации

Аттестация объектов информатизации —

1. Деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации. *[Р 50.1.056-2005 Техническая*

защита информации. Основные термины и определения. Введен в действие: 01.06.2006].

2. Комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. *[Положение по аттестации объектов информатизации по требованиям безопасности информации" (утв. Гостехкомиссией РФ 25.11.1994)]*. Выше: Аттестация

См. также: Объект информатизации, Объекты информатизации, аттестуемые по требованиям безопасности информации, Объекты информатизации, подлежащие обязательной аттестации, Система аттестации объектов информатизации по требованиям безопасности информации

Аттестация производства —

Официальное подтверждение органом по сертификации или другим специально уполномоченным органом наличия необходимых и достаточных условий производства данной продукции (исполнения данных услуг), обеспечивающих стабильность требований к ней, заданных в нормативных документах и контролируемых при сертификации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Аттестация

См. также: Орган по сертификации, Федеральные органы по сертификации

Аудит [audit] **—**

Систематический независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

Примечания:

1. Внутренние аудиты, называемые аудитами первой стороны, проводит для внутренних целей сама организация или от ее имени другая организация. Результаты внутреннего аудита могут служить основанием для декларации о соответствии. Во многих случаях, особенно на малых предприятиях, аудит должен проводиться специалистами (людьми, не несущими ответственности за проверяемую деятельность).

2. Внешние аудиты включают аудиты, называемые аудитами второй стороны и аудитами третьей стороны.

Аудиты второй стороны проводят стороны, заинтересованные в деятельности предприятия, например, потребители или другие лица от их имени. Аудиты третьей стороны проводят внешние независимые организации. Эти организации проводят сертификацию или регистрацию на соответствие требованиям, например, требованиям ГОСТ Р ИСО 9001 и ГОСТ Р ИСО 14001.

3. Аудит систем менеджмента качества и экологического менеджмента, проводимый одновременно, называют "комплексным аудитом".

4. Если аудит проверяемой организации проводят одновременно несколько организаций, то такой аудит называют "совместным аудитом". *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Ниже: Аудит безопасности автоматизированной информационной системы, Аудит менеджмента риска, Аудиторская проверка безопасности информации в информационной системе, Аудиторская проверка информационной безопасности в организации

Син.: Аудит (безопасности)

См. также: Аудитор, Выводы (наблюдения) аудита, Группа по аудиту, Заказчик аудита, Заключение по результатам аудита информационной безопасности (аудиторское заключение), Наблюдатель, Область аудита, План аудита, Проверяемая организация, Программа аудита, Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям, Сопровождающий, Технический эксперт

Аудит (безопасности) [security audit] —

1. Независимая оценка программных продуктов и процессов, проводимая уполномоченным лицом с целью оценить их соответствие требованиям. *[ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. Введен в действие: 01.03.2012]*.

2. Совокупность действий по независимой проверке и изучению документации автоматизированной информационной системы, а также по испытаниям средств защиты информации, направленная на обеспечение выполнения установленной политики безопасности информации и правил эксплуатации автоматизированной информационной системы, на выявление уязвимостей автоматизированной информационной системы и на выработку рекомендаций по устранению выявленных недостатков в средствах защиты информации, политике безопасности информации и правилах эксплуатации автоматизированной информационной системы.

Примечание - Аудит безопасности может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией (внешний аудит), а также подразделением или должностным лицом организации (внутренний аудит). *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

3. Инспекция системных записей и работы персонала с целью проверки функционирования систем защиты, их соответствия принятой стратегии требованиям эксплуатации, а также выработки соответствующих рекомендаций *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

Син.: Аудит, Контроль средств защиты

Аудит безопасности автоматизированной информационной системы —

Проверка реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценкиих эффективности и корректности, а также разработки предложений по их совершенствованию. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Аудит

См. также: Автоматизированная информационная система

Аудит информационной безопасности в организации —

См. Аудиторская проверка информационной безопасности в организации.

Аудит менеджмента риска [risk management audit] —

1. Систематический, независимый, документированный процесс получения свидетельств и объективное их оценивание для установления степени адекватности и эффективности системы риск-менеджмента или ее выделенной части. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Систематический, независимый, документированный процесс получения свидетельств и оценки их объективности для установления степени адекватности и эффективности структуры менеджмента риска или ее части. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Выше: Аудит

См. также: Менеджмент риска

Аудитор [auditor] —

Лицо, которое проводит аудит. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Группа по аудиту, Наблюдатель, Сопровождающий, Технический эксперт

Аудиторская проверка безопасности информации в информационной системе [computer system audit] —

Проверка реализованных в информационной системе процедур обеспечения безопасности информации с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Аудит

См. также: Информационная система

Аудиторская проверка информационной безопасности в организации [security audit] —

1. Систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению информационной безопасности и установлению степени выполнения в

организации критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности.
Примечание. Аудит информационной безопасности в организации может осуществляться независимой организацией (третьей стороной) по договору с проверяемой организацией, а также подразделением или должностным лицом организации (внутренний аудит). *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Аудит Син.: Аудит информационной безопасности в организации.

См. также: Выводы (наблюдения) аудита, Заказчик аудита, Критерий аудита информационной безопасности организации, Свидетельства (доказательства) аудита информационной безопасности организации, Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям, Область аудита информационной безопасности

Аутентификатор —

Блок данных, добавленный к сообщению, зашифрованный с помощью асимметричного криптографического алгоритма и используемый в процессе передачи сообщения для проверки подлинности отправителя и целостности сообщения. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Аутентификация

Аутентификационные данные [authentication data] **—**

Информация, используемая для верификации предъявленного идентификатора пользователя. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Аутентификация, Входить в систему

Аутентификация [authentication] **—**

1.Обеспечение гарантий идентичности предъявленной сущности. *[ISO/IEC 10181-2:1996 Информационные . технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основы аутентификации]*.

2.Обеспечение гарантии того, что заявленные характеристики обьекта правильны. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента*

информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013].

3.Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности). *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)].*

4.Установление (то есть проверка и подтверждение) подлинности различных аспектов информационного взаимодействия: содержания и источника передаваемых сообщений, сеанса связи, времени взаимодействия и т. д. Является важной составной частью проблемы обеспечения достоверности получаемой информации. Особенно остро эта проблема стоит в случае не доверяющих друг другу сторон, когда источником угроз может служить не только третья сторона (противник), но и сторона, с которой осуществляется информационное взаимодействие (нарушитель). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Ниже: Аутентификация абонента (пользователя), Аутентификация источника данных, Аутентификация на основе контекста, Аутентификация на основе одноразовых паролей, Аутентификация на основе сертификатов, Аутентификация отправителя данных, Аутентификация равноправного логического объекта, Аутентификация сообщения, Аутентификация сторон, Аутентификация субъекта доступа, Биометрическая аутентификация, Двухфакторная аутентификация, Интерактивная аутентификация, Многофакторная аутентификация

См. также: Идентификация, Идентификация и аутентификация, Информация аутентификации, Подлинность, Обмен аутентификацией

Аутентификация абонента (пользователя) [user authentication] —

Доказательство абонентом (законным пользователем) соответствия своему имени как участника протокола. Проводится с целью проверки прав и полномочий абонента. Как правило, осуществляется посредством протокола идентификации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Аутентификация

См. также: Аутентификация сторон, Участник (протокола)

Аутентификация источника данных [data origin authentication] —

1. Подтверждение подлинности источника полученных данных. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].*

2. Проверка и подтверждение того, что набор данных (сообщение, документ) был создан именно заявленным источником. Не надо путать с аутентификацией отправителя, так как он мог передать документ, созданный и подписанный другим лицом. Аутентификация источника данных предполагает и проверку целостности, так как если данные подверглись модификации, то они

уже имеют другой источник. Если стороны доверяют друг другу, то аутентификацию источника данных. можно осуществить применением симметричной шифрсистемы, так как правильно расшифрованное, либо сообщение с верным значением кода аутентичности сообщения подтверждает знание отправителем их общего секретного ключа. Для не доверяющих друг другу сторон необходимо использовать асимметричную шифрсистему. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Аутентификация

См. также: Аутентификация отправителя данных

Аутентификация на основе контекста [context-based authentication] —

Использует дополнительную контекстную информацию (расположение, время, физическое устройство, сеть, запрашиваемое приложение). В зависимости от контекста пользователю предлагается тот или иной способ аутентификации. Например, пользователю на рабочем месте в организации будет предложено ввести только пароль, а при удаленном доступе ему же будет предложена уже более сильная двухфакторная аутентификация. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Аутентификация

См. также: Двухфакторная аутентификация

Аутентификация на основе одноразовых паролей [One-Time Password authentication (OTP authentication)] —

Технология аутентификации с помощью одноразовых паролей, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства — токены, либо технология OOB (out of band), основанная на передаче одноразового пароля с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*

Выше: Аутентификация

См. также: Одноразовый пароль, Одноразовый пароль по дополнительному каналу

Аутентификация на основе сертификатов [Certificate-Based Authentication (CBA)] —

Аутентификация с использованием криптографических алгоритмов с открытым ключом, осуществляемая на основе имеющихся у пользователей сертификатов, выданных специальными уполномоченными организациями — удостоверяющими центрами. В этом случае нет необходимости хранить информацию о своих пользователях — они ее предоставляют сами в своих запросах в виде сертификатов, удостоверяющих личность пользователей. Данный вид аутентификации представляется естественным решением при большом количестве пользователей (может исчисляться миллионами). В таких обстоятельствах процедура предварительной регистрации пользователей,

связанная с назначением и хранением их паролей, становится крайне неудобной, а иногда и просто нереализуемой. При аутентификации на основе сертификатов задача хранения секретной информации (закрытых ключей) возлагается на самих пользователей, что делает это решение гораздо более масштабируемым, чем вариант с централизованной базой паролей. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*

Выше: Аутентификация

См. также: Удостоверяющий центр

Аутентификация отправителя данных [sender authentication] —

Подтверждение того, что отправитель полученных данных соответствует заявленному. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Аутентификация

См. также: Аутентификация источника данных, Аутентификация равноправного логического объекта, Услуга защиты

Аутентификация пользователя —

См. Аутентификация абонента (пользователя).

Аутентификация равноправного логического объекта —

Подтверждение того, что равноправный логический объект в какой-либо ассоциации является заявленным логическим объектом. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Аутентификация

См. также: Аутентификация отправителя данных, Услуга защиты

Аутентификация сообщения [message authentication] —

Проверка того, что сообщение было получено неповрежденным, неизмененным (с момента отправления), то есть проверка целостности. Если стороны доверяют друг другу, то аутентификация сообщения осуществляется применением системы имитозащиты. Для не доверяющих друг другу сторон необходимо использовать систему цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Аутентификация

См. также: Имитозащита, Система цифровой подписи

Аутентификация сторон [entity authentication] —

Проверка одной из сторон (или обеими сторонами) того, что взаимодействующая с ней сторона — именно та, за которую себя выдает. Если стороны доверяют друг другу, то аутентификацию сторон можно осуществить применением симметричной шифрсистемы (или системы имитозащиты), так как сообщение, правильно расшифрованное либо с верным значением кода аутентичности сообщения подтверждает знание отправителем их общего секретного ключа. Для не доверяющих друг другу сторон необходимо

использовать асимметричную шифрсистему (систему идентификации или систему цифровой подписи). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Аутентификация

Ниже: Взаимная аутентификация

См. также: Имитозащита, Система цифровой подписи, Односторонняя аутентификация

Аутентификация субъекта доступа —

Действия по проверке подлинности субъекта доступа в автоматизированной информационной системе. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Аутентификация

См. также: Субъект доступа (в автоматизированной информационной системе)

Аутентифицированный канал связи [authenticated communication channel] —

Канал связи, обеспечивающий целостность передаваемой по нему информации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Канал связи

См. также: Целостность информации

Аутентичность [authenticity] —

1. Свойство гарантирующее, что субъект или ресурс идентичны заявленным.

Примечание. Аутентичность применяется к таким субъектам, как пользователи, процессы, системы и информация. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Син.: Подлинность

Баг [Bug] —

1. (комп.) Баг (Software bug), ошибка в программе компьютерной, которая изначально была допущена при ее разработке, но обнаруживает себя спустя какое-то время в процессе работы программы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. (техн.) Жучок, миниатюрное прослушивающее устройство. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

3. Жаргонное слово, обычно обозначающее ошибку в программе или системе, которая выдает неожиданный или неправильный результат. Большинство багов возникают из-за ошибок, допущенных разработчиками программы в её исходном коде, либо в её дизайне. Также некоторые баги возникают из-за некорректной работы компилятора, вырабатывающего некорректный код. Термин «баг» обычно употребляется в отношении ошибок,

проявляющих себя на стадии работы программы, в отличие, например, от ошибок проектирования или синтаксических ошибок. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

База данных [database] —

1. Представленная в объективной форме совокупность самостоятельных материалов (статей, расчётов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ). *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

2. Собрание данных, организованных в соответствии с концептуальной структурой, описывающей характеристики этих данных и взаимоотношения между ними, причем такое собрание данных, которое поддерживает одну или более областей применения. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Информационная система

Базовые защитные меры [baseline controls] —

Минимальный набор защитных мер, установленный для системы или организации. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

См. также: Защитная мера

Базовый блочный алгоритм зашифрования [basic block encryption algorithm] —

См: Алгоритм блочного шифрования

Байт [byte] —

1. Последовательность, состоящая из некоторого числа бит, обрабатываемых как единый блок и обычно представляющая литеру или часть литеры.

Прим. 1: Число бит в байте фиксировано для конкретной системы обработки данных.

Прим. 2: Число бит в байте, обычно, равно 8-ми. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Единица представления данных в виде групп из 8 бит. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Данные, Бит

Банковская система Российской Федерации —

Банк России и кредитные организации, а также филиалы и представительства иностранных банков *[Федеральный закон от 02.12.1990 N 395-1-ФЗ “О банках и банковской деятельности” (в редакции Федерального*

закона от 3 февраля 1996 года N 17-ФЗ) (с изменениями на 5 мая 2014 года) (редакция, действующая с 6 мая 2014 года). Введен в действие: 02.12.1990].

Банковская тайна —

1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков. *[Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 N 14-ФЗ (с изменениями на 28 декабря 2013 года). Введен в действие 01.03.1996]*.

2. Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону. *[Федеральный закон от 02.12.1990 N 395-1-ФЗ "О банках и банковской деятельности" (в редакции Федерального закона от 3 февраля 1996 года N 17-ФЗ) (с изменениями на 5 мая 2014 года) (редакция, действующая с 6 мая 2014 года). Введен в действие: 02.12.1990]*.

Выше: Коммерческая тайна.

Банковский информационный технологический процесс —

Часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования организации банковской

системы Российской Федерации и не являющихся платежной информацией.

Примечания.

1. Платежная информация — информация, содержащаяся в документах, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой.

2. Неплатежная информация, необходимая для функционирования организации банковской системы Российской Федерации, может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Банковский технологический процесс

См. также: Банковская система Российской Федерации, Банковский платежный технологический процесс

Банковский технологический процесс —

Технологический процесс, реализующий операции по изменению и (или) определению состояния активов организации банковской системы Российской Федерации, используемых при функционировании или необходимых для реализации банковских услуг.

Примечания.

1. Операции над активами организации банковской системы Российской Федерации могут выполняться

вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем.

2. В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, бан-ковский информационный технологический процесс и др. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Банковский платежный технологический процесс, Банковский информационный технологический процесс

См. также: Автоматизированная банковская система, Информационный актив.

Банковский платежный технологический процесс —

Часть банковского технологического процесса, реализующая банковские операции над информационными активами организации банковской системы Российской Федерации, связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Банковский технологический процесс

См. также: Банковская система Российской Федерации, Банковский информационный технологический процесс

Банкомат [cash machine] —

1. Устройство для осуществления в автоматическом режиме (без участия уполномоченного лица кредитной организации или банковского платежного агента, субагента, осуществляющих деятельность в соответствии с законодательством о банках и банковской деятельности) наличных денежных расчетов и (или) расчетов с использованием платежных карт, передачи распоряжений кредитной организации об осуществлении расчетов по поручению физических лиц по их банковским счетам, а также для составления документов, подтверждающих передачу соответствующих распоряжений (абзац дополнительно включен с 1 января 2010 года Федеральным законом от 3 июня 2009 года N 121-ФЗ; дополнен с 29 сентября 2011 года Федеральным законом от 27 июня 2011 года N 162-ФЗ.) *[Федеральный закон от 22.05.2003 N 54-ФЗ*

"О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт" (ред. от 25.11.2013). Введен в действие: 27.06.2003].

2. Терминальное устройство электронной платежной банковской системы, позволяющее владельцу карточного банковского счета снимать с него деньги и вносить деньги в наличной форме, а также выполнять такие операции, как оплата товаров и услуг, получение документов, подтверждающих выполненные с его помощью операции. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009].*

Син.: Платежный терминал, Платежный терминал самообслуживания

См. также: Электронная платежная система

Безопасное состояние [secure state] —

Состояние системы, в котором выполнено одно из условий безопасности, например, ни один субъект не может получить доступ ни к какому объекту иначе как на основе проверки имеющихся у него полномочий. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/].*

Безопасность [security] —

1. Отсутствие недопустимого риска, связанного с возможностью нанесения ущерба. *[ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения. Введен в действие: 01.07.2003].*

2. Отсутствие недопустимого риска. *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003].*

3. Состояние защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)].*

4. Свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009].*

Ниже: Безопасность автоматизированной системы управления КВО, Безопасность информации (данных), Безопасность информации (при применении информационных технологий), Безопасность информационно-телекоммуникационных технологий (безопасность ИТТ), Безопасность информационной сети, Безопасность информационной технологии, Безопасность информационных ресурсов, Безопасность критической информационной инфраструктуры, Безопасность на основе открытости, Безопасность персональных данных, Безопасность связи, Безопасность сети электросвязи, Безопасность системы, Информационная безопасность, Компьютерная безопасность

См. также: Принципы обеспечения безопасности, Содержание деятельности по обеспечению безопасности, Управление безопасностью

Безопасность автоматизированной информационной системы —

Состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Безопасность системы

См. также: Безопасность информационных ресурсов, Система защиты информации автоматизированной системы

Безопасность автоматизированной системы управления КВО —

Состояние автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (далее - штатный режим функционирования) при проведении в отношении ее компьютерных атак. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

Выше: Безопасность

См. также: Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации

Безопасность информации (данных) [data security] —

1. Состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Состояние защищенности информации (данных), при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность. Примечание. Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

3. Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования,

блокирования и т.п. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №*60)].

4. Состояние защищенности информации (данных), обрабатываемой средствами вычислительной техники или автоматизированной системы, от угроз внутренних или внешних. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*. Выше: Безопасность

См. также: Информация, Данные, Конфиденциальность, Целостность, Доступность, Мониторинг безопасности информации, Показатель защищенности информации

Безопасность информации (при применении информационных технологий) —

Состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Безопасность

См. также: Информационные технологии, Безопасность автоматизированной информационной системы

Безопасность информационно-телекоммуникационных технологий (безопасность ИТТ) [ICT security] **—**

Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информационно-телекоммуникационных технологий. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Выше: Безопасность

См. также: Политика безопасности информационно-телекоммуникационных технологий (политика безопасности ИТТ)

Безопасность информационной сети —

Меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Выше: Безопасность

Син.: Сетевая безопасность.

См. также: Вторжение, Межсетевой экран (сетевой экран), Политика сетевой безопасности, Сетевой мониторинг

Безопасность информационной технологии [information technology security] —

1. Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Состояние защищенности информационной технологии, при котором обеспечивается выполнение изделием, реализующим информационную технологию, предписанных функций без нарушений безопасности обрабатываемой информации. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Безопасность

См. также: Информационные технологии, Безопасность информационной системы

Безопасность информационных ресурсов —

Состояние защищенности информационных ресурсов от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Безопасность, Негативные действия

Безопасность компьютерных систем [computer system security] —

См. Компьютерная безопасность.

Безопасность критической информационной инфраструктуры —

Состояние элементов критической информационной инфраструктуры и критической информационной инфраструктуры в целом, при котором проведение в отношении ее компьютерных атак не влечет за собой тяжких последствий. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

Выше: Безопасность

См. также: Критическая информационная инфраструктура Российской Федерации

Безопасность на основе открытости [open security] —

Деятельность, направленая на достижение безопасности приложений, основанная на философии и методологии использования программного

обеспечения с открытыми исходными кодами. Позволяет проводить независимую верификацию и тестирование исходных кодов, а также объединить усилия разработчиков на создании общих шаблонов и решений для различных технологий защиты. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Безопасность

См. также: Открытый код

Безопасность персональных данных [personal data protection] —

Обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона "О персональных данных". Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность персональных данных при их обработке в информационной системе. *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

Выше: Безопасность

См. также: Актуальные угрозы безопасности персональных данных, Система защиты персональных данных

Безопасность связи [communication security] —

1. Способность связи противостоять несанкционированному получению или изменению передаваемой информации. Безопасность связи включает обеспечение безопасности закрытой связи, безопасность радиопередач, обеспечение безопасности работы средств связи и электронного оборудования и обеспечение физической безопасности материалов и информации по вопросам безопасности связи. Обеспечение безопасности закрытой связи — компонент обеспечения безопасности связи, являющийся результатом наличия технически совершенных криптосистем и их правильного использования. Безопасность радиопередач — компонент обеспечения безопасности связи, являющийся результатом всех мер, направленных на защиту радиопередач от перехвата и использования в других целях, кроме криптоанализа. Обеспечение безопасности средств связи и электронного оборудования — компонент обеспечения безопасности связи, являющийся результатом всех мер, предпринимаемых с целью недопущения лиц, не имеющих на то разрешения, к ценной информации, которая может быть извлечена из перехвата и анализа

излучений шифровального оборудования и систем дальней связи. Физическая безопасность связи — компонент обеспечения безопасности связи, являющийся результатом физических мер, необходимых для защиты секретного оборудования, материалов и документов от доступа к ним или наблюдения за ними со стороны лиц, не имеющих на то разрешения. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*
2. Состояние защищенности связи с помощью совокупности специальных средств и методов, характеризующееся такими свойствами, как конфиденциальность, иммитостойкость, аутентификация, защита от анализа трафика, доступность, живучесть и др. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Безопасность

См. также: Анализ трафика, Криптографические средства физического и канального уровня, Межсетевой экран (сетевой экран), Оператор связи (электрической или почтовой), Политика безопасности оператора связи, Сетевая атака, Сетевые компьютерные операции, Система обеспечения безопасности сети связи общего пользования

Безопасность сети электросвязи —

Способность сети электросвязи противодействовать определенному множеству угроз, преднамеренных или непреднамеренных дестабилизирующих воздействий на входящие в состав сети средства, линии связи и технологические процессы (протоколы), что может привести к ухудшению качества услуг, предоставляемых сетью электросвязи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

Выше: Безопасность

См. также: Дестабилизирующее воздействие, Меры обеспечения безопасности, Механизм обеспечения безопасности сети электросвязи, Риск нарушения безопасности сети электросвязи, Угроза безопасности сети электросвязи, Уязвимость сети электросвязи, Устойчивость функционирования сети электросвязи

Безопасность системы [system security] —

Защищенность системы от несанкционированного использования ее ресурсов и функциональных возможностей, а также от возможных нарушений ее функционирования, вызванных различными предсказуемыми и непредсказуемыми обстоятельствами. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Выше: Безопасность

Ниже: Безопасность автоматизированной информационной системы

См. также: Ресурс (информационной системы)

Белая книга [white book] —

Базовый европейский стандарт, который определяет критерии, требования и процедуры для создания систем повышенной безопасности. Она же: ITSEC — Information Technology Security Evaluation Criteria. Стандарт имеет две различные схемы оценки: по эффективности (El-E6, E6 для самых защищенных систем) и по функциональности (F-Ш, F-AV, F-DI, F-DC, F-DX). Оценка по функциональности описывает доступность, целостность системы, целостность данных, их конфиденциальность и передачу данных. «Белая книга» разработана на основе «Зеленой книги» (Германия), а та в свою очередь, на основе «Оранжевой» и «Красной книг» (США) Стандарт дествовал с 1991 года и впоследствии был заменен международным стандартом ISO/IEC 15408-2005 «Критерии оценки безопасности информационных технологий». *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Биграмма [digram] —

Пара букв (символов), блоков текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Бизнес —

Экономическая деятельность, дающая прибыль; любой вид деятельности, приносящий доход, являющийся источником обогащения. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Бизнес-процесс

Бизнес-процесс —

Процессы, используемые в экономической деятельности организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Бизнес

Бинарный ключ [binary key] —

Ключ, заданный вектором с двоичными координатами. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Биометрическая аутентификация [bimetric authentication] —

Способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Аутентификация

Бит [bit] —

1. Любая из цифр 0 или 1, которые используются в двоичной системе. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Двоичная единица представления данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Данные, Байт

Блок данных [data block] —

Последовательность битов, имеющая фиксированную длину и используемая для представления данных в памяти или для их пересылки. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Блок текста, Данные

Блок текста [text block] —

Мулътиграмма текста (открытого текста, шифрованного текста или промежуточного), составленная из подряд идущих знаков. Обычно текст разбивается на блоки одинаковой длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Блок данных

Блокирование доступа (к информации) —

1. Прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей). *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.
2. Создание условий, препятствующих доступу к информации субъекту, имеющему право на него.
Примечание. Создание условий, препятствующих доступу к информации, может быть осуществлено по времени доступа, функциям по обработке информации (видам доступа) и (или) доступным информационным ресурсам. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Атака на отказ в обслуживании, Доступ к информации, Доступ к информации (ресурсам информационной системы)

Блокирование передачи информации (сообщения) —

Прекращение или задержка получения пользователем предназначенной для него достоверной информации (не измененных в процессе передачи сообщений) из технических средств передачи на время t* доп.,

Примечание - t* доп является одной из задаваемых качественных характеристик работы ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Блокирование персональных данных —

Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения

персональных данных). *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Выше: Обработка персональных данных

Блочная шифрсистема [block ciphering system] —

Система шифрования, в которой функция зашифрования реализуется блочным алгоритмом зашифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система шифрования

См. также: Алгоритм блочного шифрования

Бомбы с часовыми механизмами [time bombs] —

1. Файл - носитель, устанавливающий вирус в систему. Техника иногда используемая вирусописателями для "прикрытия" вирусов от антивирусных программ. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

2. Вредоносная программа, предназначенная для несанкционированной пользователем скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в теле этого типа троянцев.

Данный тип вредоносных программ обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве, неверной версии операционной системы и др.) сохраняют на диск жертвы (часто в каталог Windows, системный каталог Windows, временный каталог и т.д.) другие файлы и запускают их на выполнение.

В результате использования программ данного класса хакеры достигают двух целей:

- скрытной инсталляции троянских программ и вирусов;
- защиты от детектирования известных вредоносных программ антивирусами, поскольку не все из них в состоянии проверить все компоненты внутри подобных троянцев. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Компьютерный вирус

См. также: Антифрод системы

Бортовая ЭВМ —

Специализированная ЭВМ, предназначенная для установки на подвижном объекте. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]* .

Выше: Семейство ЭВМ

Бот [bot] —

1. Средство защиты информации, реализующее математический алгоритм преобразования информации, не использующее секретного ключа или передающее (хранящее) его с сообщением. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. (сокр. от робот) Специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь. При обсуждении компьютерных программ

термин употребляется в основном в применении к Интернету.*[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

3. Вредоносное программное обеспечение, поражающее компьютер и позволяющее осуществлять скрытое удаленное управление им. Бот может выполнять без ведома владельца компьютера такие действия как похищение данных, распространение спама, доставку и установку вредоносного обеспечения программного, участвовать в реализации DOS-атак. Боты играют ключевую роль в реализации современных целевых атак, известных как усиленные устойчивые угрозы (Advanced Persistent Threats (APTs)). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Антибот, Бот-сеть (ботнет)

Бот-сеть (ботнет) [botnet] —

Компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

См. также: Антибот, Бот, Конфикер, Карберп (троянская банковская программа)

Брешь безопасности [security flaw] —

См. Уязвимость (системы информационной).

Буткит [bootkit] —

Вредоносная программа (так называемая MBR-руткит), которая осуществляет модификацию загрузочного сектора MBR (Master Boot Record) — первого физического сектора на жёстком диске. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Вредоносное программное обеспечение

Буфер [buffer] —

Рабочая область памяти при пересылке данных.

Примечание. При операции ввода данные заносят в буферную область. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Бэкдоры [backdoors] —

См. Скрытые точки входа.

Важнейшая запись [vital record] —

Электронная или бумажная запись, которая необходима для сохранения, продолжения или восстановления деятельности организации и для защиты прав организации, ее служащих, клиентов и заинтересованных сторон. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-*

коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014].

Вакцинирование [vaccination] —

Обработка файлов, дисков, каталогов, проводимая с использованием специальных программ, создающих условия подобные тем, которые создаются определенным компьютерным вирусом и затрудняющих повторное его появление. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Введен в действие: 01.07.1999]*.

Ввод данных [data input] —

Операция чтения данных с носителя, запись этих данных в память данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Вывод данных

Веб-анонимайзер [web-anonymizer] —

Веб-сайт, предоставляющий услугу анонимайзера. Заходя на веб-сайт, пользователь вводит в адресную строку адрес веб-страницы, которую он желает посетить анонимно. Анонимайзер загружает эту страницу себе, обрабатывает ее и передает пользователю от своего имени (имени сервера-анонимайзера). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Ведение контрольных журналов [audit logging] —

Фиксирование данных о событиях, связанных с информационной безопасностью, в целях проверки, анализа и постоянного мониторинга. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Инструментальные средства аудита, Проверка безопасности, Сбор и корреляция событий безопасности, Мониторинг, Системный журнал

Ведомость применимости [statement of applicability] —

Документ, определяющий цели применения мер и средств контроля и управления и меры и средства контроля и управления, являющиеся адекватными и применимыми для СМИБ организации. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

Син.: Декларация о применимости, Положение о применимости

См. также: Цель применения мер и средств контроля и управления

Вектор инициализации [initialization vector] —

Вектор, который передается по каналу управления и используется для инициализации алгоритма шифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Синхропосылка

Верификация [verification] —

Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Ниже: Верификация и подтверждение правильности, Верификация программ

См. также: Верифицировать.

Верификация и подтверждение правильности [Verification and Validation (V&V)] —

Общий термин для обозначения полного набора проверок, которым подвергается система для получения гарантий ее соответствия своему назначению. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Выше: Верификация

См. также: Верифицировать

Верификация программ [program verification] —

Любой метод, который убеждает в том, что программа будет выполнять именно то, что от нее ожидается; доказательство того, что поведение программы соответствует спецификации на эту программу. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Выше: Верификация

См. также: Верифицировать

Верифицировать [verify] —

Провести строгую детальную проверку с независимым определением ее достаточности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Верификация

Вероятность (в области риск-менеджмента) [probability] —

Мера возможности наступления события, выраженная числом межу 0 и 1, где 0 - это невозможность и 1 - достоверность. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Возможность (в области риск-менеджмента), Правдоподобность появления (события) (в области риск-менеджмента), Событие

Вес булевой функции [weight of boolean function] —

Число двоичных наборов в табличном задании булевой функции, на которых функция принимает значение «1». *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ветвящаяся бомба [fork bomb] —

Вид атаки на отказ в обслуживании, при которой используется операция порождения параллельных процессов, с помощью которой работающие процессы порождают другие работающие процессы. Обычно при этом не осуществляется размножение и распространение, как это имеет место в случае вирусов или червей сетевых, а делается расчет на ограниченность числа одновременно выполняемых программ и процессов на одном компьютере. Этот тип самоповторяющихся программ иногда называют wabbit, bacteria или rabbit-программами. Поскольку каждый дочерний процесс занимает некоторый объем памяти и времени работы процессора, то работа системы замедляется, она перестает реагировать на события и ее использование становится невозможным *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Атака на отказ в обслуживании

Взаимная аутентификация [mutual authentication] —

Вариант аутентификации сторон, при котором каждая из сторон проверяет, что взаимодействующая с ней сторона — именно та, за которую себя выдает. Взаимная аутентификация реализуется таким протоколом идентификации, в котором каждый из участников является одновременно и доказывающим, и проверяющим. Это позволяет за один сеанс выполнения протокола каждым из участников доказать другому участнику свою идентичность. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Аутентификация сторон.

Взаимоувязанная сеть связи Российской Федерации —

Комплекс технологически сопряженных сетей электросвязи на территории Российской Федерации, обеспеченный общим централизованным управлением. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Информационная безопасность взаимоувязанной сети связи Российской Федерации, Сеть связи

Взламывание пароля [password cracking] —

Техника (способ) тайно получать доступ к системе (сети) информационной, в которой нападающая сторона с помощью вскрывателя паролей пробует угадать (подобрать) или украсть пароли. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Пароль

Виды вторжений —

Некоторыми видами вторжений являются: маскирование, воспроизведение, модификация сообщений, отклонение услуги, внутренние вторжения, внешние вторжения, «лазейка», «троянский конь» *[ГОСТ Р ИСО*

7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].

Ниже: Внутренние вторжения, Методы внешних вторжений, Лазейка, Маскирование, Отклонение услуги, Троянский конь

Виды механизмов защиты —

Некоторыми видами механизмов защиты являются: шифрование, аспекты административного управления ключами, механизмы цифровой подписи, механизмы управления доступом, механизмы целостности данных, механизмы обмена информацией аутентификации, механизмы заполнения трафика, механизм управления маршрутизацией, механизм нотаризации, физическая или персональная защита, надежное аппаратное/программное обеспечение. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ниже: Аппаратные средства защиты, Административное управление ключом, Заполнение трафика, Нотаризация (удостоверение подлинности), Управление доступом, Управление маршрутизацией, Физическая защита, Целостность данных, Цифровая подпись, Шифрование

Виды угроз [threat types] —

Угрозы могут классифицироваться на случайные и преднамеренные и могут быть активными и пассивными *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ниже: Преднамеренные угрозы, Случайные угрозы, Активная угроза, Пассивная угроза

Виды угроз информационной безопасности Российской Федерации —

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:
• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
• угрозы информационному обеспечению государственной политики Российской Федерации;
• угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
• угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. *[Доктрина информационной безопасности Российской Федерации*

(утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].

Ниже: Угрозы информационной безопасности в области науки и техники, Угрозы информационной безопасности в общегосударственных информационных и телекоммуникационных системах, Угрозы информационной безопасности в правоохранительной и судебной сферах, Угрозы информационной безопасности в сфере внешней политики, Угрозы информационной безопасности в сфере внутренней политики, Угрозы информационной безопасности в сфере духовной жизни, Угрозы информационной безопасности в сфере обороны, Угрозы информационной безопасности в сфере экономики, Угрозы информационной безопасности в условиях чрезвычайных ситуаций, Угрозы безопасности информационных и телекоммуникационных средств и систем, Угрозы информационному обеспечению государственной политики Российской Федерации, Угрозы развитию отечественной индустрии информатизации

См. также: Внешние источники угроз информационной безопасности Российской Федерации, Внутренние источники угроз информационной безопасности Российской Федерации, Угрозы информационной безопасности Российской Федерации

Виртуальная локальная вычислительная сеть [virtual local area network (VLAN)] —

Независимая сеть, созданная с логической точки зрения внутри физической сети. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012].*

Выше: Локальная вычислительная сеть

Виртуальная машина [virtual machine] —

Система обработки данных, появляющаяся как уникальный экземпляр, предназначенный для расположения у конкретного пользователя, но функциональные возможности которой достигаются путем разделения ее ресурсов с другими пользователями. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения].*

См. также: Система обработки данных

Виртуальная частная сеть [virtual private network (VPN)] —

Методология, технология и продукты обеспечения информационной безопасности в корпоративных сетях, функционирующих на принципах Интернет-технологий, путем построения защищенных подсетей (защищенных виртуальных сетей). Перевод термина VPN как: «виртуальные частные сети» не совсем корректен, правильнее переводить «виртуальные защищенные сети» *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001].*

Выше: Компьютерная сеть

См. также: Защищаемая сеть связи, Криптомаршрутизатор, Туннелирование

Виртуальные деньги [virtual money] —

Платежные средства, представляющие собой записи (в т. н. виртуальном бумажнике или персональном компьютере) о наличии условных единиц, приобретаемых заранее в качестве предоплаты конкретных услуг (телефонные карты, электронные жетоны и др.). Имеют заранее определенное назначение и ограниченное хождение. Обеспечивают возможность отслеживания транзакций. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Система (протокол) электронных платежей

Виртуальный [virtual] —

1. Применяется к чему-либо вторичному, что появляется из чего-либо первичного для того, чтобы получить

определенные характеристики, причем, вторичное служит суррогатом этого первичного. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Определение, характеризующее процесс или устройство в системе обработки информации кажущихся реально существующими, поскольку все их функции реализуются какими-либо другими средствами. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Вирус [virus] —

См. Компьютерный вирус.

Вишинг [vishing — voice phishing] —

Телефонный фишинг - вишинг назван так по аналогии с фишингом. Данная техника основана на использовании системы предварительно записанных голосовых сообщений, с целью воссоздать "официальные звонки" банковских и других IVR систем. Обычно, жертва получает запрос (чаще всего через фишинг электронной почты) связаться с банком и подтвердить или обновить какую-либо информацию. Система требует аутентификации пользователя, посредством ввода PIN-кода или пароля. Поэтому, предварительно записав ключевую фразу, можно выведать всю нужную информацию. Например, любой может записать типичную команду: "Нажмите единицу, чтобы сменить пароль. Нажмите двойку, чтобы получить ответ оператора" и воспроизвести ее вручную в нужный момент времени, создав впечатление работающей в данный момент системы предварительно записанных голосовых сообщений. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Вредоносное программное обеспечение, Социальная инженерия

См. также: Фишинг

Владелец информации [information owner] —

Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации. *[Лаборатория Сетевой*

Безопасности Your Private Network http://ypn.ru/102/introduction-to-information-protection-and-information-security/2/].

Син.: Собственник информации.

См. также: Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения, собственность.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения —

Субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Владелец информации

Владелец риска [risk owner] **—**

1. Лицо или организационная единица, которые имеют полномочия и несут ответственность за управление рисками. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Физическое лицо или сущность (логический объект), обладающие обязанностями и полномочиями для осуществления менеджмента риска и любой связанной с ним деятельности и обработки риска. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Менеджмент риска, Управление рисками

Владелец сайта в сети "Интернет" —

Лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети "Интернет", в том числе порядок размещения информации на таком сайте. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Владелец сертификата ключа проверки электронной подписи [owner of signature verification key certificate] **—**

Лицо, которому в установленном Федеральным законом от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

См. также: Сертификат ключа проверки электронной подписи, Пользователь сертификата ключа проверки электронной подписи

Внешние источники угроз информационной безопасности Российской Федерации —

Внешними источниками угроз безопасности информационной Российской Федерации являются:

• деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

• стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

• обострение международной конкуренции за обладание информационными технологиями и ресурсами;

• деятельность международных террористических организаций; увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

• деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

• разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним. [Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].

См. также: Внутренние источники угроз информационной безопасности Российской Федерации, Угрозы информационной безопасности Российской Федерации

Внешний воздействующий фактор —

Явление, процесс или среда, внешние по отношению к изделию или его составным частям, которые вызывают или могут вызвать ограничение или потерю работоспособного состояния изделия в процессе эксплуатации. *[ГОСТ 26883-86 (СТ СЭВ 5127-85) Внешние воздействующие факторы. Термины и определения. Введен в действие: 01.07.1987]*.

См. также: Внутренний воздействующий фактор

Внешний инцидент (или инцидент, имеющий внешний характер) —

Инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным образом. *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

Выше: Инцидент информационной безопасности

См. также: Внутренний инцидент (или инцидент, имеющий внутренний характер).

Внешний нарушитель [outside adversary] —

См. Противник

Внешний объект ИТ [external IT entity] —

Любые продукт или система ИТ, доверенные или нет, находящиеся вне объекта оценки и взаимодействующие с ним. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Внешняя сущность (для объекта оценки), Доверенный продукт ИТ, Объект оценки, Пользователь

Внешняя область применения (в области риск-менеджмента) [external context] —

Внешние условия, в которых организация работает и достигает своих целей.

Примечание - Внешняя область применения может включать в себя:

- внешнюю среду, связанную с культурной, социальной, политической, законодательной, регулирующей, экономической, природной или конкурентной сферой на международном, национальном, региональном или местном уровне;

- ключевые критерии и тенденции, которые могут воздействовать на достижение установленных целей организации;

- взаимоотношения с внешними причастными сторонами, восприятие ими риска и значимость для организации этих причастных сторон. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Внешняя ситуация (контекст) (в области риск-менеджмента)

См. также: Внутренняя область применения (в области риск-менеджмента), Установление области применения (в области риск-менеджмента)

Внешняя память [external storage] —

Память, данные в которой доступны центральному процессору посредством операции ввода-вывода. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Выше: Память

Внешняя ситуация (контекст) (в области риск-менеджмента) [external context] —

Внешняя среда, в которой организация стремится к достижению своих целей.

Примечание. Внешняя ситуация (контекст) может включать:

- культурную, социальную, правовую, регулирующую, финансовую, технологическую, экономическую, естественную и рыночную среду, на международном, национальном, региональном или на местном уровне;

-основные движущие силы и тенденции, влияющие на цели организации;

- взаимосвязи с заинтересованными сторонами, их ожидания и ценности. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Син.: Внешняя область применения (в области риск-менеджмента)

См. также: Внутренняя ситуация (контекст) (в области риск-менеджмента), Установление области применения (в области риск-менеджмента)

Внешняя сущность (для объекта оценки) [external entity] **—**

Человек или ИТ-сущность, взаимодействующие с объектом оценки из-за пределов границ объекта оценки.

Примечание — В качестве внешней сущности может также рассматриваться пользователь объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Внешний объект ИТ, Пользователь

Внутренние вторжения [inside intrusion] **—**

Происходят, когда уполномоченные пользователи системы ведут себя непреднамеренным или неполномочным способом *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды вторжений

Внутренние источники угроз информационной безопасности Российской Федерации —

Внутренними источниками угроз безопасности информационной Российской Федерации являются:

• критическое состояние отечественных отраслей промышленности;

• неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

• недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

• недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

• неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

• недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

• недостаточная экономическая мощь государства;

• снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

• недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

• отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Внешние источники угроз информационной безопасности Российской Федерации, Угрозы информационной безопасности Российской Федерации.

Внутренний воздействующий фактор —

Воздействие на информацию или ее носитель, приводящее к искажению, уничтожению, блокированию информации защищаемой и/или ее носителей при случайных ошибках владельца информации (субъекта доступа). *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Внешний воздействующий фактор

Внутренний инцидент (или инцидент, имеющий внутренний характер) —

Инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или другими способами). *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

Выше: Инцидент информационной безопасности

См. также: Внешний инцидент (или инцидент, имеющий внешний характер)

Внутренний нарушитель [inside adversary] **—**

См. Нарушитель.

Внутренняя область применения (в области риск-менеджмента) [external context] —

Внутренние условия, в которых организация работает и достигает своих целей.

Примечание - Внутренняя область применения может включать в себя:

- управление, организационную структуру, обязанности и подотчетность;
- политику, цели и задачи, а также стратегию их достижения;
- возможности организации с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (формальные и неформальные);
- взаимоотношения с внутренними причастными сторонами, восприятие ими риска и значимость для организации этих причастных сторон;
- культуру организации;
- стандарты, руководящие принципы и модели работы, принятые в организации;
- форму и объем договорных отношений. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Внутренняя ситуация (контекст) (в области риск менеджмента)

См. также: Внешняя область применения (в области риск-менеджмента), Установление области применения (в области риск-менеджмента).

Внутренняя ситуация (контекст) (в области риск менеджмента) [internal context] —

Внутренняя среда, в которой организация стремится к достижению своих целей.

Примечание. Внутренняя ситуация (контекст) может включать:

- руководство, организационную структуру, роли и ответственности;
- политики, цели и стратегии, доступные с точки зрения их достижения;
- возможности, понимаемые в отношении ресурсов и знания (например, капитал, время, люди, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);
- взаимосвязи с внутренними заинтересованными сторонами, их ожиданиями и ценностями;
- организационную культуру;
- стандарты, руководства и модели, принятые организацией;
- форму и содержание контрактных отношений.

[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].

Син.: Внутренняя область применения (в области риск-менеджмента).

См. также: Внешняя ситуация (контекст) (в области риск менеджмента), Установление области применения (в области риск-менеджмента).

Воздействие [impact] —

1. Неблагоприятное изменение уровня достигнутых бизнес-целей. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Результат нежелательного инцидента информационной безопасности. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Ниже: Дестабилизирующее воздействие, Информационно-психологическое воздействие, Информационно-техническое воздействие, Непреднамеренное воздействие на информацию, Несанкционированное воздействие на информацию, Преднамеренное силовое электромагнитное воздействие на информацию, Программное воздействие, Психологическое воздействие.

См. также: Инцидент информационной безопасности, Фактор, воздействующий на защищаемую информацию

Воздействие на риск [risk treatment] —

Процесс модификации (изменения) риска.

Примечание 1. Воздействие на риск может включать:

- избежание риска посредством решения не начинать или не продолжать деятельность, в результате которой возникает риск;
- принятие или увеличение риска для использования благоприятной возможности;
- устранение источника риска;
- изменение возможности;
- изменение последствий;
- разделение риска с другой стороной или сторонами (включая контракты и финансирование риска);
- осознанное удержание риска.

Примечание 2. Воздействие на риск, имеющий отрицательные последствия, иногда называют «смягчением риска», «устранением риска», «предупреждением риска» и «снижением риска».

*Примечание 3. В*оздействие на риск может создавать новые риски или изменять
существующие риски.

[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].

Ниже: Финансирование риска

См. также: Принятие риска

Возможность (в области риск-менеджмента) [likelihood] —

Шанс того, что что-то может произойти.

Примечание 1. В терминологии риск-менеджмента термин «возможность» означает шанс того, что что-то может произойти, независимо от того, задан ли он, измеряем или определен объективно или субъективно, качественно или количественно, и описывается ли с помощью общих понятий или математически (например, как вероятность или частота за данный период времени).

Примечание 2. Английский термин «likelihood» не имеет прямого перевода на некоторые языки: вместо этого, часто используется перевод слова «probability» (вероятность). Однако, в английском языке, вероятность (probability) часто понимают в узком математическом смысле. Поэтому в терминологии риск-менеджмента термин «likelihood» используется с той целью, чтобы придать ему настолько же широкий смысл, какой имеет слово «вероятность» во многих языках, кроме английского. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

Син.: Правдоподобность появления (события) (в области риск-менеджмента).

См. также: Вероятность (в области риск-менеджмента), Событие.

Восприятие риска [risk perception] —

Представления заинтересованных сторон о риске. Примечание. Восприятие риска отражает потребности, проблемы, знание, доверие и ценности заинтересованных сторон. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

Восстановление [recovering] —

Событие, заключающееся в том, что после неисправности объект снова становится способным выполнять требуемую функцию. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].*

Ниже: Восстановление (защитных мер обеспечения ИБ ИТС), Восстановление ИКТ после бедствия.

Восстановление (защитных мер обеспечения ИБ ИТС) —

Процесс перевода защитных мер обеспечения информационной безопасности информационно-телекоммуникационных систем в штатное состояние после восстановления деятельности организации при условии наличия (новой) карты рисков информационной безопасности деятельности организации.

Примечание. Восстановление включает идентификацию карты рисков

информационной безопасности деятельности организации, настройку или замену защитных мер информационной безопасности, регулирование и контроль состояния защитных мер информационной безопасности, контроль работоспособности объекта и его рисков информационной безопасности, имеющего указанные защитные меры информационной безопасности. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009]*.

Выше: Восстановление

Восстановление данных [data recovering] —

Действия по воссозданию данных, которые были утеряны или изменены в результате несанкционированных воздействий. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Восстановление ИКТ после бедствия [ICT disaster recovery] —

Способность элементов ИКТ организации поддерживать ее критические функции бизнеса на приемлемом уровне в течение определенного периода времени после нарушения. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

Выше: Восстановление

См. также: Заданная точка восстановления (ЗТВ), Заданное время восстановления (ЗВВ), Нарушение, План восстановления ИКТ после бедствия

Врачебная тайна —

Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении. *[Федеральный закон от 21.11.2011 N 323-ФЗ " Об основах охраны здоровья граждан в Российской Федерации" (с изменениями на 28 декабря 2013 года). Введен в действие: 22.11.2011]*.

Выше: Профессиональная тайна

Вредоносная программа —

См. Вредоносное программное обеспечение.

Вредоносное программное обеспечение [malware, malicious software] —

1. Программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо к ухудшению параметров функционирования абонентского терминала или сети связи. *[Постановление Правительства РФ от 10.09.2007 N 575 "Об утверждении Правил оказания телематических услуг связи" (ред. от 16.02.2008). Вступило в силу 01.08.2008]*.

2.Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на

информацию или ресурсы информационной системы. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

3. Любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

4. К вредоносному программному обеспечению относятся сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие какой-либо вред компьютеру, на котором они запускаются, или другим компьютерам в сети. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

5. Программа, скрытно устанавливаемая на компьютер и выполняющая некоторые операции без разрешения пользователя. Может выступать в форме исполняемого кода, скриптов, активного контента и др. Для скрытой установки могут использоваться троянские программы, эксплойты, социальная инженерия (провоцируется запуск вредоносной программы самим пользователем), маскировка под другого субъекта (spoofing) и др. В процессе функционирования может использовать такие технологии, как размножение (вирус), распространение («червь»), отложенная активация (логическая «бомба»), сокрытие следов (руткит), полиморфизм, реализовать функции живучести (создание «неубиваемых» процессов), самозащиты (противодействие антивирусным программам), а также выполнять скрытную несанкционированную загрузку и установку программного обеспечения (обновлений, дополнений, модулей расширения или иного программного обеспечения). Целью устанавливаемого вредоносного программного обеспечения может быть мониторинг информации о работе сети (sniffer), сбор и передача информации о работе системы (spyware), модификация системных настроек (hijacking), создание помех в работе, вплоть до полной блокировки процессов и уничтожения данных (teardrop attacks), установка скрытых точек входа (backdoors, trapdoors), сбор и передача личной информации пользователя (паролей, номеров банковских карт) (crimeware), блокировка доступа с целью выкупа (ransomware), получение доступа, использование дорогостоящего ресурса, скрытое удаленное управление и создание bot-сети, а также нежелательная реклама и рассылка спама, накрутка результатов голосования, скрытое неосознанное воздействие на человека и др. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Ниже: Буткит, Вишинг, Дифейсмент, Кейлоггер, Люки, Руткит, Скрытые точки входа, Троянская программа.

Син.: Вредоносная программа, Вредоносное программное средство.

См. также: Атака, Изменение настроек браузера, Интернет-мошенничество, Преступное/мошенническое программное обеспечение, Социальная инженерия, Шпионское программное обеспечение, Потенциально нежелательные программы

Вредоносное программное средство [malware] —

Вредоносное программное средство, специально разработанное для повреждения или разрушения системы посредством нарушения ее конфиденциальности, целостности и (или) доступности.

Примечание. Примерами вредоносного программного средства являются вирусы и "троянские кони". *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Син.: Вредоносное программное обеспечение

См. также: Компьютерный вирус

Временная метка [timestamp] —

Информация о времени создания сообщения (электронного документа), добавляемая к этому сообщению (документу) с целью ее использования при проверке и подтверждении целостности документа. Временная метка должна обладать свойствами, напоминающими свойства цифровой подписи: невозможность подмены (в т. ч. перенесения на другой электронный документ), невозможность изменения даты и (или) времени и т. д. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Электронный документ, Центр установки меток (временных)

Временная сложность алгоритма [time complexity] —

Функция, выражающая зависимость числа элементарных операций, производимых при работе алгоритма, от длины записи исходных данных. Обычно рассматривается временная сложность алгоритма в худшем случае, то есть максимальное значение временной сложности по всем исходным данным одинаковой длины. Рассматривается также временная сложность алгоритма в среднем, то есть среднее значение временной сложности при случайном выборе исходных данных одинаковой длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Емкостная сложность алгоритма, Коммуникационная сложность (протокола), Практическая стойкость (криптосистемы)

Время жизни ключа [key life period, key life time] —

Временной интервал цикла жизненного ключа от генерации до уничтожения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Жизненный цикл ключей

Вскрыватель паролей [password cracker] —

Компьютерная программа, которая осуществляет подбор или похищение паролей. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*.

Вспомогательные технические средства и системы (ВТСС) —

Технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях.

К ним относятся:

· различного рода телефонные средства и системы;

· средства и системы передачи данных в системе радиосвязи;

· средства и системы охранной и пожарной сигнализации;

· средства и системы оповещения и сигнализации;

· контрольно-измерительная аппаратура;

· средства и системы кондиционирования;

· средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.д.);

· средства электронной оргтехники;

· средства и системы электрочасофикации;

· иные технические средства и системы. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

См. также: Защищаемые помещения, Основные технические средства и системы (ОТСС)

Встраиваемые криптографические средства [build-in cryptographic mechanisms] **—**

Криптографические средства, внешние по отношению к операционной системе, но зависящие от нее. К ним относятся различные интерфейсы прикладного программирования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографические средства

Вторжение [intrusion] **—**

1. Несанкционированный доступ к сети или подсоединенной к сети системе, т.е. преднамеренный или случайный несанкционированный доступ к информационной системе, включая злонамеренную деятельность против информационной системы или несанкционированное использование ресурсов в информационной системе. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Неправомочный доступ или проникновение любого рода (физическое или информационное) в компьютеры, информационные системы и сети непосредственно или опосредованно через корреспондирующие сети или системы. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

Ниже: Вторжение (в автоматизированную информационную систему)

См. также: Виды вторжений, Преднамеренные угрозы, Система обнаружения вторжения, Обнаружение вторжений, Предотвращение вторжений

Вторжение (в автоматизированную информационную систему) —

Выявленный факт попытки несанкционированного доступа к ресурсам автоматизированной информационной системы. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Вторжение

См. также: Несанкционированный доступ

Входить в систему [logon, login] —

Ввод идентификационных данных и, возможно, аутентификационных данных в систему обработки данных, чтобы можно было работать с данными. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Аутентификационные данные, Единая авторизация, Идентификационные данные, Выходить из системы

Выборочная подделка цифровой подписи [selective forgery] —

Подделка цифровой подписи, при которой противник и/или нарушитель, не владеющий секретным ключом, выбирает сообщение (отсюда название угрозы), и затем, получив открытый ключ, подделывает цифровую подпись для этого сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Подделка цифровой подписи

См. также: Универсальная подделка цифровой подписи, Экзистенциальная подделка цифровой подписи

Вывод данных [data output] —

Операция чтения данных в памяти данных и по следующая их запись на носитель данных или отображение на экране. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Ввод данных

Выводы аудита информационной безопасности —

Результат оценки собранных свидетельств аудита безопасности информационной *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Син.: Выводы (наблюдения) аудита

См. также: Свидетельства (доказательства) аудита информационной безопасности организации, Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям

Выводы (наблюдения) аудита [audit findings] —

1. Результаты оценки собранных свидетельств аудита на соответствие критериям аудита.

Примечания:

1. Выводы аудита указывают на соответствие или несоответствие.

2. Выводы аудита могут вести к идентификации возможностей для улучшения или отражению наилучших практик.

3. Если критерии аудита выбираются, исходя из правовых или других обязательных требований, то наблюдением (выводом) аудита определяется соответствие или несоответствие данным требованиям. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

Син.: Выводы аудита информационной безопасности

См. также: Свидетельства (доказательства) аудита информационной безопасности организации, Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям

Выделенное помещение —

Специальное помещение, предназначенное для регулярного проведения собраний, совещаний, бесед и других мероприятий секретного характера. *[ОСТ В1 00464-82 Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. Введен в действие: 01.01.1998]*.

См. также: Защищаемые помещения

Выходить из системы [logoff, logout] —

Выполнять последовательность операций, необходимых для завершения сеанса работы или для принудительного отсоединения от системы обработки данных. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Входить в систему

Вычислительная машина — [computer]

Совокупность технических средств, создающая возможность проведения обработки информации и получение результата в необходимой форме.

Примечание. Как правило, в состав ВМ входит и системное программное обеспечение. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Электронная вычислительная машина (ЭВМ)

Вычислительная сеть —

См. Компьютерная сеть.

Гамма (шифра) [keystream, ciphering sequence, key sequence] —

1. Псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

2. Управляющая последовательность знаков (блоков) алфавита, используемая в поточных шифрсистемах, реализующих гаммирование. Для обеспечения криптографической стойкости гамма должна удовлетворять ряду требований, в частности, быть близкой по своим свойствам к реализации

идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Управляющая последовательность

См. также: Гаммирование, Идеальная случайная последовательность, Ключевая последовательность, Перекрытие гаммы

Гаммирование [running key ciphering, one-time padding] —

1. Процесс наложения по определенному закону гаммы шифра на открытые данные. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

См. также: Гамма, Латинский квадрат

2. Шифрование, в котором функция зашифрования f(y ,x) обратима по каждой переменной (y обозначает знак (блок) гаммы шифра, x — знак (блок) текста открытого, значение функции f(y,x) — знак (блок) текста шифрованного). Важным частным случаем является так называемое модульное гаммирование, когда f(y ,x) = x+y(mod N), где N — размер числового алфавита {0, 1,..., N-1}, из которого выбираются y и x. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Гамма (шифра), Шифр гаммирования

Гарантии [assurance] —

См. Доверие

Генератор ключей [key generator] —

Техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), ключевой последовательности, векторов инициализации и т.п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Генератор псевдослучайных подстановок [pseudorandom permutation generator] —

Генератор псевдослучайных функций из семейства, в котором каждая функция является подстановкой. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Генератор псевдослучайных функций

Генератор псевдослучайных функций [pseudorandom function generator] —

Алгоритм, который псевдослучайным образом выбирает функцию из заданного семейства псевдослучайных функций. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Генератор псевдослучайных подстановок, Семейство псевдослучайных функций

Генератор функций с секретом [trapdoor function generator] —

См. Функция с секретом.

Гибкость организации (в области риск-менеджмента) [resilience] —

Способность организации к адаптации в сложной и изменчивой окружающей среде. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Син.: Устойчивость организации (в области риск-менеджмента)

Главный ключ [master key] —

Элемент составного ключа, который используется для шифрования ключей, предназначенных для шифрования разовых ключей или для генерации других видов ключей посредством шифрования определенных данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Иерархия ключей, Разовый ключ

Глубина анализа скрытого канала —

Степень варьирования применяемых средств по сложности для идентификации скрытого канала и его характеристик. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Идентификация скрытого канала, Скрытый канал

Государственная политика обеспечения информационной безопасности Российской Федерации —

Политика, определяющая основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей и ответственности за защищенность интересов Российской Федерации в информационной сфере в рамках закрепленных за ними направлений деятельности, базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Система обеспечения информационной безопасности Российской Федерации

Государственная тайна —

Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Примечание. Отнесение информации к государственной тайне осуществляется в соответствии с Законом «О государственной тайне». *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21*

декабря 2013 года). Введен в действие: 21.09.1993], [ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000].

См. также: Допуск к государственной тайне, Отнесение сведений к государственной тайне и их засекречивание, Перечень сведений, составляющих государственную тайну, Сведения, не подлежащие отнесению к государственной тайне и засекречиванию, Система защиты государственной тайны, Разглашение государственной тайны.

Готовность ИКТ к обеспечению непрерывности бизнеса (ГИКТОНБ) [ICT readiness for business continuity - IRBC] —

Способность организации поддерживать свои операции бизнеса путем предупреждения, обнаружения, реагирования на нарушения и восстановления услуг ИКТ. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: Восстановление ИКТ после бедствия, Нарушение, План восстановления ИКТ после бедствия.

Готовность системы [system availability] —

Мера способности системы выполнять свои функции при нахождении в рабочем состоянии. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Гриф ограничения доступа к документу —

Реквизит, свидетельствующий об особом характере документа и ограничивающий доступ к нему. *[ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения. Введен в действие: 01.03.2014]*.

См. также: Реквизит документа, Гриф секретности

Гриф секретности —

Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него. *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Гриф ограничения доступа к документу, Носитель сведений, составляющих государственную тайну, Реквизит документа, Сведения особой важности, Секретные сведения, Совершенно секретные сведения, Степень секретности сведений, составляющих государственную тайну

Группа по аудиту [audit team] —

Один или несколько аудиторов, проводящих аудит, при необходимости поддерживаемые техническими экспертами.

Примечания:

1. Один из аудиторов в группе по аудиту, как правило, назначается руководителем группы.

2. Группа по аудиту может включать в себя аудиторов-стажеров. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Аудитор, Наблюдатель, Сопровождающий, Технический эксперт

Группа реагирования на инциденты информационной безопасности (ГРИИБ) [Information Security Incident Response Team (ISIRT)] —

Группа обученных и доверенных членов организации.

Примечание. Данная группа обрабатывает инциденты ИБ во время их жизненного цикла и иногда может дополняться внешними экспертами, например, из общепризнанной группы реагирования на компьютерные инциденты или компьютерной группы быстрого реагирования (КГБР). [*ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Введен в действие: 01.07.2008]*.

См. также: Инцидент информационной безопасности, Реагирование на инцидент.

Групповая цифровая подпись **[group digital signature]** —

Цифровая подпись, сформированная с использованием групповой схемы цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Цифровая подпись.

См. также: Схема групповой цифровой подписи.

Групповой протокол [group-oriented protocol] —

Криптографический протокол, в котором какой-либо алгоритм, требующий знания секретного ключа, является распределенным. Например, в протоколе групповой подписи подписывающий заменяется группой участников таким образом, что корректная подпись может быть сформирована только при участии всех членов группы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический протокол

Групповой протокол подписи [group signature protocol] —

Описание алгоритма формирования цифровой подписи, предполагающего одновременное участие заранее определенной группы участников. В случае отсутствия хотя бы одного участника из группы формирование подписи невозможно. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Алгоритм формирования цифровой подписи.

Данные [data] —

1. Представление информации в некотором формализованном виде, пригодном для передачи, интерпретации или обработки.

Примечание: данные могут обрабатываться людьми или автоматическими средствами. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

3. Сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их проявления, отображенные на материальном носителе, используемые в целях сохранения знаний. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Ниже: Данные пользователя, Данные трассировки защиты.

См. также: Байт, Бит, Информация.

Данные пользователя [user data] —

Данные для пользователя, не влияющие на выполнение функциональных возможностей безопасности объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

Выше: Данные

См. также: Функциональные возможности безопасности объекта оценки

Данные трассировки защиты —

Накопленные и готовые к использованию данные, предназначенные для детализации причины анализа процедур защиты. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Данные

См. также: Анализ процедур защиты

Двусторонний протокол [two-party protocol] —

Протокол с двумя участниками. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*

Выше: Протокол

Двухфакторная аутентификация [two-factor authentication] —

Аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*

Выше: Аутентификация

См. также: Многофакторная аутентификация

Декларация о применимости [statement of applicability] —

Документированное заявление, описывающее цели и механизмы контроля, которые имеют отношение и применимы к СУИБ организации.

Примечание. Цели и механизмы контроля базируются на результатах и выводах, полученных в процессе оценки рисков и обработки рисков,

законодательных требованиях и требованиях нормативной базы, договорных обязательствах и бизнес-требованиях организации к информационной безопасности. *[BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements Дата принятия: 14.10.2005 Перевод: ООО «GlobalTrust Solutions»].*

Син. Ведомость применимости, Положение о применимости

Декларирование соответствия —

Форма подтверждения соответствия продукции требованиям технических регламентов. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003].*

См. также: Технический регламент, Сертификат соответствия

Демилитаризованная зона (ДМЗ) [demilitarized zone; DMZ] **—**

Пограничный сегмент сети (также известный как защищенная подсеть), выполняющий функции "нейтральной зоны" между сетями. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012].*

Демонстрируемое соответствие [demonstrable conformance] **—**

Связь между заданием безопасности и профилем защиты, при которой задание безопасности обеспечивает решение общей проблемы безопасности, определенной в профиле защиты.

Примечание — профиль защиты и задание безопасности могут содержать совершенно разные утверждения, относящиеся к разным сущностям, использующие разные понятия и т.д. Демонстрируемое соответствие также является подходящим для типа объекта оценки, для которого уже существует несколько сходных профилей защиты, позволяя разработчику задания безопасности утверждать о соответствии одновременно всем этим профилям защиты и, таким образом экономить трудозатраты. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].*

См. также: Задание по безопасности, Профиль защиты

Депонирование ключей [key escrow] **—**

Хранение копии ключа криптосистемы у доверенного лица (организации, участника протокола и т. п.) с целью восстановления работоспособности криптосистемы, например, в случае утери ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

См. также: Стандарт шифрования с депонированием ключей EES

Дестабилизирующее воздействие —

Действие, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети электросвязи характера, приводящее к выходу из строя элементов сети. *[ГОСТ*

Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007].

Выше: Воздействие

См. также: Безопасность сети электросвязи

Дешифрование [decryption, breaking of cryptosystem] —

1. Процесс, обратный соответствующему обратимому процессу шифрования. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Процесс аналитического раскрытия противником и/или нарушителем сообщения открытого без предварительного полного знания всех элементов системы криптографической. Если этот процесс поддается математической формализации, говорят об алгоритме дешифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Алгоритм расшифрования, Шифрование

Диалоговый режим [conversational mode] —

Режим взаимодействия человека с системой обработки информации, при котором человек и система обмениваются информацией в темпе, который соизмерим с темпом обработки информации человеком. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Интерактивный режим, Режим пакетной обработки, Режим разделения времени, Режим реального времени, Система обработки информации

Динамический анализ исходных текстов программ —

Совокупность методов контроля (не) соответствия реализованных и декларированных в документации функциональных возможностей программного обеспечения, основанных на идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)]*.

См. также: Статический анализ исходных текстов программ

Директива 1999/93/ЕС [Directive 1999/93/EC] —

Директива 1999/93/ЕС Европейского парламента и Совета от 13 декабря 1999 г. о порядке использования электронных подписей в Европейском Сообществе. Является основным исходным документом для стран Евросоюза в области нормативного регулирования и стандартизации вопросов применения электронной подписи. Главная цель Директивы — унификация правил использования электронной подписи и наиболее общая формулировка условий, необходимых для признания юридической равнозначности электронной и

собственноручной подписей. На основе анализа законов, принятых в различных странах мира, в Директиве были закреплены наиболее существенные моменты. Они сформулированы в ст.5 Директивы: необходимо использовать усиленную электронную подпись, которая должна быть основана на квалифицированном сертификате и сформирована с помощью защищенного устройства создания подписи. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Электронная подпись

Директива о приватности [data protection Directive 95/46/EC] —

Директива 95/46/ЕС один из важнейших документов информационного права Европейского сообщества, регламентирующий вопросы правового режима обмена персональными данными с организациями и лицами внутри ЕС и с таковыми в третьих странах, то есть странах, не подпадающих под юрисдикцию ЕС, в частности, США. Директива о приватности разрабатывалась и принималась в контексте гражданско-правового законодательства ЕС (Community Law), называемого также «первым столпом» европейского сотрудничества. В этом же духе рассматривались и задачи определения условий правового режима обмена персональными данными с организациями и лицами в третьих странах. Общий принцип регулирования таков: передача данных персональных запрещается, если законодательство третьей страны не обеспечивает их «адекватной защиты», эквивалентной высоким стандартам, установленным Директивой 95/46. Директива о приватности была изначально ориентирована на экономическую сферу и не регулирует вопросы передачи данных в третьи страны в контексте европейского сотрудничества — сотрудничества в сфере сдерживания преступности. До настоящего времени каждое европейское ведомство в этой сфере пока действует по собственным стандартам, организуя самостоятельно сбор и хранение данных, обмен ими с третьими странами. В 1998 году в Еврокомиссии создана Рабочая группа «Информационные системы и защита данных», призванная довести стандарты защиты персональных данных при сотрудничестве в рамках «третьего столпа» до уровня, адекватного уровню, предусмотренному Директивой 95/46. Активное участие в этом процессе принимает — Комитет по гражданским правам и свободам, юстиции и внутренним делам ЕС. Ранее Директива 95/46 подпадала под сферу интересов только Комитета по правовым вопросам и внутреннему рынку ЕС. С февраля 2000 года в Брюсселе состоялись слушания в Европарламенте по теме «ЕС и защита данных», на которых вопросы регулирования правовой защиты персональных данных рассматривались в числе одного из иных вопросов. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

См. также: Персональные данные

Дискретизационный принцип контроля доступа [discretionary access control] —

Контроль доступа, реализуемый путем контроля комплексом средств защиты доступа именованных субъектов (пользователей) к именованным

объектам (например, файлам, программам, томам). Для каждой пары (субъект — объект) в средстве вычислительной тезники должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (например, читать, писать). Контроль доступа должен быть применим к каждому объекту и к каждому субъекту. *[ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Введен в действие: 01.01.1996]*.

См. также: Дискреционное управление доступом, Мандатный принцип контроля доступа, Матрица доступа

Дискретный —

1. Применяется к данным, которые состоят из различимых элементов, таких как литеры или применяется к физическим количественным характеристикам, имеющим конечное число значений или значений, четко отличаемых друг от друга, а также применяется к процессам и функциональным блокам, в которых используются такие данные. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Определение, относящееся к данным, представленным отдельными элементами, например, знаками или физическими величинами, принимающими конечное число вполне определенных значений. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Дискреционное управление доступом [discretionary access control] —

Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*

Выше: Управление доступом

См. также: Дискретизационный принцип управления доступом, Мандатное управление доступом, Матрица доступа

Диспетчер доступа [security kernel] —

Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*

Син.: Ядро защиты

См. также: Концепция диспетчера доступа, Комплекс средств защиты

Дистанционное управление компонентами межсетевого экрана —

Выполнение функций по сопровождению МЭ (компоненты) администратором МЭ с узла (рабочей станции) сети, на котором не функционирует МЭ (компонента) с использованием сетевых протоколов.

[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)].

См. также: Администратор межсетевого экрана, Локальное (местное) управление компонентами межсетевого экрана, Централизованное управление компонентами межсетевого экрана.

Дифейсмент [defacement] —

Искажение веб-страниц. Вид компьютерного вандализма, иногда являющийся для хакера забавой, а иногда средством выражения политических пристрастий. Искажения могут производиться в какой-то части сайта или выражаться в полной замене существующих на сайте страниц (чаще всего, стартовой). *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

Выше: Вредоносное прогрпммное обеспечение, Сетевая атака, Интернет-мошенничество

Дифференциальная атака [differential attack] —

См. Разностная атака

Дифференциально-линейная атака [differential-linear attack] —

См. Разностно-линейная атака

Дифференциальный метод [differential cryptanalysis] —

См. Разностный метод

Длина (размер) ключа [key length] —

Длина слова в определенном алфавите, представляющего ключ. Длина бинарного ключа измеряется в битах. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Доверенная функциональность [trusted functionality] —

Функционирование, которое воспринимается правильным с точки зрения некоторого критерия, например, критерия, представляемого посредством стратегии защиты. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Стратегия защиты

Доверенный ИТ продукт [trusted IT product] —

Продукт ИТ, отличный от объекта оценки, для которого имеются свои функциональные требования, организационно скоординированные с объектом оценки, и который, как предполагается, реализует свои функциональные требования корректно.

Примечание. Примером доверенного продукта ИТ является продукт, который был отдельно оценен. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Внешний объект ИТ, Объект оценки, Доверенный канал

Доверенный канал [trusted channel] —

Средство взаимодействия между функциональными возможностями безопасности объекта оценки и удаленным доверенным продуктом ИТ, обеспечивающее необходимую для этого степень уверенности в безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Доверенный продукт ИТ, Объект оценки

Доверенный (достоверный) маршрут [trusted path] —

Средство взаимодействия между пользователем и функциональными возможностями безопасности объекта оценки, обеспечивающее необходимую для этого степень уверенности в безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Функциональные возможности безопасности объекта оценки

Доверие [assurance] —

1. Основание для уверенности в том, что объект оценки отвечает конкретным функциональным требованиям безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Основание для уверенности в том, что объект соответствует целям безопасности. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

3. Основание для уверенности в том, что сущность отвечает своим целям безопасности. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

Син.: Гарантии

См. также: Цель безопасности

Доказательство знания [proof of knowledge] —

Интерактивное доказательство, при котором доказывающий убеждает проверяющего в том, что он владеет секретной информацией, не раскрывая ее. Доказательство знания характеризуется двумя свойствами: полнотой (протокола) и корректностью (протокола). К категории доказательства знания относятся протоколы идентификации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Интерактивное доказательство

Ниже: Доказательство с нулевым разглашением

См. также: Полнота (протокола), Протокол идентификации

Доказательство с нулевым разглашением [zero-knowledge proof] —

Доказательство знания, которое обладает свойством нулевого разглашения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Доказательство знания

Ниже: Идентификация с нулевым разглашением, Не интерактивное доказательство с нулевым разглашением, Совершенное доказательство с нулевым разглашением

См. также: Нулевое разглашение

Доказуемая стойкость [provable security] —

См. Криптографическая стойкость, Теоретическая стойкость (криптосистемы).

Доктрина информационной безопасности Российской Федерации —

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения безопасности информационной Российской Федерации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Документ [document] —

1. Зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать. *[ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения. Введен в действие: 01.03.2014]*.

2. Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Примечание. Под материальным носителем подразумевается изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т. п. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Конфиденциальный документ, Подлинный документ, Электронный документ

Син.: Документированная информация

См. также: Документация, Реквизит документа

Документ сертификации [certification document] —

Документ, указывающий, что СМИБ организации-клиента соответствует стандартам СМИБ и дополнительной документации, требуемой в рамках этой системы. *[ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введен в действие: 01.10.2009]*.

См. также: Сертификат, Орган сертификации

Документация —

Совокупность взаимосвязанных документов, объединенных общей целевой направленностью. [Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)].

См. также: Документ, Информационная база автоматизированной системы

Документированная информация —

Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Выше: Информация

Син.: Документ

См. также: Компьютерная информация, Цифровая информация, Носитель документированной информации

Долговременный ключ [long-term key] —

Элемент составных ключей, действующий в неизменном виде длительное время. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Иерархия ключей, Разовый ключ

Доля секрета [share, secret share] —

Ключевая информация, получаемая отдельным участником схемы разделения секрета, позволяющая ему вместе с другими участниками правомочной коалиции восстановить значение секрета. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.
См. также: Структура доступа, Схема разделения секрета

Домен безопасности [security domain] —

Совокупность активов и ресурсов, подчиняющихся единой политике безопасности. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Политика сетевой безопасности, Шлюз безопасности

Доменное имя —

Обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет". *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

См. также: Сайт в сети “Интернет”, Сетевой адрес

Дополнение [appendix] —

Строка бит, формируемая из цифровой подписи и произвольного текстового поля. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Подписанное сообщение

Допуск к государственной тайне —

Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций — на проведение работ с использованием таких сведений. Примечание. Допуск должностных лиц и граждан к государственной тайне предусматривает:

• принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;

• согласие на частичные, временные ограничения их прав в соответствии со статьей 24 Закона Российской Федерации от 21.07.93 № 5485-1 в редакции Федерального закона Российской Федерации от 06.10.97 г. № 131-ФЗ «О государственной тайне»;

• письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;

• определение видов, размеров и порядка предоставления льгот, предусмотренных Законом Российской Федерации от 21.07.93 г. № 5485-1 в редакции Федерального закона Российской Федерации от 06.10.97 г. № 131-ФЗ «О государственной тайне»;

• ознакомление с нормами законодательства Российской Федерации о государственной тайне, предусматривающими ответственность за его нарушение;

• принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну. Льготы для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе;

• процентные надбавки к заработной плате в зависимости от степени секретности сведений, к которым они имеют доступ;

• преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий. Для сотрудников структурных подразделений по защите государственной тайны дополнительно к льготам, установленным для должностных лиц и граждан, допущенных к государственной тайне на постоянной основе, устанавливается процентная надбавка к заработной плате за стаж работы в указанных структурных подразделениях. Устанавливаются три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: сведения особой важности, совершенно секретные или

секретные. *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Государственная тайна, Доступ к сведениям, составляющим государственную тайну, Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.

Допустимый риск [risk tolerance] **—**

1. Риск, который организация и причастные стороны готовы сохранять после обработки риска для достижения своих целей.

Примечание.

1. Допустимость риска связана с законодательными и обязательными требованиями. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

2. Риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]*.

Выше: Риск

См. также: Определение приемлемости уровня риска, Допустимый риск нарушения информационной безопасности.

Допустимый риск нарушения информационной безопасности —

Риск нарушения информационной безопасности, предполагаемый ущерб от которого организация банковской системы Российской Федерации в данное время и в данной ситуации готова принять. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Риск нарушения информационной безопасности

См. также: Допустимый риск

Дорожное яблоко —

1. Этот метод атаки представляет собой адаптацию троянского коня и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD или флэш в месте, где носитель может быть легко найден (туалет, лифт, парковка). Носитель подделывается под официальный и сопровождается подписью, призванной вызвать любопытство. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*

2. Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник подбрасывает «инфицированные» носители информации в местах общего доступа, где эти носители могут быть легко найдены, такими как туалеты, парковки, столовые, или на рабочем месте атакуемого сотрудника. Носители оформляются как официальные для компании, которую атакуют, или сопровождаются подписью, призванной вызвать любопытство. К примеру, злоумышленник может подбросить CD, снабжённый корпоративным логотипом и ссылкой на официальный сайт компании, снабдив его надписью «Заработная плата руководящего состава». Диск может быть оставлен на полу лифта или в

вестибюле. Сотрудник по незнанию может подобрать диск и вставить его в компьютер, чтобы удовлетворить своё любопытство. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Социальная инженерия

Достоверная вычислительная база [Trusted Computing Base (TCB)] —

Совокупность защитных механизмов вычислительной системы, включая программные и аппаратные компоненты, ответственные за поддержание политики безопасности. Достоверная вычислительная база состоит из одной или нескольких компонентов, которые вместе отвечают за реализацию единой политики безопасности в рамках системы. Способность достоверной вычислительной базы корректно проводить единую политику безопасности зависит в первую очередь от механизмов самой достоверной вычислительной базы, а так же от корректного управления со стороны администрации системы. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Политика безопасности информации

Достоверность [reliability] —

Свойство соответствия предусмотренному поведению и результатам. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Ниже: Достоверность (информации, данных)

Достоверность (информации, данных) [validity, adequacy] —

Свойство информации быть правильно воспринятой, вероятность отсутствия ошибок; степень соответствия данных, хранимых в памяти ЭВМ или документах, реальному состоянию отображаемых ими объектов предметной области. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Выше: Достоверность

Доступ [access] —

1. Средства доступа к ресурсу, возможность или разрешение иметь доступ к нему, возможность или разрешение обращаться к ресурсу или использовать его. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Извлечение информации из памяти средства вычислительной техники (электронно-вычислительной машины) или помещение информации в память средства вычислительной техники (электронно-вычислительной машины). *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Ниже: Доступ (в автоматизированной информационной системе), Доступ к информации, Доступ к информации (ресурсам информационной системы),

Доступ к информации, составляющей коммерческую тайну, Доступ к конфиденциальной информации, Доступ к сведениям, составляющим государственную тайну, Доступ с собственного устройства, Коллективный (групповой) доступ, Ограниченный доступ, Несанкционированный доступ, Санкционированный доступ к информации

См. также: Контроль доступа, Механизм (средство) разграничения доступа, Управление доступом, Права доступа, Рубежи защиты информации, Список доступа

Доступ (в автоматизированной информационной системе) —

Получение возможности ознакомления с информацией, ее обработки и (или) воздействия на информацию и (или) ресурсы автоматизированной информационной системы с использованием программных и (или) технических средств.

Примечание. Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Доступ

См. также: Объект доступа (в автоматизированной информационной системе)

Доступ к информации [access to information] **—**

1. Возможность получения информации и ее использования. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

2. Получение субъектом возможности ознакомления с информацией, в том числе с помощью технических средств. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

3. Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Выше: Доступ

См. также: Обработка информации, Модификация информации, Уничтожение информации

Доступ к информации (ресурсам информационной системы) —

Получение возможности ознакомления с информацией, обработки информации и (или) воздействия на информацию и (или) ресурсы информационной системы с использованием программных и (или) технических

средств. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Доступ

См. также: Обработка информации, Модификация информации, Уничтожение информации.

Доступ к информации, составляющей коммерческую тайну —

Ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации. *[Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]*.

Выше: Доступ

См. также: Информация, составляющая коммерческую тайну (секрет производства), Коммерческая тайна, Режим коммерческой тайны.

Доступ к конфиденциальной информации —

Санкционированное полномочным должностным лицом ознакомление конкретного лица с информацией, содержащей сведения конфиденциального характера. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Выше: Доступ

См. также: Сведения конфиденциального характера

Доступ к сведениям, составляющим государственную тайну —

Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну. *[Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

Выше: Доступ

См. также: Допуск к государственной тайне, Носитель сведений, составляющих государственную тайну

Доступ с собственного устройства [Bring Your Own Device (BYOD)] —

Тенденция, заключающаяся в предоставлении сотрудникам доступа к ресурсам организации с любых мобильных устройств, включая собственные (ноутбуки, планшеты, смартфоны и т. п.). В целях обеспечения безопасности информационных ресурсов корпоративной сети предполагает использование детализированного набора усиленных политик безопасности, учитывающих не только идентификационные данные каждого пользователя и его статус, но и вид и степень защищенности подключаемого мобильного устройства, место, с которого пользователь подключается к сети. С учетом этих факторов предлагается способ безопасного подключения к сети: по Wi-Fi из офиса, удаленно через VPN и др. Основными технологиями, применяемыми в рамках BYOD, являются: управление мобильными устройствами (MDM), распознавание мобильных устройств и их операционных систем, автоматическая рассылка и проверка установленных обновлений и антивирусных средств, шифрование сохраняемых данных на устройстве для

защиты от утери или кражи мобильного устройства, контроль приложений с использованием сценария, запрет по умолчанию и др. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Доступ

См. также: Управление мобильными устройствами

Доступность [availability] —

1. Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

3. Свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ниже: Доступность информационных активов, Доступность информации

См. также: Информационная безопасность, Конфиденциальность, Целостность

Доступность информации [information availability] —

1. Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно.

Примечание. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

2. Обеспечение возможности получения доступа к информации для пользователя в нужное для него время. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Выше: Доступность

См. также: Конфиденциальность информации, Целостность информации

Доступность информационных активов [accessibility, availability] —

Свойство информационной безопасности организации банковской системы Российской Федерации, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте,

необходимых пользователю, и в то время, когда они ему необходимы. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*

Выше: Доступность

См. также: Информационный актив, Конфиденциальность информационных активов, Целостность информационных активов.

Драйвер [driver] —

Программа, предназначенная для управления работой периферийных устройств, обычно в мини- и микроЭВМ. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Дроп —

Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества; обозначает участника, который с целью обналичивания снимает деньги в банкомате с подставного счета, предварительно переведенные на этот счет с одного из «буферных» счетов. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Интернет-мошенничество, Дроповод-нальщик, Заливщик, Кардселлер, Кодер (программист), Поставщик трафика

Дроповод-нальщик —

Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества; обозначает участника, который управляет «дропами», снимающими деньги в банкоматах, организуя процесс разбиения общей суммы на более мелкие и снятия денег с «буферных» счетов с целью их обналичивания. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Интернет-мошенничество, Дроп, Заливщик, Кардселлер, Кодер (программист), Поставщик трафика

Дроппер [dropper] —

1. Файл - носитель, устанавливающий вирус в систему. Техника иногда используемая вирусописателями для "прикрытия" вирусов от антивирусных программ. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

2. Вредоносная программа, предназначенная для несанкционированной пользователем скрытой инсталляции на компьютер-жертву вредоносных программ, содержащихся в теле этого типа троянцев.

Данный тип вредоносных программ обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве, неверной версии операционной системы и др.) сохраняют на диск жертвы (часто в каталог Windows, системный каталог Windows, временный каталог и т.д.) другие файлы и запускают их на выполнение.

В результате использования программ данного класса хакеры достигают двух целей:

- скрытной инсталляции троянских программ и вирусов;

- защиты от детектирования известных вредоносных программ антивирусами, поскольку не все из них в состоянии проверить все компоненты внутри подобных троянцев. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Компьютерный вирус

См. также: Антифрод системы, Троянская программа

Единая авторизация [Single Sign-On (SSO)] —

Технология единого входа и авторизации, при которой пользователь для получения доступа в течение одного сеанса сразу к нескольким приложениям или нескольким разделам портала должен ввести имя/пароль только однократно. Процесс авторизации использует одну учетную запись и предоставляет доступ сразу ко всем приложениям, к которым у пользователя имеется право доступа, без повторной аутентификации и автоматически прекращает доступ, если пользователь в течение одного сеанса переключается от одного ресурса к другому. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Авторизация

Син.: Однократный вход.

См. также: Входить в систему, Учетная запись

Единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов —

Централизованная, иерархическая, территориально распределенная структура, включающая силы и средства обнаружения и предупреждения компьютерных атак, а также органы управления различных уровней, в полномочия которых входят вопросы обеспечения безопасности автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

Ниже: Силы обнаружения и предупреждения компьютерных атак, Средства обнаружения и предупреждения компьютерных атак

Единая система идентификации и аутентификации —

Федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Емкостная сложность алгоритма [space complexity] —

Функция, выражающая зависимость числа ячеек памяти, используемых в работе алгоритма, от длины записи исходных данных. Обычно рассматривается с. а. е. в худшем случае, то есть максимальное значение емкостной сложности по всем исходным данным одинаковой длины. Рассматривается также с. а. е. в среднем, то есть среднее значение сложности емкостной при случайном выборе исходных данных одинаковой длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Временная сложность алгоритма, Коммуникационная сложность (протокола), Практическая стойкость (криптосистемы)

Живучесть [viability] —

Свойство системы оставаться работоспособной в условиях внешних воздействий. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

См. также: Живучесть программного изделия, Отказоустойчивая система

Живучесть программного изделия [program viability] —

Показатель качества программного изделия, характеризующий его способность сохранять нормальное функционирование при машинных сбоях или частичном выходе оборудования из строя. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

См. также: Живучесть

Жизненный цикл [life-cycle] —

Последовательность стадий существования обьекта (например некоторого продукта или системы) во времени. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

Ниже: Жизненный цикл ключей

Жизненный цикл ключей [key lifetime] —

Последовательность стадий, которые проходят ключи от момента генерации до момента уничтожения. Включает такие основные стадии, как: генерация, регистрация ключей (и пользователей), инициализация, период действия, хранение, смена, архивирование, уничтожение и восстановление. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Жизненный цикл

Журналистская тайна —

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне.

Редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом.

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего и его законного представителя.

Редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, прямо или косвенно указывающие на личность несовершеннолетнего, признанного потерпевшим, без согласия самого несовершеннолетнего и (или) его законного представителя. *[Закон РФ от 27.12.1991 N 2124-1 "О средствах массовой информации" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.02.1992]*.

Выше: Профессиональная тайна

Заверение (подлинности) [notarization] —

См. Нотаризация

Зависимость [dependency] —

Соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено, чтобы и другие требования могли отвечать своим целям. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Требование безопасности (объекта оценки), Элемент

Загрузка в память [load] —

Пересылка данных между различными уровнями памяти данных с целью непосредственного их использования в операциях центрального процессора. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]***.**

Загрузочный вирус [boot virus] —

Компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера. При включении или перезагрузке компьютера Boot-вирус заменяет собой загрузочный код, и таким образом получает управление ещё до непосредственного запуска операционной системы. Вместо операционной системы загружается вирус, размещая в памяти свое тело, которое хранит в неиспользованных секторах, идущих после MBR, но до первого загрузочного сектора раздела. Перехватив обращения к дискам, вирус продолжает загрузку операционной системы. Размножается вирус записью в загрузочную область других накопителей компьютера. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Компьютерный вирус

Задание по безопасности [security target] —

1. Зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта оценки. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Демонстрируемое соответствие, Профиль защиты, Требование безопасности (объекта оценки)

Заданная точка восстановления (ЗТВ) [recovery point objective - RPO] —

Момент времени, к которому должны быть восстановлены данные после произошедшего нарушения. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: Восстановление ИКТ после бедствия, Заданное время восстановления (ЗВВ), Нарушение, План восстановления ИКТ после бедствия

Заданное время восстановления (ЗВВ) [recovery time objective - RTO] —

Период времени после произошедшего нарушения, в течение которого должны быть восстановлены минимальные уровни услуг и (или) продукты, а также поддерживающие системы, прикладные программы или функции. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: Восстановление ИКТ после бедствия, Заданная точка восстановления (ЗТВ), Нарушение, План восстановления ИКТ после бедствия

Задача дискретного логарифмирования [discrete logarithm problem] —

Задача нахождения дискретного логарифма в конечной группе. В последние десятилетия интерес к задаче дискретного логарифмирования существенно усилился в связи с синтезом асимметричных шифрсистем. Разработан ряд алгоритмов логарифмирования в мультипликативных группах конечных полей и других конечных группах. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Задача факторизации целых чисел [integer factoring problem] —

Задача разложения целого положительного числа в произведение простых чисел. Задача факторизации целых чисел является классической математической задачей. В последние десятилетия интерес к ней существенно усилился в связи с синтезом асимметричных шифрсистем. Разработан ряд алгоритмов факторизации целых чисел. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Заинтересованная сторона [stakeholder] **—**

Лицо или организация, которые могут воздействовать, или на которые могут воздействовать, или которые считают, что на них влияет какое-либо решение или деятельность.

Примечание. Лицо, принимающее решения, может быть заинтересованной стороной.

[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]

Син.: Причастная сторона

См. также Третья сторона

Заказчик аудита [audit client] **—**

Организация или лицо, заказавшие аудит.

Примечание. В случае внутреннего аудита заказчиком аудита может быть проверяемая организация или лицо, ответственное за управление программой аудита. Запросы, касающиеся проведения внешнего аудита, могут поступать из таких источников, как контролирующие органы, стороны, с которыми организация имеет контрактные отношения, или потенциальные заказчики. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Аудиторская проверка информационной безопасности в организации, Проверяемая организация

Закладочное устройство —

1. Техническое средство (устройство) приема, передачи и обработки информации, преднамеренно устанавливаемое на объекте информатизации или в контролируемой зоне в целях перехвата информации или несанкционированного воздействия на информацию и (или) ресурсы автоматизированной информационной системы.

Примечание. Местами установки закладочных средств (устройств) на охраняемой территории могут быть любые элементы контролируемой зоны, например: ограждение, конструкции, оборудование, предметы интерьера, транспортные средства. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

2. Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации). *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

См. также: Аппаратная закладка, Специальная проверка, Средство поиска закладочных устройств.

Заключение по результатам аудита информационной безопасности (аудиторское заключение) —

Качественная или количественная оценка соответствия установленным критериям аудита информационной безопасности, представленная аудиторской группой после рассмотрения всех выводов аудита информационной безопасности в соответствии с целями аудита информационной безопасности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Критерий аудита информационной безопасности организации, Свидетельства (доказательства) аудита информационной безопасности организации, Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям

Законный пользователь [legal user] —

Официально зарегистрированный в системе пользователь. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Незарегистрированный пользователь, Пользователь автоматизированной системы

Закрытый ключ [private key] —

Сохраняемый в тайне компонент ключевой пары, применяющейся в асимметричных шифрах, т. е. таких шифрах, в которых для прямого и обратного преобразований используются разные ключи. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык]*.

Выше: Ключ

Син.: Личный ключ, Секретный ключ

См. также: Открытый ключ

Закрытый стандарт [proprietary standard] —

Стандарт, обычно разработанный и используемый какой-либо организацией либо индустриальной компанией, выпускающей, например, средства программного обеспечения или технические средства. Спецификация такого стандарта является собственностью этой компании и не обязательно публикуется для широкого доступа. В отличие от открытых стандартов, сфера применения закрытых стандартов ограничена, их поддерживает ограниченный круг специалистов. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Выше: Стандарт

Син.: Частный стандарт

См. также: Открытый стандарт

Заливщик —

Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества; обозначает участника, который скрытно с помощью предварительно установленной вредоносной программы управляет компьютером потерпевшего и производит платеж от его имени. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Интернет-мошенничество, Дроп, Дроповод-нальщик, Кардселлер, Кодер (программист), Поставщик трафика

Замысел защиты информации —

Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Организационно-технические мероприятия по защите информации, Цель защиты информации.

Заполнение трафика —

Генерация фиктивных сеансов обмена данными, фиктивных блоков данных и/или фиктивных данных в составе блоков данных *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды механизмов защиты

Ниже: Механизм (средство) заполнения трафика

Запоминающее устройство [storage unit] —

Устройство, реализующее функцию памяти данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Память данных

Зашифрование данных —

Процесс преобразования открытых данных в зашифрованные при помощи шифра. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

См. также: Алгоритм зашифрования, Расшифрование, Расшифровка данных,

Защита [protection, security, lock out] —

Термин «защита» используется в смысле минимизации уязвимости средств и ресурсов. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ниже: Защита данных, Защита и контроль информации, Защита информации, Защита компьютерной системы, Защита от несанкционированного доступа (Защита от НСД), Защита объекта, Защита программных средств

Защита данных [data protection] —

1. Применение административных, технических или физических мер борьбы с несанкционированным доступом к данным. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Система мер и средств, обеспечивающих предотвращение неавторизованного доступа к данным. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

3. Охрана данных от несанкционированного, умышленного или случайного их раскрытия, модификации или уничтожения. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Защита

См. также: Носитель данных, Криптографическая защита

Защита и контроль информации [Information Protection and Control (IPC)] —

Решения класса IPC предназначены для защиты информации от внутренних угроз и предотвращения различных видов утечек. Как правило IPC включает шифрование носителей информации, контроль технических каналов утечки с помощью технологий (DLP), анализ входящих и архивирование исходящих потоков информации. Применение шифрования позволяет обеспечить защиту в случае, когда физический носитель информации попадает в руки инсайдера или лиц, не имеющих легального доступа. Анализ входящего и исходящего трафика позволяет избежать утечки информации, а также осуществить защиту от вирусов и спама. Ведение архивов способствует эффективному расследованию происшествий и предотвращению возможных утечек в будущем. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Защита

См. также: Система предотвращения утечек

Защита информации [protection of information] —

1. Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. [*Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

3. Совокупность методов, средств и мероприятий, обеспечивающих целостность, конфиденциальность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера, реализация которых может привести к нанесению ущерба владельцам или пользователям информации. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Выше: Защита.

Ниже: Защита информации от (иностранной) разведки, Защита информации от непреднамеренного воздействия, Защита информации от несанкционированного воздействия (ЗИ от НСВ), Защита информации от несанкционированного доступа (ЗИ от НСД), Защита информации от преднамеренного воздействия, Защита информации от разглашения, Защита информации от утечки, Комплексная защита информации, Техническая защита информации, Правовая защита информации, Физическая (непосредственная) защита информации, Организационная защита информации.

См. также: Защищаемая информация, Концепция защиты информации, Криптографическая защита информации, Мероприятие по защите информации, Методы защиты информации, Носитель информации, Система защиты информации, Способ защиты информации, Способы действий по защите информации.

Защита информации от (иностранной) разведки —

Защита информации, направленная на предотвращение получения (иностранной) разведкой защищаемой информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации

См. также: Защищаемая информация

Защита информации от непреднамеренного воздействия —

Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации

См. также: Защищаемая информация, Непреднамеренное воздействие, Носитель защищаемой информации

Защита информации от несанкционированного воздействия (ЗИ от НСВ) —

Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации

См. также: Защищаемая информация, Несанкционированное воздействие на информацию, Носитель защищаемой информации, Средство защиты информации от несанкционированного воздействия.

Защита информации от несанкционированного доступа (ЗИ от НСД) [protection from unauthorized access] —

1. Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание. Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Предотвращение или существенное затруднение несанкционированного доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Выше: Защита информации, Защита от несанкционированного доступа (Защита от НСД).

См. также: Защищаемая информация, Несанкционированный доступ к информации, Носитель защищаемой информации, Система защиты информации от несанкционированного доступа.

Защита информации от преднамеренного воздействия —

Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного воздействия, и (или) воздействия различной физической природы, осуществляемого в террористических или криминальных целях. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации

См. также: Защищаемая информация, Носитель защищаемой информации, Преднамеренное силовое электромагнитное воздействие на информацию.

Защита информации от разглашения —

Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации

См. также: Разглашение информации

Защита информации от утечки —

Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами. Примечание. Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации

См. также: Утечка информации

Защита компьютерной системы —

Предохранение компьютерной системы и ее данных от повреждения или потери. Главная цель защиты компьютерной системы, особенно в системах, которые доступны многим пользователям через линии связи — предотвращение несанкционированного использования системы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Защита

См. также: Компьютерная система

Защита объекта —

Проведение комплекса мероприятий по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, носитель информации, информационный процесс. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Защита

См. также: Защищаемая информация, Носитель защищаемой информации, Несанкционированное воздействие на информацию, Непреднамеренное воздействие, Утечка информации

Защита от несанкционированного доступа (Защита от НСД) [protection from unauthorized access] **—**

Предотвращение или существенное затруднение несанкционированного доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Ниже: Защита информации от несанкционированного доступа (ЗИ от НСД)

См. также: Комплекс средств защиты, Несанкционированный доступ, Система разграничения доступа, Средства защиты от несанкционированного доступа

Защита программных средств —

Организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих

действий. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Введен в действие: 01.07.1999]*.

Выше: Защита

См. также: Защищаемые программные средства, Несанкционированный доступ к программным средствам.

Защитная мера [safeguard] **—**

1. Сложившаяся практика, процедура или механизм обработки риска. Примечание. Следует заметить, что понятие «защитная мера» может считаться синонимом понятию «контроль». *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Мера, используемая для уменьшения риска. *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]*.

3. Сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения безопасности информационной организации банковской системы Российской Федерации. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Син.: Мера безопасности, Мера обеспечения безопасности

См. также: Базовые защитные меры

Защищаемая автоматизированная информационная система —

Автоматизированная информационная система, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Автоматизированная информационная система

См. также: Защищаемая информационная система, Защищаемая информация

Защищаемая информационная система —

Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Информационная система

См. также: Защищаемая автоматизированная информационная система, Защищаемая информация

Защищаемая информационная технология —

Информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности. *[Р 50.1.053-2005 Информационные технологии.*

Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006].

Выше: Информационная технология

См. также: Защищаемая информация, Защищаемый процесс (информационной технологии)

Защищаемая информация —

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Примечание. Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008].*

См. также: Защита информации, Категорирование защищаемой информации, Носитель защищаемой информации, Собственник информации, Фактор, воздействующий на защищаемую информацию

Защищаемая сеть связи —

Сеть связи, используемая при обмене защищаемой информацией с требуемым уровнем ее защищенности. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006].*

Выше: Сеть связи

См. также: Защита информации, Виртуальная частная сеть

Защищаемые информационные ресурсы (автоматизированной информационной системы) —

1. Информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищенности.

Примечание. Информационные ресурсы включают в себя документы и массивы документов, используемые в автоматизированных информационных системах. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006].*

Выше: Защищаемые ресурсы (информационной системы)

Защищаемые помещения —

Помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.). *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»].*

См. также: Выделенное помещение

Защищаемые программные средства —

Программные средства, используемые в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности.

[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006].

См. также: Защита программных средств, Защищаемая информация

Защищаемые ресурсы (информационной системы) —

Ресурсы, использующиеся в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Ресурс (информационной системы)

Ниже: Защищаемые информационные ресурсы (автоматизированной информационной системы)

См. также: Защищаемая информация

Защищаемый объект информатизации [target of protection] —

Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Объект информатизации

См. также: Защищаемая информация

Защищаемый процесс (информационной технологии) —

Процесс, используемый в информационной технологии для обработки защищаемой информации с требуемым уровнем ее защищенности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Защищаемая информационная технология, Защищаемая информация

Защищенная автоматизированная система [protected automated system] —

Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Выше: Автоматизированная система

См. также: Комплекс средств защиты

Защищенная операционная система [secure operating system] —

1. Операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АСТРАСТ, 2009]*.

2. Операционная система, прошедшая аттестацию по определенному оценочному уровню доверия. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Операционная система

См. также: Оценочный уровень доверия

Защищенное устройство создания подписи [secure signature creation device, SSCD] —

Устройство создания электронной подписи, т. е. сконфигурированное программное или аппаратное устройство создания подписи, которое удовлетворяет требованиям, сформулированным в приложении III Директивы 1999/93/ЕС. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Процесс формирования подписи

Защищенность информации —

Соответствие эффективности защиты информации требованиям нормативных документов. *[ОСТ В1 00464-82 Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. Введен в действие: 01.01.1998]*.

См. также: Эффективность защиты информации, Показатель защищенности информации

Защищенность информационной сферы Взаимоувязанной сети связи Российской Федерации —

Способность ВСС РФ к недопущению, либо обнаружению и ликвидации определенной угрозы информационной безопасности ВСС РФ с заданным уровнем качества служб информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Информационная безопасность взаимоувязанной сети связи Российской Федерации, Информационная сфера взаимоувязанной сети связи Российской Федерации, Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации

Защищенность объекта защиты —

Способность объекта защиты противостоять иностранным техническим разведкам и предотвращать утечку информации о нем по техническим каналам. *[ОСТ В1 00464-82 Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. Введен в действие: 01.01.1998]*.

См. также: Защита информации от (иностранной) разведки, Объект защиты информации, Утечка информации

Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники —

Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники характеризуется тем, что

только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к чтению, записи, созданию или уничтожению информации. Защищенность обеспечивается тремя группами требований к средствам защиты, реализуемым в средствах вычислительной техники:

• требования к разграничению доступа, предусматривающие то, что средства вычислительной техники должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;
• требования к учету, предусматривающие то, что средства вычислительной техники должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

• требования к гарантиям, предусматривающие необходимость наличия в составе средств вычислительной техники технических и программных механизмов, позволяющих получить гарантии того, что средства вычислительной техники обеспечивают выполнение требований к разграничению доступа и к учету. *[ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Введен в действие: 01.01.1996]*.

См. также: Защищенность средств вычислительной техники, Защищенные средства вычислительной техники, Несанкционированный доступ к информации, Обработка информации, Разграничение доступа

Защищенность средств вычислительной техники —

Защищенность средств вычислительной техники есть потенциальная защищенность, то есть свойство предотвращать или существенно затруднять несанкционированный доступ к информации в дальнейшем при использовании средств вычислительной техники в автоматизированной системе. *[Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники, Защищенные средства вычислительной техники, Показатель защищенности средств вычислительной техники

Защищенные средства вычислительной техники —

Средства вычислительной техники общего и специального назначения, защищенные от утечки, искажения или уничтожения информации за счет несанкционированного доступа. *[Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники, Защищенность средств вычислительной техники, Сертификат защиты

Защищенный канал связи [private communication channel] —

Канал связи, обеспечивающий недоступность пересылаемой по нему информации пассивному противнику. Защищенный канал связи моделируется протоколом конфиденциальной передачи сообщений. Для других типов криптографических протоколов защищенный канал связи может служить криптографическим примитивом. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Канал связи

Зевс (троянская банковская программа) [Zeus, ZBot] —

1. Троянская программа нового типа, появившаяся в 2007 году, и предназначенная для атаки серверов и перехвата данных. Ущерб от данного троянского коня был огромный. Разработана группой украинских хакеров. ZeuS был написан на Visual C++. Предназначен для всех версий Windows, и из-за своей структуры, позволяющей работать без подключения программы к драйверам - может заразить компьютер даже из гостевой учётной записи.

После того, как произошло заражение, троянская программа внедряется в систему и перехватывает ваши регистрационные данные. Получив ваши данные, программа переводит деньги на счета других зараженных небольшую сумму денег, тем самым, делая невозможным найти счет взломщика.

Некоторые версии ZeuS маскируются цифровой подписью Лаборатории Касперского. После внимательного изучения этой подписи были выявлены некоторые различия, в связи с чем подпись была признана подделкой. Помимо версий для Windows существует ещё 5 разновидностей вируса для мобильных устройств. Они направлены на устройства с операционной системой BlackBerry и Android. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

2. Троянские программы семейства ZBot (ZeuS) появились в 2007 году. Благодаря простоте конфигурации и удобству использования для кражи веб-данных, ZeuS стал одной из самых распространяемых и продаваемых программ-шпионов на черном рынке интернета.

Вот беглое описание того, что делает эта программа, попав в систему жертвы:

1. Все, что вы «запоминаете» на компьютере (например, ставя галочку «Сохранить пароль»), становится доступным и для троянца, будь то логины, пароли или какие-то другие данные, например, для автозаполнения полей на веб-страничках.

2. Даже если вы ничего не отмечали для запоминания, троянец следит за тем, какие клавиши вы нажимаете, и введенная последовательность символов, которая дает допуск к вашим деньгам, будет «подсмотрена» и отправлена злоумышленникам.

3. Чтобы избежать «подсматривания» вводимых с клавиатуры данных, на сайтах зачастую используется такой инструмент, как виртуальная клавиатура. При вводе пароля вы щелкаете левой кнопкой мыши по клавишам клавиатуры, которая отображается на экране монитора. В этом случае ZeuS включает другой механизм перехвата данных пользователя: как только вы нажимаете левую кнопку мыши, ZeuS запоминает картинку — область экрана вокруг курсора, — так что злоумышленник будет знать, какие клавиши вы выбирали на экране мышкой.

4. ZeuS контролирует все данные, проходящие через ваш браузер. Если вы попытаетесь открыть веб-страницу, адрес которой присутствует в файле конфигурации ZeuS, троянец может изменить скачанный код страницы до того, как вы увидите ее в окне браузера. Как правило, изменение представляет собой добавление новых полей для ввода личных и секретных данных. Ну попросил у вас банк (а вы же уверены, что находитесь на сайте банка), кроме пользовательского пароля, ввести еще и ваш пин-код для карты — отчего не ввести? Но это уловка мошенника! Запрос пин-кода добавил ZeuS, а в изначальном коде странички банка такого запроса не было! Введенный пин-код троянец перехватывает и отправляет своему хозяину.

5. Некоторые сайты, когда вы регистрируетесь на них, создают на вашем компьютере специальные цифровые подписи, достоверность которых проверяется при последующих посещениях. Такие подписи называются сертификатами. Если ваш браузер не предоставит сайту соответствующего сертификата, сайт не даст вам полноценного доступа. На зараженном компьютере ZeuS находит такие сертификаты безопасности, крадет их и пересылает злоумышленнику.

Если злоумышленнику понадобится ваш компьютер как инструмент для совершения противозаконных действий (например, для рассылки спама), то ZeuS предоставит своему хозяину возможность установить на зараженной машине все необходимое для этого программное обеспечение.

Итак, в случае заражения вашего компьютера троянцем ZeuS, если у вас есть что взять, то преступник вас ограбит. Если взять у вас нечего, злоумышленник вряд ли расстроится — в любом случае у него будет возможность использовать ваш компьютер в своих преступных целях.

Зараженные компьютеры, связанные с одним «хозяином», составляют так называемый ботнет, или зомби-сеть. Злоумышленник управляет попавшимися в его сети компьютерами, как кукловод марионетками. Пользователи могут даже не догадываться, что с их компьютеров рассылается спам, что злоумышленник использует их выход в интернет, чтобы скрыть свою точку доступа во всемирную паутину. Месяцами жертвы могут пребывать в блаженном неведении, что их компьютеры участвуют в преступных махинациях. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/].*

Выше: Троянская программа

См. также: Карберп, троянская банковская программа

Знак охраны авторского права —

Правообладатель для оповещения о принадлежащем ему исключительном праве на произведение вправе использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и состоит из следующих элементов:

- латинской буквы "С" в окружности;
- имени или наименования правообладателя;
- года первого опубликования произведения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Авторские права, Знак охраны товарного знака, Знак охраны топологии интегральной микросхемы

Знак охраны товарного знака —

Правообладатель для оповещения о своем исключительном праве на товарный знак вправе использовать знак охраны, который помещается рядом с товарным знаком, состоит из латинской буквы "R" или латинской буквы "R" в окружности ® либо словесного обозначения "товарный знак" или "зарегистрированный товарный знак" и указывает на то, что применяемое обозначение является товарным знаком, охраняемым на территории Российской Федерации. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Знак охраны авторского знака, Знак охраны топологии интегральной микросхемы

Знак охраны топологии интегральной микросхемы —

Правообладатель для оповещения о своем исключительном праве на топологию вправе использовать знак охраны, который помещается на топологии, а также на изделиях, содержащих такую топологию, и состоит из выделенной прописной буквы "Т", даты начала срока действия исключительного права на топологию и информации, позволяющей идентифицировать правообладателя. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Знак охраны авторского знака, Знак охраны товарного знака.

Знак правовой охраны смежных прав —

Изготовитель фонограммы и исполнитель, а также иной обладатель исключительного права на фонограмму или исполнение вправе для оповещения о принадлежащем ему исключительном праве использовать знак охраны смежных прав, который помещается на каждом оригинале или экземпляре фонограммы и (или) на каждом содержащем ее футляре и состоит из трех элементов - латинской буквы "Р" в окружности, имени или наименования обладателя исключительного права, года первого опубликования фонограммы. [Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N

230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008].

См. также: Знак охраны авторского знака, Знак охраны топологии интегральной микросхемы, Смежные права, Объекты смежных прав

Зомби [zombies] —

Маленькие компьютерные программы, разносимые по сети интернет компьютерными червями. Программы - зомби устанавливают себя в пораженной системе и ждут дальнейших команд к действию. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

Выше: Компьютерный вирус

См. также: Сетевой червь

Идеальная случайная последовательность [ideal random sequence] —

Последовательность, являющаяся реализацией последовательности независимых случайных величин, имеющих равномерное распределение на заданном конечном алфавите. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Истинно случайная последовательность

Идеальная схема разделения секрета [ideal secret sharing scheme] —

Схема разделения секрета, в которой число битов, содержащихся в каждой доле секрета, равно числу битов, содержащихся в самом секрете. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема разделения секрета

Идентификатор [identifier] —

Представление, однозначно идентифицирующее сущность (например пользователя, процесс или диск) в контексте конкретного объекта оценки.

Примечание — Примером такого представления может быть строка символов. Для человека-пользователя таким представлением может быть полное или сокращенное имя или (также уникальный) псевдоним. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

Ниже: Идентификатор доступа

См. также: Идентификация

Идентификатор доступа [access identifier] —

Уникальный признак субъекта или объекта доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Выше: Идентификатор

Идентификатор ключа [key identifier] —

Указатель на ключ, представляющий собой системное имя ключа в программной реализации криптографического алгоритма и имеющий

установленный в системе формат. Используется в качестве переменной при записи различных криптографических операций в тексте программы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Идентификационные данные [identity] —

Совокупность уникальных идентификационных данных, соответствующая конкретному участнику, позволяющая осуществить однозначную его идентификацию в системе. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*

См. также: Идентификация, Входить в систему

Идентификация [identification] —

1. Действия по присвоению субъектам и объектам доступа идентификаторов и (или) действия по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

2. Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

3. Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

4. Процедура установления присвоенного данной стороне уникального системного имени — идентификатора, которое позволяет отличать ее от других сторон. Обычно процедура идентификации заключается в предъявлении этого имени и предшествует процедуре аутентификации, то есть подтверждению правильности идентификации. Термин и. часто для краткости используют для обозначения общей процедуры идентификации/аутентификации сторон (см., например, протокол идентификации). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Идентификатор, Идентификация и аутентификация, Идентификационные данные, Идентификация пользователя (в информационной системе), Аутентификация, Механизм (средство) разграничения доступа, Управление идентификацией

Идентификация и аутентификация [Identification and Authentication (I&A)] —

Общий термин для обозначения процесса представления своего идентификатора и подтверждения подлинности (идентичности) пользователем системы, который выполняется им для получения доступа к ресурсам. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Идентификатор, Идентификация, Аутентификация

Идентификация пользователя (в информационной системе) [user identification in an information system] —

Присвоение пользователям идентификаторов и проверка вхождения предъявляемых идентификаторов в список присвоенных идентификаторов. Обязательно должна дополняться аутентификацией — проверкой принадлежности пользователю предъявленного им идентификатора. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Идентификатор, Идентификация, Аутентификация

Идентификация риска [risk identification] —

1. Процесс обнаружения, распознавания и описания рисков. Примечание 1. Идентификация включает распознавание источников риска,событий, их причин и возможных последствий. Примечание 2. Идентификация риска может использовать исторические данные, теоретический анализ, обоснованную точку зрения и экспертные мнения и потребности заинтересованных сторон. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Процесс обнаружения, распознавания и описания рисков. Примечание 1. Идентификация риска включает в себя идентификацию источников риска, событий и их причин, а также их возможных последствий. Примечание 2. Идентификация риска может включать в себя статистические данные, теоретический анализ, обоснованные точки зрения и экспертные заключения и потребности заинтересованных сторон. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Регистр рисков, Менеджмент риска

Идентификация с нулевым разглашением [zero-knowledge identification] —

Вид доказательства с нулевым разглашением, целью которого является аутентификация сторон, т. е. доказательство одним из участников своей идентичности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Доказательство с нулевым разглашением

Идентификация скрытого канала —

Выявление возможности существования скрытого канала и определение его места в классификации. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Глубина анализа скрытого канала, Скрытый канал

Идентификация специального защитного знака —

Определение подлинности и целостности СЗЗ по его характерным признакам, а также отсутствия изменений в расположении СЗЗ на объекте защиты или документе путем визуального осмотра или с помощью технических средств общего применения, специализированных технических средств с использованием или без использования специальных методик. *[Руководящий документ Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

Ниже: Подлинность специального защитного знака, Целостность специального защитного знака

См. также: Специальный защитный знак (СЗЗ)

Иерархия ключей [hierarchy of keys] **—**

Структура ключевого множества криптосистемы, отражающая различные функции, выполняемые отдельными частями составного ключа. Например, ключевое множество криптосистемы может иметь древовидную структуру, если каждый ключ состоит из двух подключей: общего для всех законных пользователей сети связи долговременного ключа и уникального для каждого сеанса связи разового ключа. Ключевое множество может иметь также матричную структуру, если каждый ключ состоит из трех подключей: уникального для каждой пары пользователей и каждого сеанса связи разового ключа, уникального для каждой пары пользователей долговременного ключа для шифрования разовых ключей и индивидуального главного ключа пользователя для хранения в зашифрованном виде долговременного ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Главный ключ, Долговременный ключ, Разовый ключ

Избирательная защита поля —

Защита конкретных полей внутри сообщения, подлежащего передаче. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Услуга защиты, Целостность выделенных полей

Изменение настроек браузера [browser hijacking] **—**

Модификация настроек Web-браузера с помощью вредоносного программного обеспечения. Термин «hijacking» (от hijacker — «налетчик», «грабитель») использован в связи с тем, что изменение производится без ведома и разрешения пользователя. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Вредоносное программное обеспечение

Изобретение —

Техническое решение в любой области, относящееся к продукту (в частности, устройству, веществу, штамму микроорганизма, культуре клеток растений или животных) или способу (процессу осуществления действий над материальным объектом с помощью материальных средств).

Не являются изобретениями:

1) открытия;

2) научные теории и математические методы;

3) решения, касающиеся только внешнего вида изделий и направленные на удовлетворение эстетических потребностей;

4) правила и методы игр, интеллектуальной или хозяйственной деятельности;

5) программы для ЭВМ;

6) решения, заключающиеся только в представлении информации. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Патентные права

Имитация [imitation] —

Активная атака на криптографический протокол, целью которой является навязывание противником и/или нарушителем одной из сторон сообщения от имени другой стороны, которое не будет отвергнуто при приеме. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Активная атака

Имитовставка [message authentication code] —

Отрезок информации фиксированной длины, полученной по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*. См. также: Код аутентичности сообщения, Имитозащита

Имитозащита [integrity protection, protection from imitation] —

Защита сообщений в системе связи от навязывания ложных данных. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

См. также: Аутентификация сообщения, Аутентификация сторон, Имитовставка, Имитостойкость, Система имитозащиты

Имитостойкость [imitation resistance] —

Свойство криптографической системы (криптографического протокола), характеризующее способность противостоять активным атакам со стороны противника и/или нарушителя, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Активная атака, Имитозащита

Инволютивный алгоритм шифрования [involutive encryption algorithm] —

Алгоритм шифрования, для которого алгоритмы зашифрования и расшифрования совпадают. Другими словами, если к открытому тексту дважды

применить алгоритм зашифрования, то получится тот же самый открытый текст. Исторически для таких алгоритмов употребляется название «обратимый», но правильно называть их именно «инволютивными», в соответствии с общим пониманием инволюции в математике. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм шифрования

Инициатор [trigger] —

Событие, которое инициирует реакцию системы.

Примечание. Также известен, как инициирующее событие. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

Инсайдер [insider] —

Член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике. Термин используется в контексте, связанном с секретной, скрытой или какой-либо другой закрытой информацией или знаниями: инсайдер — это член группы, обладающий информацией, имеющейся только у этой группы.

В современном запутанном мире, с его обилием информации, понятие инсайдерских данных распространено как источник последовательного и верного управления. В данной ситуации, инсайдер противопоставляется внешнему специалисту. Специалист может обеспечить всесторонний теоретический анализ, который будет затем основой для экспертного заключения, а инсайдер обладает реальной информацией «из первых рук».

Инсайдер — нейтральный термин, в зависимости от контекста он может иметь положительное или отрицательное. Вероятно, можно сказать, что во всех контекстах инсайдер связан с относительно большой, возможно, даже личной властью и всегда порождает реакции опасения и уважения, в зависимости от обстоятельств.

Активное участие — определяющий фактор: если человек просто очевидец, это не делает его инсайдером. Инсайдер — тот, кто не просто ознакомлен с фактами и деятельностью, а тот, кто в курсе повседневной работы и отношений людей в определенной группе. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Инструментальные средства аудита [audit tools] —

Автоматизированные инструментальные средства, помогающие анализировать содержание журналов событий. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Ведение контрольных журналов

Интегрированная автоматизированная система —

Совокупность двух или более взаимоувязанных автоматизированных систем, в которой функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую автоматизированную систему. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

Выше: Автоматизированная система

Интеллектуальная собственность —

Результаты интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана. К ним относятся:

1) произведения науки, литературы и искусства;

2) программы для электронных вычислительных машин (программы для ЭВМ);

3) базы данных;

4) исполнения;

5) фонограммы;

6) сообщение в эфир или по кабелю радио- или телепередач (вещание организаций эфирного или кабельного вещания);

7) изобретения;

8) полезные модели;

9) промышленные образцы;

10) селекционные достижения;

11) топологии интегральных микросхем;

12) секреты производства (ноу-хау);

13) фирменные наименования;

14) товарные знаки и знаки обслуживания;

15) наименования мест происхождения товаров;

16) коммерческие обозначения.

Примечание: Интеллектуальная собственность охраняется законом. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Интеллектуальные права, Изобретение, Использование (интеллектуального) произведения

Интеллектуальные права —

Включают исключительное право, являющееся имущественным правом, а в случаях, предусмотренных Гражданским Кодексом РФ, также личные неимущественные права и иные права (право следования, право доступа и другие). *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Интеллектуальная собственность

Интерактивная аутентификация [interactive authentication] **—**

Аутентификация, осуществляемая с помощью интерактивного протокола. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Аутентификация

См. также: Интерактивный протокол

Интерактивное доказательство [interactive proof] —

Понятие теории сложности вычислений, составляющее основу понятия доказательства с нулевым разглашением. Интерактивное доказательство — доказательство путем выполнения протокола с двумя участниками, доказывающим и проверяющим, в процессе работы которых участники обмениваются сообщениями (запросы и ответы), обычно зависящими от случайных чисел, которые могут содержаться в секрете. Цель доказывающего — убедить проверяющего в истинности некоторого утверждения. Проверяющий либо принимает, либо отвергает доказательство. В отличие от обычного математического понятия доказательства в данном случае доказательство носит не абсолютный, а вероятностный характер и характеризуется двумя вероятностями. Если доказываемое утверждение верно, то доказательство должно быть верным с вероятностью, стремящейся к единице при увеличении числа циклов протокола. Если же доказываемое утверждение ложно, то при увеличении числа циклов протокола вероятность правильности доказательства должна стремиться к нулю. Криптографическое качество протокола интерактивного доказательства характеризуется свойствами полноты, корректности и нулевого разглашения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Доказательство знания

См. также: Доказательство с нулевым разглашением

Интерактивный протокол [interactive protocol] —

Протокол, выполняемый за два цикла (раунда) или более. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Интерактивный режим [interactive mode] —

Режим взаимодействия процесса обработки информации системы обработки информации с человеком, выражающийся в разного рода воздействиях на этот процесс, предусмотренных механизмом управления конкретной системы и вызывающих ответную реакцию процесса. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Диалоговый режим, Режим пакетной обработки, Режим разделения времени, Режим реального времени, Система обработки информации, Сеанс работы

Интересы в информационной сфере —

Реальная причина действий, лежащая в основе мотивов развития информационной сферы государства, общества, личности. В Доктрине информационной безопасности РФ определены интересы государства, общества, личности в сфере информационной безопасности. *[Доктрина*

информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].

Ниже: Интересы государства в информационной сфере, Интересы личности в информационной сфере, Интересы общества в информационной сфере

См. также: Информационная безопасность Российской Федерации, Информационная сфера

Интересы государства в информационной сфере —

Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Интересы в информационной сфере, Национальные интересы России в информационной сфере

Интересы личности в информационной сфере —

Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающей личную безопасность. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Интересы в информационной сфере

Интересы общества в информационной сфере —

Обеспечение интересов личности в этой сфере, упрочении демократии, создание правового социального государства, достижение и поддержание общественного согласия, в духовном обновлении России. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Интересы в информационной сфере

Интернет-мошенничество [Internet fraud] —

Вид «высокотехнологической» преступности в кредитно-финансовой сфере, носит организованный и, как правило, международный характер. Для получения нелегальных доходов криминальными структурами широко применяются современные технологии, такие как атака блокировки доступа с целью получения выкупа или создание бот-сетей. С помощью последних

осуществляются кражи личных данных, таких как пароли доступа, данные банковских и идентификационных карт. Получая доступ к зараженным вирусом персональным компьютерам, на которых используются системы дистанционного банковского обслуживания, преступники получают возможность распоряжаться средствами на банковских счетах своих жертв. Как правило, украденные деньги выводятся на карточные счета, оформленные на подставных лиц, и снимаются наличными в банкоматах. В настоящее время внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества, наблюдается специализация и разделение труда: администратор зараженных компьютеров — управляет бот-сетью; заливщик — скрытно управляет компьютером потерпевшего и производит платеж; поставщик трафика — обеспечивает поток новых заражений; кардселлер — снабжает картами и «буферными» счетами; организатор — управляет действиями, распределяет деньги, оперативно переставляя их с «буферного» счета на карточные для обналичивания; дроп — снимает деньги в банкомате; дроповод-нальщик — управляет «дропом», организует снятие; кодеры (программисты) пишут троянцев и продают их на закрытых форумах для «своих» и т. п. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Ниже: Дифейсмент, Кардинг, Скамминг, Фишинг, Фарминг, Фрод См. также: Мошенничество в сфере компьютерной информации, Дроп, Дроповод-нальщик, Заливщик, Кардселлер, Кодер (программист), Поставщик трафика, Социальная инженерия

Интерфейс [interface] **—**

1. Разделительная граница, определенная с помощью характеристик этой границы.

Прим.: Интерфейс может быть определен на физическом уровне, на уровне компьютерных программ или на чисто логическом уровне. к примеру, характеристики границы — это идентификаторы физических соединений, описания сигналов, которыми обмениваются стороны через границу или спецификация функций, выполняемых по обе стороны границы. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Совокупность средств и правил, обеспечивающих взаимодействие устройств вычислительной машины или системы обработки информации и (или) программ. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Интерфейс функциональных требований безопасности объекта оценки [TSF interface] **—**

Средства, через которые внешние сущности (или субъект в объекте оценки, но за пределами функциональных требований безопасности объекта оценки) передают данные к функциональным требованиям безопасности объекта оценки, получают данные от функциональных требований безопасности объекта оценки и обращаются к сервисам функциональных

требований безопасности объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Внешняя сущность (для объекта оценки), Требование безопасности (объекта оценки)

Интранет [intranet] —

Частная компьютерная сеть, использующая Интернет-протоколы и возможность сетевого соединения для безопасного коллективного использования части информации или операций организации ее сотрудниками. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Инфокоммуникационная структура сети электросвязи —

Совокупность информационных ресурсов и инфраструктуры сети электросвязи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

Ниже: Информационные ресурсы сети электросвязи, Инфраструктура сети электросвязи

Информативный сигнал —

1. Сигнал, по параметрам которого может быть определена защищаемая информация. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

2. Электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и обсуждаемая в защищаемых помещениях. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

Выше: Сигнал

См. также: Защищаемая информация, Конфиденциальная информация, Побочные электромагнитные излучения и наводки

Информатизация [informatization] —

Процесс интенсификации производства и распространения знаний и информации, основанный на использовании информационно-коммуникационных технологий. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Информационно-коммуникационные технологии, Средства информатизации

Информационная база автоматизированной системы [informational background of AS] —

Совокупность упорядоченной информации, используемой при функционировании АС. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Документация

Информационная безопасность [information security] —

1. Состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Обеспечение конфиденциальности, доступности и целостности информации; дополнительно могут подразумеваться другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность. *[Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности ISO/IEC 17999: 2005]*.

3. Защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность. *[ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Введен в действие: 01.01.2014]*.

4. Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информационно-телекоммуникационных технологий. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

5. Безопасность, связанная с угрозами в информационной сфере.

Примечание.

1. Защищенность достигается обеспечением совокупности свойств информационной безопасности — доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств информационной безопасности определяется ценностью указанных активов для интересов (целей) организации банковской системы Российской Федерации

2. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений. *[Стандарт*

Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)].

6. Состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств, как целостность, объективность, доступность и конфиденциальность. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009].*

Выше: Безопасность

Ниже: Информационная безопасность взаимоувязанной сети связи Российской Федерации, Информационная безопасность объекта информатизации, Информационная безопасность организации, Информационная безопасность Российской Федерации, Международная информационная безопасность

См. также: Защита информации, Доступность, Конфиденциальность, Целостность, Меры обеспечения информационной безопасности, Надежность, Система обеспечения информационной безопасности, Общие методы обеспечения информационной безопасности, Осознание необходимости обеспечения информационной безопасности, План работ по обеспечению информационной безопасности, Риск информационной безопасности

Информационная безопасность взаимоувязанной сети связи Российской Федерации —

Состояние (степень) защищенности информационной сферы Взаимоувязанной сети связи Российской Федерации от заданного множества угроз информационной безопасности Взаимоувязанной сети связи Российской Федерации. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].*

См. также: Защищенность информационной сферы Взаимоувязанной сети связи Российской Федерации, Информационная сфера взаимоувязанной сети связи Российской Федерации, Информация управления информационной безопасностью Взаимоувязанной сети связи Российской Федерации, Меры обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации, Механизм обеспечения информационной безопасности (защиты) Взаимоувязанной сети связи Российской Федерации, Нарушитель информационной безопасности Взаимоувязанной сети связи Российской Федерации, Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации, Объект информационной безопасности Взаимоувязанной сети связи Российской Федерации, Политика информационной безопасности Взаимоувязанной сети связи Российской Федерации, Проект информационной безопасности Взаимоувязанной сети связи Российской Федерации, Система обеспечения информационной

безопасности сети связи Российской Федерации, Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации

Информационная безопасность объекта информатизации —

Состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Объект информатизации

Информационная безопасность организации —

Состояние защищенности интересов организации в условиях угроз в информационной сфере.

Примечание. Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Организация, Информационный актив, Политика информационной безопасности (организации), Обеспечение информационной безопасности организации, Цель информационной безопасности (организации), Угроза информационной безопасности организации.

Информационная безопасность Российской Федерации —

Состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Интересы в информационной сфере

Информационная война [information war] **—**

1. Противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Противоборство между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической, экономической и социальной систем, а также массированной психологической обработки населения с целью дестабилизации общества и государства. *[Доклад Генерального секретаря ООН от 10 июня 2000г.]*.

3. Действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации, и системам информационным противника при одновременной защите собственной информации, процессов, основанных на информации и системах информационных. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Информационное оружие, Международная информационная безопасность, Международный информационный терроризм

Информационная инфраструктура [information infrastructure] —

1. Совокупность технических средств и систем формирования, преобразования, передачи, использования и хранения информации. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

3. Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

Примечание. Информационная инфраструктура — включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

4. Технические средства и системы формирования, обработки, хранения и передачи информации, включая массивы и базы данных и собственную информацию и ее потоки. *[Доклад Генерального секретаря ООН от 10 июня 2000г.]*.

Ниже: Информационная инфраструктура системы (сети) связи

См. также: Информационные ресурсы, Объект информатизации, Система обработки информации, Средства обработки информации

Информационная инфраструктура системы (сети) связи —

Совокупность информационных подсистем, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения,

обработки и передачи информации в системе (сети) связи. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Информационная инфраструктура

См. также: Информационная сфера взаимоувязанной сети связи Российской Федерации

Информационная система [information system] —

1. Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

2. Система обработки информации, работающая совместно с организационными ресурсами, такими как люди, технические средства и финансовые ресурсы, которые обеспечивают и распределяют информацию. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

3. Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Примечание. Информационные системы предназначены для хранения, обработки, поиска, распространения, передачи и предоставления информации. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

4. Автоматизированная система, результатом функционирования которой является представление выходной информации для последующего использования. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Система

Ниже: Автоматизированная информационная система, Защищаемая информационная система, Информационная система общего пользования, Информационная система персональных данных, Система обработки информации.

См также: База данных, Информационная технология, Обработка информации, Предоставление информации, Распространение информации, Ресурс (информационной системы), Оператор информационной системы, Средства информатизации.

Информационная система, обрабатывающая биометрические персональные данные —

Информационная система, в которой обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных. *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

Выше: Информационная система персональных данных.

Информационная система, обрабатывающая общедоступные персональные данные —

Информационная система, в которой обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных". *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

Выше: Информационная система персональных данных

См. также: Общедоступные персональные данные

Информационная система, обрабатывающая персональные данные сотрудников оператора —

Информационная система, в которой обрабатываются персональные данные только указанных сотрудников. *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

Выше: Информационная система персональных данных

Информационная система, обрабатывающая специальные категории персональных данных —

Информационная система, в которой обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных. *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

Выше: Информационная система персональных данных

Информационная система общего пользования —

Информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об*

электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011].

Выше: Информационная система

См. также: Участники электронного взаимодействия

Информационная система персональных данных —

Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007].*

Ниже: Информационная система, обрабатывающая биометрические персональные данные, Информационная система, обрабатывающая общедоступные персональные данные, Информационная система, обрабатывающая персональные данные сотрудников оператора, Информационная система, обрабатывающая специальные категории персональных данных.

Информационная среда [information environment] —

Совокупность технических и программных средств хранения, обработки и передачи информации, а также существующих в стране политических, экономических и культурных условий реализации процессов развития и использования информационно-коммуникационных технологий. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009].*

См. также: Информационно-коммуникационные технологии, Средства обработки информации

Информационная сфера [information sphere] —

1. Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

2. Сфера (среда) деятельности субъектов, связанная с созданием, преобразованием и потреблением информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000].*

3. Представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)].*

См. также: Информационная инфраструктура, Интересы в информационной сфере

Информационная сфера взаимоувязанной сети связи Российской Федерации —

Совокупность информационных ресурсов и информационной структуры Взаимоувязанной сети связи Российской Федерации. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Защищенность информационной сферы Взаимоувязанной сети связи Российской Федерации, Информационная инфраструктура системы (сети) связи

Информационная технология [information technology] —

1. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

Ниже: Защищаемая информационная технология, Обработка информации, Предоставление информации, Распространение информации

См. также: Информационные технологии

Информационно-безопасная (защищенная) сеть связи общего пользования (служба электросвязи) —

Сеть связи общего пользования (служба электросвязи), обеспечивающая заданный уровень качества служб информационной безопасности ССОП (службы электросвязи) по отношению к заданному множеству угроз информационной безопасности ССОП (службы электросвязи) и предоставление пользователю по его запросу определенных услуг информационной безопасности ССОП (службы электросвязи). *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Ниже: Служба электросвязи, Сеть связи общего пользования

Информационно-коммуникационные технологии —

Совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, преобразования, передачи, использования и хранения информации. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

См. также: Информатизация

Информационно-психологическая безопасность —

Состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере. *[Ковалева Н.Н. Информационное право России. Учебное пособие. М., 2007.]*

См. также: Информационно-психологическое воздействие.

Информационно-психологическое воздействие —

1. Применение информационно-психологических способов и средств воздействия на психику человека с целью ее модификации в нужном для воздействующей стороны направлении. [*И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

2. Комплекс мероприятий по воздействию на интеллектуальную, рационально-волевую и эмоционально-чувственную сферу психики и подсознание информационно-психологических объектов, направленных на формирование у них прогнозируемых мнений и взглядов, мировоззренческих и психологических установок, поведенческих реакций. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Воздействие

Ниже: Манипулятивное воздействие

См. также: Информационно-психологическая безопасность

Информационно-телекоммуникационная сеть —

Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Выше: Сеть

Информационно-телекоммуникационная система [information-telecommunication system] —

Совокупность компьютерных систем, объединенных системой передачи данных. Компьютерные системы реализуют функции автоматизации процессов сбора, обработки и хранения информации, а системы передачи данных позволяют осуществлять обмен этой информацией между ними, а также обеспечивать доступ удаленных пользователей к хранящейся и обрабатываемой информации. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

Выше: Система

См. также: Критичный компонент (информационно-телекоммуникационной системы).

Информационно-техническое воздействие —

Комплекс программных (программно-аппаратных) и радиоэлектронных средств, направленных на манипулирование функционированием информационно-технических объектов, а также прекращение (затруднение) работы или вывод их из строя на определенный период. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Воздействие

См. также: Средства информационного воздействия

Информационное обеспечение автоматизированной системы [AS information support] —

Совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Автоматизированная система, Методическое обеспечение автоматизированной системы, Организационное обеспечение автоматизированной системы, Правовое обеспечение автоматизированной системы, Программное обеспечение автоматизированной системы, Техническое обеспечение автоматизированной системы

Информационное оружие [information weapon] —

1. Информационные технологии, средства и методы, предназначенные для ведения информационной войны. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Совокупность специальных методов (физических, информационных, программных, радиоэлектронных) и средств, предназначенных для временного или безвозвратного вывода из строя функций или служб инфраструктуры информационно-коммуникационной в целом или отдельных ее элементов. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Информационная война

Информационное пространство —

Сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

См. также: Информационная инфраструктура

Информационное средство [information facility] **—**

Комплекс упорядоченной относительно постоянной информации на носителе данных, описывающей параметры и характеристики заданной области применения и соответствующей документации, предназначенный для поставки пользователю.

Примечание. Документация информационного средства может поставляться на носителе данных. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Документация

Информационные ресурсы [information resource] **—**

1. Информационная инфраструктура, а также собственно информация и ее потоки. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

Выше: Ресурс.

Ниже: Информационные ресурсы сети электросвязи.

См. также: Информационная инфраструктура.

Информационные ресурсы сети электросвязи —

Совокупность хранимых (используемых для обеспечения процессов функционирования сети электросвязи), обрабатываемых и передаваемых данных, содержащих информацию пользователей и/или системы управления сетью электросвязи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

Выше: Инфокоммуникационная структура сети электросвязи, Информационные ресурсы.

Информационные сети общего пользования —

Вычислительные (информационно-телекоммуникационные сети) открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

Син.: Сеть связи общего пользования

См. также: Абонент сети, Вычислительная сеть, Провайдер сети

Информационные технологии —

1. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

2. Практическая деятельность и прикладная наука, имеющие дело с данными и информацией.

Примечание. Примером является сбор, изображение, обработка, обеспечение безопасности, передача, взаимообмен, представление, управление, организация, хранение и восстановление данных и информации. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Ниже: Обработка информации, Предоставление информации, Распространение информации

См. также: Информационная технология, Услуги информационных технологий

Информационный актив [information assets] —

1. Знания или данные, которые имеют значение для организации. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации банковской системы Российской Федерации; находящаяся в распоряжении организации банковской системы Российской Федерации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Актив

См. также: Классификация информационных активов, Доступность информационных активов, Конфиденциальность информационных активов, Целостность информационных активов, Объект среды информационного актива.

Информационный объект [information object] —

1. Элемент программы, содержащий фрагменты информации, циркулирующей в программе. В зависимости от языка программирования в качестве информационных объектов могут выступать переменные, массивы, записи, таблицы, файлы, фрагменты оперативной памяти и т. п. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)]*.

2. Представление объекта предметной области в информационной системе, определяющее его структуру, атрибуты, ограничения целостности и, возможно, поведение. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Выше: Объект

Информационный поток [information flow] —

Процесс взаимодействия источника информации и ее получателя.

Примечание. Информационный поток может быть разрешенным и неразрешенным. Информационный поток между объектами X и Y существует, если средняя взаимная информация I (X, Y) больше 0. Математическая модель информационного потока может определяться как конечный автомат, в котором источник сообщения посылает входное слово на вход автомата, а получатель сообщения видит выходную последовательность автомата. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Управление информационным потоком

Информационный процесс [information process] —

1. Процесс создания, сбора, обработки, накопления, хранения, поиска, распространения и использования информации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и применения (потребления) информации. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

3. Процесс создания, сбора, хранения, обработки, отображения, передачи, распространения и использования информации. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Информационная технология

Информация [information] —

1. Сведения (сообщения, данные) независимо от формы их представления. Информация в зависимости от категории доступа к ней подразделяется на информацию общедоступную, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

3. Форма представления информации может быть классифицирована по степени упорядоченности; форме закрепления; доступности, содержанию, затратам интеллектуального труда человека. По степени упорядоченности различают информацию и документированную информацию. По форме закрепления информация подразделяется на представленную в письменном виде (рукопись, машинопись, нотная запись и т. д.), в устной форме (публичное произнесение, публичное исполнение и т. д.), в виде звуко- или видеозаписи механической, магнитной, цифровой, оптической и т. д.), в виде изображения (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видео- или фотокадр и т. д.), в объемно-пространственной форме (скульптура, модель, макет, сооружение и т. д.). По доступности информация разделяется на открытую (общедоступную) и ограниченного доступа. По содержанию информация может быть классифицирована по сфере применения; ценности информации от времени; предназначению. По сфере применения информация может быть разделена на экономическую, социально значимую, служебную, частную, развлекательную и тому подобную. По ценности информации от времени информация может быть разделена на оперативную, неоперативную и памятники культуры. Ценность оперативной информации существенно зависит от времени, прошедшего с момента ее возникновения. Ценность неоперативной информации в меньшей степени зависит от времени. Произведения художественной литературы или искусства могут сохранять свою ценность в течение нескольких лет. Если ценность этих произведений не уменьшается в течение десятков лет, они могут быть отнесены к памятникам культуры. По предназначению информация подразделяется на массовую, групповую и индивидуальную. Массовая информация представляет собой сведения, предназначенные для неограниченного круга лиц. Групповая информация ориентирована на использование вполне определенным кругом лиц, имеющих отношение к содержащимся в ней сведениям. Индивидуальная информация ориентирована на конкретного человека. По затратам интеллектуального труда человека на создание информации она условно может быть разделена на высокоинтеллектуальную, распорядительную и бытовую. *[Родионов С., Комов С., Ракитин В., Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Ниже: Документированная информация, Информация ограниченного доступа, Информация, составляющая коммерческую тайну (секрет производства), Компьютерная информация

См. также: Данные, Защита информации, Разрушение информации

Информация аутентификации —

Информация, используемая для установления подлинности запрашиваемой личности. *[ГОСТ Р ИСО 7498-2-99 Информационная*

технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].

См. также: Аутентификация

Информация об авторском праве —

Любая информация, которая идентифицирует произведение, автора или иного правообладателя, либо информация об условиях использования произведения, которая содержится на оригинале или экземпляре произведения, приложена к нему или появляется в связи с сообщением в эфир или по кабелю либо доведением такого произведения до всеобщего сведения, а также любые цифры и коды, в которых содержится такая информация. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Авторские права

Информация ограниченного доступа [information with restricted access] **—**

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим тайну коммерческую, тайну служебную и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение. Информация, составляющая профессиональную тайну, подлежит защите в случаях, если на ее обладателей федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. Не может быть ограничен доступ к: 1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления; 2) информации о состоянии окружающей среды; 3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну); 4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией; 5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами. [Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о

защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]

2. Вид сведений, доступ к которым ограничен и разглашение которых может нанести ущерб интересам других лиц, общества и государства. [ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]

3. Вид сведений, доступ к которым ограничен в соответствии с законодательством и разглашение которых может нанести ущерб интересам других лиц, общества и государства. [И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]

4. В составе информации ограниченного доступа различают сведения, составляющие государственную тайну, и конфиденциальную информацию. Информация ограниченного доступа подразделяется на секретную и конфиденциальную. [Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]

Выше: Информация

Ниже: Конфиденциальная информация, Секретная информация

Информация, составляющая коммерческую тайну (секрет производства) [commercial information] —

Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. [Федеральный закон от 29.07.2004 N 98-ФЗ “О коммерческой тайне” (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]

Выше: Информация

См. также: Доступ к информации, составляющей коммерческую тайну, Коммерческая тайна, Обладатель информации, составляющей коммерческую тайну, Передача информации, составляющей коммерческую тайну, Режим коммерческой тайны, Предоставление информации, составляющей коммерческую тайну, Секрет производства (ноу-хау), Ценная информация

Информация управления информационной безопасностью Взаимоувязанной сети связи Российской Федерации —

Информация, необходимая для реализации функции управления в системе обеспечения информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети*

связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].

См. также: Информационная безопасность взаимоувязанной сети связи Российской Федерации

Инфраструктура [infrastructure] —

1. Совокупность зданий, оборудования и служб обеспечения, необходимых для функционирования организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи). *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Инфраструктура сети электросвязи

Инфраструктура открытых ключей [Public Key Infrastructure (PKI)] —

Подсистема ключевой системы асимметричной шифрсистемы. Предназначена для обеспечения (с помощью сертификатов ключей) доверия законных пользователей к подлинности ключей, соответствия ключей пользователям и оговоренным условиям их применения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключевая система асимметричной шифрсистемы

Инфраструктура сети электросвязи —

Совокупность средств связи, линий связи, сооружений связи, технологических систем связи, технологий и организационных структур, обеспечивающих информационное взаимодействие компонентов сети электросвязи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

Выше: Инфокоммуникационная структура сети электросвязи, Инфраструктура

Инцидент (компьютерный) [incident] —

1. Факт нарушения штатного режима функционирования элемента критической информационной инфраструктуры или критической информационной инфраструктуры в целом. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

2. Зафиксированный случай попытки получения доступа несанкционированного или проведения атаки на компьютерную систему. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Инцидент информационной безопасности, Силы ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре, Средства ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре

Инцидент в системе дистанционного банковского обслуживания (или инцидент, связанный с мошенничеством или покушение м на совершение мошенничества в системе дистанционного банковского обслуживания) —

Внешний или внутренний инцидент, в результате которого были созданы, п одписаны с помощью электронной подписи и переданы в банк платежные поруче ния без санкции со стороны уполномоченных на совершение указанных действий лиц. *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

См. также: Антифрод системы

Инцидент информационной безопасности [information security incident] —

1. Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ. *[ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Введен в действие: 01.07.2008]*.

2. Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечания. Инцидентами информационной безопасности являются:

• утрата услуг, оборудования или устройств;
• системные сбои или перегрузки;
• ошибки пользователей;
• несоблюдение политик или рекомендаций;
• нарушение физических мер защиты;
• неконтролируемые изменения систем;
• сбои программного обеспечения и отказы технических средств;
• нарушение правил доступа. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

3. Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

Примечания.

1) Реализация угрозы информационной безопасности — реализация нарушения свойств информационной безопасности информационных активов организации банковской системы Российской Федерации.

2) Нарушение может вызываться источниками угроз безопасности информационной — либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

4. Системное событие, в рамках которого произошло нарушение политики безопасности. *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

Ниже: Внешний инцидент (или инцидент, имеющий внешний характер), Внутренний инцидент (или инцидент, имеющий внутренний характер).

См. также: Информационная безопасность, Инцидент (компьютерный), Менеджмент инцидента информационной безопасности, Угроза (безопасности информации), Центр управления безопасностью.

Инъекция SQL [SQL injection] —

Один из распространенных способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода. Внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере. Основана на некорректной обработке входных данных, используемых в SQL-запросах. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Атака

Исключение риска [risk avoidance] —

Решение об исключении угрозы появления опасной ситуации или действий, связанных с возможностью ее возникновения.

Примечание - Решение может быть принято на основе результатов сравнительной оценки риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

См. также: Сравнительная оценка риска

Искусственный интеллект [artifical intelligence] —

1. Направление в компьютерной науке, относящееся к развитию систем обработки данных, которые выполняют функции, обычно связываемые с человеческим интелектом, в частности, такие функции, как рассуждение, обучение и самосовершенствование. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Способность вычислительной машины моделировать процесс мышления за счет выполнения функций, которые обычно связывают с человеческим интеллектом.

Примечание. Такими функциями являются, например, обучение и логический вывод. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Использование (интеллектуального) произведения —

Использованием произведения независимо от того, совершаются ли соответствующие действия в целях извлечения прибыли или без такой цели, считается, в частности:

1) воспроизведение произведения;

2) распространение произведения;

3) публичный показ произведения;

4) импорт оригинала или экземпляров произведения в целях распространения;

5) прокат оригинала или экземпляра произведения;

6) публичное исполнение произведения;

7) сообщение в эфир;

8) сообщение по кабелю;

9) перевод или другая переработка произведения;

10) практическая реализация архитектурного, дизайнерского, градостроительного или садово-паркового проекта;

11) доведение произведения до всеобщего сведения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Интеллектуальная собственность

Испытания [test] **—**

Экспериментальное определение количественных и/или качественных характеристик свойств объекта испытаний как результата воздействия на него при его функционировании, при моделировании объекта и/или воздействий. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

Ниже: Аттестационные испытания, Контрольные испытания, Сертификационные испытания, Типовые испытания

См. также: Испытательная лаборатория (центр), Метод испытаний

Испытательная лаборатория (центр) —

Юридическое лицо, аккредитованное в установленном порядке для проведения исследований (испытаний) и измерений продукции. *[Постановление Правительства РФ от 21.04.2010 N 266 " Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной*

информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения". Вступило в силу 12.05.2010].

См. также: Испытания.

Истинно случайная последовательность [true random sequence] —

Последовательность, порожденная недетерминированным физическим устройством или процессом. Такая последовательность (в отличие от псевдослучайной последовательности) непредсказуема и невоспроизводима. Статистические свойства истинно случайной последовательности могут отличаться от статистических свойств идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Идеальная случайная последовательность, Псевдослучайная последовательность

Источник риска [risk source] —

Элемент, который отдельно или в комбинации, имеет собственный потенциал, чтобы вызвать риск.

Примечание. Источник риска может быть материальным и нематериальным. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Ниже: Источник риска информационной безопасности организации

См. также: Опасность

Источник риска информационной безопасности организации —

Объект или действие, способное вызвать (создать) риск.

Примечание 1. Риск отсутствует при отсутствии взаимодействия объекта, лица или организации с источником риска.

Примечание 2. Источник риска может быть материальным или нематериальным. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Источник риска

Источник угрозы безопасности информации —

1. Сущность, которая негативно воздействует на активы. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы

безопасности информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Угроза (безопасности информации), Негативные действия

Исчерпывающий анализ скрытых каналов [exhaustive covert channel analysis] —

Анализ, при котором требуется представление дополнительного свидетельства, показывающего, что план идентификации скрытых каналов достаточен для утверждения того, что были испробованы все возможные пути исследования скрытых каналов. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Систематический анализ скрытых каналов

Итеративный алгоритм шифрования [iterative encryption algorithm] —

Алгоритм шифрования, для которого соответствующие алгоритм зашифрования и алгоритм расшифрования состоят из последовательных однотипных циклов шифрования. Подобные алгоритмы относительно просто реализуются и позволяют обеспечивать, в частности, свойство перемешивания, свойство рассеивания и свойство усложнения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм шифрования

См. также: Цикл (раунд) шифрования

Итерация —

Использование компонента для выражения двух или более отдельных требований. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

Канал [channel] —

Маршрут передачи информации. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ниже: Канал ввода-вывода, Канал передачи данных, Канал проникновения, Канал связи, Канал утечки информации, Коммуникационный канал.

Канал ввода-вывода [input-output channel] —

Устройство, обеспечивающее пересылку данных между основной памятью ЭВМ и периферийными устройствами. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Выше: Канал

Канал передачи данных [data transmission channel] —

1. Канал электросвязи для передачи сигналов данных. *[ГОСТ 17657-79 Передача данных. Термины и определения. Введен в действие: 01.07.1980]*.

2. Физическая среда, по которой передается информация из одного устройства в другое. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Канал.

Син.: Среда передачи.

Канал проникновения [insecurity channel] —

Физический путь от злоумышленника к источнику конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Выше: Канал.

Канал связи [communication channel] —

1. Физическая среда, аппаратные и в некоторых каналах программные средства передачи информации. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

2. Совокупность технических средств (передатчик, линия связи, приемник, аппаратные и программные средства), обеспечивающих передачу сигналов от источника до получателя сигнала. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Канал.

Ниже: Аутентифицированный канал связи, Защищенный канал связи.

См. также: Механизм передачи информации.

Канал утечки информации [information leakage channel] —

Физический путь от источника информации конфиденциальной к злоумышленнику, по которому возможно несанкционированное получение охраняемых сведений (совокупность источника тайны коммерческой, физической среды и средства промышленного шпионажа). *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Выше: Канал.

Ниже: Технический канал утечки информации.

См. также: Специальное исследование (объекта защиты информации).

Карберп (троянская банковская программа) [Carberp] —

Вредоносная программа, создающая bot-сети для хищения финансовых средств в системах дистанционного банковского обслуживания, нацеленные, в первую очередь, на атаки компаний, которые осуществляют ежедневно большое количество денежных транзакций. Одна из самых распространенных вредоносных программ в России. Появилась в начале 2010 года. Похищает пользовательские данные, собирая пароли к учетным записям и ключевую информацию с помощью кейлоггера и снятия скриншотов рабочего стола. Отправляет найденную информацию в командный центр в виде cab-архива.

Внедряет JS-скрипты на интернет-страницы, загружает дополнительные плагины, модифицирует загрузочные области дисков для расширения возможностей влияния на систему. Эксплуатирует 4 уязвимости в операционных системах Microsoft Windows для повышения привилегий пользователя. Использует защищенный протокол обмена данными между компьютерами жертвы и командным центром. Предпринимает активные меры по скрытию своего присутствия в системе. Использует большое количество нестандартных способов обхода эвристических алгоритмов современных антивирусов и сканеров. Предусмотрены возможности обновления, самоудаления и загрузки дополнительных модулей, которые нейтрализуют работу антивирусных систем и занимаются устранением конкурентов, включая своих предшественников Zeus и SpyEye. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

Выше: Троянская программа.

См. также: Бот-сеть (ботнет), Зевс (троянская банковская программа).

Кардинг [carding] —

Вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Для этого могут использоваться такие методы, как взлом серверов интернет-магазинов, платежных и расчетных систем, хищение данных с персональных компьютеров, фишинг, скимминг и т.п. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Интернет-мошенничество, Социальная инженерия

Ниже: Скимминг

См. также: Фишинг

Кардселлер [cardseller] —

Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества; обозначает участника, который снабжает других участников группировки картами, открытыми на подставные счета, и «буферными» счетами. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Интернет-мошенничество, Дроп, Заливщик, Дроповод-нальщик, Кодер (программист), Поставщик трафика

Категорирование защищаемой информации [classifying information] —

Установление градаций важности защищаемой информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

См. также: Защищаемая информация

Качество услуги [quality of service] —

Обобщенный эффект услуги, который определяет, в какой степени потребитель удовлетворен ею. *[ОСТ 45.127-99 Система обеспечения*

информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].

См. также: Услуга

Квалифицированная электронная подпись (усиленная квалифицированная электронная подпись) [qualified electronic signature] —

Электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи: 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи;

и двум дополнительным признакам:

1) ключ проверки подписи электронной указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ. Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

4) Квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены) *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011].*

Выше: Электронная подпись.

См. также: Владелец сертификата ключа проверки электронной подписи, Квалифицированный сертификат ключа проверки электронной подписи, Неквалифицированная электронная подпись (усиленная неквалифицированная электронная подпись), Простая электронная подпись, Электронный документ.

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) —

Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. Квалифицированный сертификат ключа проверки электронной подписи подлежит созданию с использованием средств аккредитованного удостоверяющего центра. Квалифицированный сертификат должен содержать следующую информацию:

1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;

2) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата - для физического лица либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для юридического лица;

3) страховой номер индивидуального лицевого счета владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица;

4) ключ проверки электронной подписи;

5) наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом;

6) наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра;

7) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);

8) иная информация о владельце квалифицированного сертификата (по требованию заявителя). *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Сертификат ключа проверки электронной подписи

Квантовая криптографическая система [quantum cryptographic system] —

Криптографическая система, использующая квантовые каналы связи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая система

Квантовая криптография [quantum cryptography] —

Раздел криптографии, посвященный применению методов квантовой физики для синтеза и анализа криптографических систем. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптография

Квантовое распределение ключей [quantum key distribution] —

Процедура распределения секретных ключей, реализуемая с помощью квантовых криптографических протоколов и квантовых каналов связи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Квантовый криптографический протокол, Протокол распределения ключей.

Квантовый генератор псевдослучайных последовательностей [quantum pseudorandom generator] —

Генератор псевдослучайных последовательностей, основанный на использовании квантовых эффектов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Квантовый криптоанализ [quantum cryptanalysis] —

Криптографический анализ, основанный на применении алгоритмов квантовых вычислений. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптоанализ

Квантовый криптографический протокол [quantum cryptographic protocol] —

Криптографический протокол, использующий квантовый канал связи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический протокол

Кви про кво [quid pro quo] —

1. Злоумышленник может позвонить по случайному номеру в компанию и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» вводит команды, которые позволяют хакеру запустить вредоносное программное обеспечение. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. В английском языке это выражение обычно используется в значении «услуга за услугу». Данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону или электронной почте. Зачастую злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на

рабочем месте сотрудника и предлагает помощь в их устранении. В процессе «решения» технических проблем, злоумышленник вынуждает цель атаки совершать действия, позволяющие атакующему запускать команды или устанавливать различное программное обеспечение на компьютере «жертвы». *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Социальная инженерия

Кейлоггер [keylogger] —

Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д.

Дополнительно могут делаться периодические снимки экрана (а в некоторых случаях — даже видеозапись экрана) и копироваться данные из буфера обмена.

Несанкционированное применение кейлоггеров (в том числе аппаратных или программных продуктов, включающих в себя кейлоггер в качестве модуля) позволяет злоумышленнику:

- перехватывать чужую информацию, набираемую пользователем на клавиатуре;
- получить несанкционированный доступ к логинам и паролям доступа в различные системы, включая системы типа «банк-клиент»;
- получить несанкционированный доступ к системам криптографической защиты информации пользователя компьютера — парольным фразам;
- получить несанкционированный доступ к авторизационным данным кредитных карточек. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Вредоносное программное обеспечение

См. также: Руткит

Кибернетическое пространство [cyberspase] —

Обобщенный термин для обозначения всей совокупности взаимосвязанных компьютерных сетей, по которым передается цифровая информация. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Компьютерная сеть

Киберпреступность [cyber cryme] —

Действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Компьютерная атака, Компьютерная безопасность, Компьютерное преступление

Кибертерроризм [cyber terrorism] —

Действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных

общественно опасных последствий, если они совершенны с целью нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угрозы совершения указанных действий в тех же целях. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

Син.: Терроризм в информационном пространстве

См. также: Международный информационный терроризм

Класс защищенности автоматизированной системы —

Определенная совокупность требований по защите информации, предъявляемых к автоматизированной системе. *[ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

См. также: Автоматизированная система

Класс защищенности средств вычислительной техники (автоматизированной системы) [protection class of computer system] **—**

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Средства вычислительной техники

Классификация информационных активов —

Разделение существующих информационных активов организации банковской системы Российской Федерации по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств информационной безопасности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Информационный актив

Классификация методов защиты информации —

Деление методов защиты информации по направлениям на основе общности однородных признаков. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Методы защиты информации

Классы механизмов защиты —

Все механизмы защиты относятся к одному из перекрывающихся классов: предотвращение, обнаружение, восстановление. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ключ [key] **—**

Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Ниже: Закрытый ключ, Ключ зашифрования, Ключ подписи, Ключ проверки подписи, Ключ проверки электронной подписи, Ключ расшифрования, Ключ шифрования данных, Ключ электронной подписи, Открытый ключ, Разовый ключ, Сеансовый ключ, Секретный ключ.

Син.: Ключ (криптосистемы).

См. также: Время жизни ключа, Жизненный цикл ключа.

Ключ (криптосистемы) [key (of a cryptosystem)] —

1. Последовательность символов, управляющая операциями шифрования и дешифрования. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

3. Изменяемый элемент (параметр), каждому значению которого однозначно соответствует одно из отображений, реализуемых криптосистемой. Все возможные значения ключа составляют множество ключевое криптосистемы. Ключи могут быть составными, т. е. содержать несколько частей, обеспечивающих различные функции криптосистемы. Например, при реализации алгоритма шифрования электронной схемой в качестве ключей могут использоваться начальные состояния элементов памяти схемы, функциональные узлы и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Ключ.

См. также: Ключевой загрузчик.

Ключ зашифрования [enciphering key] —

Ключ, используемый при зашифровании. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ

См. также: Ключ расшифрования

Ключ подписи [signature key] —

Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита*

информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013].

Выше: Ключ.

Син.: Ключ электронной подписи.

См. также: Ключ проверки подписи, Процесс формирования подписи.

Ключ проверки подписи [verification key] —

Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

Выше: Ключ.

Син.: Ключ проверки электронной подписи.

См. также: Ключ подписи.

Ключ проверки электронной подписи [signature verification data] —

Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Ключ.

Син.: Ключ проверки подписи.

См. также: Ключ электронной подписи.

Ключ расшифрования [decryption key] —

Ключ, используемый при расшифровании. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ.

См. также: Ключ зашифрования.

Ключ шифрования данных [data encryption key] —

Элемент составного ключа, предназначенный для шифрования данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ

Ключ шифрования ключей [Key Enciphering Key (KEK)] —

Элемент составного ключа, используемый для шифрования разовых ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ.

См. также: Разовый ключ.

Ключ электронной подписи [signature creation data] —

Уникальная последовательность символов, предназначенная для создания электронной подписи. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Ключ.

Син.: Ключ подписи.

См. также: Ключ проверки электронной подписи, Процесс формирования подписи, Электронная подпись.

Ключевая последовательность [key stream] —

В поточных шифрсистемах — управляющая последовательность, однозначно определяющая в каждом такте выбор функции зашифрования для зашифрования очередного знака открытого текста. Иногда термин ключевая последовательность используется в качестве синонима гаммы в шифре гаммирования. [Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].

Выше: Управляющая последовательность.

См. также: Гамма (шифра).

Ключевая система [key system] —

Состоит из ключевого множества (криптосистемы) и двух подсистем: системы установки ключей и системы управления ключами. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система идентификации, Система имитозащиты, Система цифровой подписи.

Ниже: Ключевое множество (криптосистемы), Система установки ключей, Система управления ключами.

Ключевая система асимметричной шифрсистемы [key system of a public key cryptosystem] —

Ключевая система, основанная на использовании каждым участником пары, состоящей из открытого ключа и секретного ключа. Такие системы облегчают реализацию многих ключевых протоколов по сравнению с симметричными шифрсистемами. Вместе с тем, для обеспечения взаимного доверия между пользователями требуется дополнительная система, называемая инфраструктурой открытых ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Инфраструктура открытых ключей

См. также: Ключевая система, Ключевая система симметричной шифрсистемы

Ключевая система информационной инфраструктуры —

См. Критически важная система информационной инфраструктуры.

Ключевая система симметричной шифрсистемы [key system of a secret key cryptosystem] —

Ключевая система, основанная на использовании только секретных ключей, что исключает необходимость механизмов доверия, свойственных асимметричным шифрсистемам,но вместе с тем, затрудняет реализацию ряда протоколов жизненного цикла ключей (например, распределения ключей). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Ключевая система, Ключевая система асимметричной шифрсистемы.

Ключевое множество (криптосистемы) [key set (of a cryptosystem)] —

Множество всех возможных значений ключа криптосистемы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключевая система.

См. также: Криптопровайдер.

Ключевой загрузчик [key gun] —

Устройство для безопасной транспортировки и загрузки ключа (криптосистемы). Имеет физическую и логическую защиту от несанкционированного считывания. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Код аутентификации [authentication code] —

Вид алгоритма имитозащищающего кодирования информации. Как правило, код аутентификации сопоставляет сообщению его код аутентичности сообщения. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения. К коду аутентификации предъявляются требования: невозможность вычисления кода аутентичности для заданного сообщения без знания ключа; невозможность подбора для одного или нескольких сообщений с известными значениями кода аутентичности другого сообщения с известным значением кода аутентичности без знания ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Алгоритм имитозащищающего кодирования.

См. также: Код аутентичности сообщения, Криптографическая хеш-функция, задаваемая ключом.

Код аутентичности сообщения [message authentication code, seal, integrity check value] —

В протоколах аутентификации сообщений с доверяющими друг другу участниками — специальный набор символов, добавляемый к сообщению и предназначенный для обеспечения его целостности и аутентификации источника данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Аутентификация сообщения, Аутентификация сторон, Имитовставка, Код аутентификации, Режим выработки кода аутентичности сообщения.

Кодер (программист) —

1. Программист, специализирующийся на кодировании — написании исходного кода по заданным спецификациям. *[Свободная энциклопедия. Википедия www.wikipedia.org, русский язык.]*

2. Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества; обозначает участника, который, пишет троянские и др. вредоносные программы

и продает их на закрытых форумах для «своих». *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Интернет-мошенничество, Дроп, Заливщик, Дроповод-нальщик, Кардселлер, Поставщик трафика.

Коллективный (групповой) доступ [shared access] —

Совместное использование вычислительной системы двумя или более пользователями в пакетном или интерактивном режимах. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Доступ

Коллизия [collision, existential collision] —

Для хеш-функции h — такая пара значений x, y ее аргумента, что x y и h(x) = h(y). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Коммерческая тайна —

Режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. *[Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]*.

Выше: Сведения конфиденциального характера.

Ниже: Банковская тайна, Тайна страхования.

См. также: Информация, составляющая коммерческую тайну, Режим коммерческой тайны, Ценная информация.

Коммуникационная сложность (протокола) [communication complexity] —

Функция, выражающая зависимость максимального количества битов информации, пересылаемых в процессе выполнения распределенного алгоритма от длины записи исходных данных. Коммуникационная сложность — показатель эффективности реализации криптографических протоколов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Временная сложность алгоритма, Емкостная сложность алгоритма, Практическая стойкость (криптосистемы).

Коммуникационный канал —

Совокупность носителей информации, доставляющих сообщение от источника к приемнику. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Выше: Канал.

Коммутаторный ключ [commutation key] —

Ключ, являющийся подстановкой степени n или бесповторной выборкой размера m из n элементов, m < n. Например, в шифре замены простой ключ

представляет собой подстановку на множестве блоков текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Простой шифр замены.

Комплекс БР ИББС —

Взаимоувязанная совокупность документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Комплекс средств автоматизации автоматизированной банковской системы —

Совокупность всех компонентов автоматизированной банковской системы организации банковской системы Российской Федерации, за исключением людей. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Автоматизированная банковская система.

Комплекс средств защиты [trusted computing base] —

1. Совокупность всех средств защиты. *[ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Введен в действие: 01.01.1996]*.

2. Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Защита от несанкционированного доступа (Защита от НСД)

Комплекс технического контроля —

Совокупность средств измерения, регистрации, обработки результатов контроля и средств управления ими, конструктивно и функционально связанных и совместно используемых для комплексного технического контроля. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Метод контроля, Система контроля.

Комплексная защита информации —

Реализация требований по защите от несанкционированного доступа к информации, от утечки по техническим каналам, от возможно внедренных специальных электронных устройств и программ — ”вирусов”. *[Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в*

автоматизированных системах и средствах вычислительной техники» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)].

Выше: Защита информации.

См. также: Техническая защита информации, Правовая защита информации, Физическая (непосредственная) защита информации, Организационная защита информации, Несанкционированный доступ к информации, Утечка информации по техническому каналу, Антивирусная защита.

Комплексный технический контроль —

Выявление достаточности и эффективности мероприятий по противодействию техническим средствам разведки иностранных государств (противника), а также проверки выполнения установленных норм и требований по радиоэлектронной защите своих радиоэлектронных систем и средств. Различают радио, фотографический, визуально-оптический, телевизионный, радиолокационный, инфракрасный, химический, акустический, гидроакустический, радиотепловой контроль, контроль лазерных излучений и контроль эффективности защиты информации от ее утечки при эксплуатации технических средств передачи и обработки информации. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Контроль эффективности защиты информации.

Компонент [component] —

Наименьшая выбираемая совокупность элементов, которая может быть включена в профиль защиты, задание по безопасности или пакет. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Задание по безопасности, Профиль защиты, Пакет, Элемент

Компрометация [compromise] —

Утеря критичной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т. д.). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Критическая информация, Неавторизованный доступ.

Компрометация абонента [compromise of a party] —

Факт ознакомления противника и/или нарушителя с секретными ключами абонента защищенной сети связи (законного пользователя, участника (протокола)). Может иметь явный или тайный характер. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Компрометация криптографических ключей.

Компрометация криптографических ключей [cryptographic key disclosure] —

Событие, в результате которого возможно использование ключей неуполномоченными лицами или процессами. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Компрометация абонента, Скомпрометированный ключ.

Компьютер [computer] —

Функциональный блок, который может выполнять соответствующие вычисления, включая числовые арифметические операции и логические операции без вмешательства человека.

Примечание 1. Компьютер может состоять из одного блока или из многих соединенных блоков.

Примечание 2. В английском языке термин «компьютер», обычно, относится к цифровому компьютеру. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Компьютеризация [computerization] —

Автоматизация каких-либо процессов в любой области деятельности человека за счет применения вычислительных машин. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Компьютерная атака [computer attack] —

1. Целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

2. Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

Выше: Атака.

См. также: Вредоносное программное обеспечение, Киберпреступность, Компьютерный вирус, Хакер.

Компьютерная безопасность [computer security] —

Область компьютерных технологий, связанная с информационной безопасностью компьютеров и компьютерных сетей. Концентрируется на обеспечении доступности и корректности выполнения операций компьютерной системы безотносительно к хранимой или обрабатываемой в ней информации. Предполагает защищенность компьютерных ресурсов, безопасность архитектуры, разработки. Непосредственно связана с безопасностью разработки, информационных технологий, компьютерных сетей, автоматизированных, информационно-телекоммуникационных систем и т. п. Понятийная сфера компьютерной безопасности затрагивает такие дисциплины, как этика, анализ рисков, компьютерные преступления, предупреждение,

обнаружение и лечение компьютерных атак, обнаружение вторжений, идентичность и анонимность в киберпространстве. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Безопасность.

Син.: Безопасность компьютерных систем.

См. также: Безопасность автоматизированной компьютерной системы, Безопасность информационной технологии, Безопасность информационной сети, Безопасность информационно-телекоммуникационных технологий (Безопасность ИТТ), Киберпреступность, Компьютерная атака, Компьютерная криптография, Компьютерное преступление.

Компьютерная информация [electronic data] —

Информация на машинном носителе, в электронно-вычислительной машине, системе электронно-вычислительных машин или их сети. *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

Выше: Информация.

См. также: Документированная информация, Цифровая информация.

Компьютерная криптография [computer cryptography] —

Общее название области криптографических исследований, связанной с применением криптографии для обеспечения компьютерной безопасности. Изучает особенности реализации криптографических систем в операционных системах, компьютерных сетях, системах управления базами данных и т. п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптография.

См. также: Компьютерная безопасность.

Компьютерная сеть [computer network] —

1. Сеть, в узлах которой содержатся компьютеры и оборудование коммуникации данных. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

3. Комплекс компьютеров, вспомогательного оборудования, каналов связи и специального программного обеспечения для передачи данных между элементами сети.

В зависимости от задач, типа оборудования и линий связи вычислительные сети разделяются на локальные, корпоративные, территориальные и глобальные сети.

Сети создаются для более полного использования ресурсов или их перераспределения, для быстрой и автоматической связи с передачей больших объемов данных. Ресурсы бывают как вычислительные и технические (например, задача решается на нескольких компьютерах, или несколькими компьютерами используется один принтер), так и информационные (например, абоненты сети могут пользоваться одной базой данных). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Сеть.

Ниже: Виртуальная частная сеть, Локальная вычислительная сеть, Одноранговая сеть.

Син.: Вычислительная сеть.

См. также: Кибернетическое пространство.

Компьютерная система [computer system] —

Обобщенное название для компьютера или компьютерной сети. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Защита компьютерной сети, Компьютерная безопасность

Компьютерное преступление [computer crime] —

1. Обобщенный термин для обозначения уголовно наказуемых деяний, квалифицируемых как преступления в сфере компьютерной информации (глава 28 УК РФ), мошенничество в сфере компьютерной информации (Глава 21, Статья 159.6 УК РФ), а также другие виды преступлений, включая, шантаж, вымогательство и др., при совершении которых использование компьютера было существенным. *[Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изменениями на 5 мая 2014 года) (редакция, действующая с 16 мая 2014 года). Введен в действие 01.01.1997]*.

2. Преступление, совершенное с помощью или при непосредственном использовании системы обработки данных или сети. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Ниже: Преступления в сфере компьютерной информации, Мошенничество в сфере компьютерной информации.

См. также: Киберпреступность, Компьютерная безопасность.

Компьютерный вирус [computer virus] —

1. Вредоносная программа, способная создавать вредоносные программы и (или) свои копии. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*

2. Вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. [*ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

3. Программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Введен в действие: 01.07.1999]*.

4. Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Примечание. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

5. Родовое наименование большого числа достаточно разнообразных программ вредоносных, главной отличительной чертой которых является способность к «саморазмножению» или «самораспространению» при определенных условиях. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

6. К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от сетевых червей компьютерные вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия компьютерного вируса попадает на удалённый компьютер только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съёмный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вирусом вложением.

Некоторые компьютерные вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например backdoor-процедуру или троянскую компоненту уничтожения информации на диске. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

7. Программы или фрагменты программного кода, которые, попав на компьютер, могут вопреки воле пользователя выполнять различные операции на этом компьютере — создавать или удалять объекты, модифицировать файлы данных или программные файлы, осуществлять действия по собственному

распространению по локальным вычислительным сетям или по сети Интернет. Модификация программных файлов, файлов данных или загрузочных секторов дисков таким образом, что последние сами становятся носителями вирусного кода и в свою очередь могут осуществлять вышеперечисленные операции, называется заражением (инфицированием) и является важнейшей функцией компьютерных вирусов. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

8. Вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Ниже: Анти-антивирусный вирус, Антивирусный вирус, Дроппер, Загрузочный вирус, Зомби, Логическая бомба, Макровирусы, Почтовая бомба, Троян, Троянский конь, Полиморфные (зашифрованные) вирусы, Сетевой червь.

См. также: Вредоносное программное обеспечение, Интернет-мошенничество, Социальная инженерия.

Компьютерный ресурс [computer resource] —

Любой компонент системы обработки данных, необходимый для выполнения требуемых операций.

Прим.: В качестве примеров можно привести устройство хранения, устройство ввода-вывода, один или несколько блоков обработки, данные, файлы и программы. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Син: Ресурс системы обработки информации.

Контрагент —

Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию. *[Федеральный закон от 29.07.2004 N 98-ФЗ “О коммерческой тайне” (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]*.

См. также: Передача информации, составляющей коммерческую тайну, Обладатель информации, составляющей коммерческую тайну.

Контрафакт —

В случае, когда изготовление, распространение или иное использование, а также импорт, перевозка или хранение материальных носителей, в которых выражены результат интеллектуальной деятельности или средство индивидуализации, приводят к нарушению исключительного права на такой результат или на такое средство, такие материальные носители считаются контрафактными и по решению суда подлежат изъятию из оборота и уничтожению без какой бы то ни было компенсации, если иные последствия не

предусмотрены Гражданским Кодексом РФ. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Интеллектуальные права, Использование (интеллектуального) произведения, Патентные права.

Контролирование риска [risk control] —

Мера, которая модифицирует (изменяет) риск. Примечание 1. Контролирование риска может включать любой процесс, политику, методику, практику или другие действия, модифицирующие риск. Примечание 2. Контролирование риска может не всегда приводить к желаемому или ожидаемому эффекту. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Мониторинг (в области риск-менеджмента)

Контролируемая зона [controllable territory] —

1. Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств. *[ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. Введен в действие: 01.07.2008]*.

2. Пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств.

Примечание. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения); ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения. *[ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

См. также: Система контроля и управления доступом (СКУД), Физическая охрана средств вычислительной техники.

Контроль доступа [access control] —

Обеспечение того, чтобы доступ к активам был санкционирован и ограничен в соответствии с требованиями коммерческой тайны и безопасности. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

Ниже: Контроль доступа в информационной системе.

Син.: Управление доступом.

См. также: Доступ, Контролируемая зона, Механизм (средство) разграничения доступа, Система контроля и управления доступом (СКУД), Осведомленность об идентификационных данных.

Контроль доступа в информационной системе [access control] —

Проверка выполнения субъектами доступа установленных правил разграничения доступа в информационной системе. [*Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Контроль доступа.

См. также: Правила доступа, Система разграничения доступа.

Контроль обеспечения информационной безопасности организации —

Проверка соответствия обеспечения информационной безопасности в организации, наличия и содержания документов требованиям нормативных документов, технической, правовой организационно-распорядительной документации в области информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Син.: Мониторинг информационной безопасности организации.

См. также: Лицо, ответственное за информационную безопасность.

Контроль приложений с запретом по умолчанию [Application Control Default Deny] —

Технология обеспечения безопасности корпоративной сети — контроль приложений (Application Control), дополненная сценарием Default Deny («Запрет по умолчанию»), при котором пользователи могут запускать только проверенные и авторизованные программы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Управление приложениями.

Контроль средств защиты [security audit] —

См. Аудит (безопасности).

Контроль эффективности защиты информации —

1. Проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

2. Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

См. также: Комплексный технический контроль, Норма эффективности защиты информации, Средство контроля эффективности защиты информации.

Контрольная сумма [checksum] —

Некоторое значение, рассчитанное из последовательности данных путём применения определённого алгоритма, используемое для проверки

правильности передачи данных (для исключения влияния каких-либо помех при передаче).

С точки зрения математики КС является хеш-функцией, используемой для вычисления контрольного кода — небольшого количества бит внутри большого блока данных, например сетевого пакета или блока компьютерного файла, применяемого для обнаружения ошибок при передаче или хранении информации. Результат вычисления КС добавляется в конец блока данных непосредственно перед началом передачи или сохранения данных на каком-либо носителе информации. Впоследствии он проверяется для подтверждения её целостности. Популярность КС обусловлена тем, что подобная проверка просто реализуема в двоичном цифровом оборудовании, легко анализируется и хорошо подходит для обнаружения общих ошибок, вызванных наличием шума в каналах передачи данных.

Некоторые виды контрольных сумм:

- Циклический избыточный код (в частности, CRC8, CRC16, CRC32) применяется для проверки целостности передачи данных. Программы-архиваторы включают CRC исходных данных в созданный архив для того, чтобы получающий мог удостовериться в корректности полученных данных. Прост в реализации, при этом обеспечивает низкую вероятность возникновения коллизии, когда разные данные имеют одну и ту же контрольную сумму. Для вычисления используются побитовый сдвиг и исключающее ИЛИ.

- MD5 и другие криптографические хеш-функции используются, например, для подтверждения целостности и подлинности передаваемых данных.

- Под названием «контрольное число» входит в состав номеров товаров и различных документов. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Син.: Криптографическое контрольное значение.

См. также: Хеш-значение.

Контрольные испытания [check test] —

Испытания, проводимые для контроля качества объекта. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

Выше: Испытания.

См. также: Аттестационные испытания, Сертификационные испытания, Типовые испытания.

Конфигурация [configuration] —

Способ, с помощью которого хардвер и софтвер или система обработки данных организуются и объединяются. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Конфигурация системы обработки информации, Список конфигурации, Система управления конфигурацией, Управление конфигурацией.

Конфигурация системы обработки информации [configuration] —

Совокупность функциональных частей системы обработки информации и связей между ними, обусловленная основными техническими характеристиками этих функциональных частей, а также требованиями решаемых задач. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Конфигурация

Конфиденциальная информация —

1. Информация, требующая защиты. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

2. Документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

3. Служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной (промышленной) тайне, государственной службе и других законодательных актов; сведения, не отнесенные к государственной тайне, доступ к которым ограничивается в соответствии с законодательством Российской Федерации. К ней относятся сведения конфиденциального характера. Сведения, не подлежащие отнесению к конфиденциальной информации:

• сведения, не подлежащие ограничению в доступе к ним в соответствии с законодательством РФ;

• сведения, подлежащие распространению в СМИ *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Выше: Информация ограниченного доступа.

См. также: Доступ к конфиденциальной информации, Сведения конфиденциального характера, Конфиденциальный документ.

Конфиденциальность [confidentiality] —

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

2. Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

3.Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

4. Свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

5. Состояние информации (ресурсов автоматизированной информационной системы), при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Безопасность информации (данных), Информационная безопасность, Доступность, Целостность, Конфиденциальность информации.

Конфиденциальность информации [privacy, confidentiality] —

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Означает, что информация предназначена только определенному кругу лиц и должна храниться в тайне от всех остальных *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Конфиденциальность, Доступность информации, Целостность информации.

Конфиденциальность информационных активов [information assets confidentiality] —

Свойство информационной безопасности организации банковской системы Российской Федерации, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Доступность информационных активов, Целостность информационных активов, Информационный актив.

Конфиденциальность потока трафика —

См. Конфиденциальность трафика.

Конфиденциальность трафика [traffic (flaw) confidentiality] —

1. Услуга конфиденциальности, предназначенная для защиты от анализа трафика. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Свойство, характеризующее защищенность системы связи от получения противником и/или нарушителем информации о передаваемых в системе данных и/или функционировании системы в целом путем анализа трафика. Защита от анализа трафика обеспечивается путем сокрытия идентификаторов и адресов отправителя и получателя, длин пакетов, интенсивности передач и т. п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Конфиденциальность потока трафика.

См. также: Анализ трафика.

Конфиденциальный документ —

Документ ограниченного доступа на любом носителе, содержащий конфиденциальную информацию. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Документ.

См. также: Конфиденциальная информация.

Конфиденциальный набор ключей [validator] —

Комплект, состоящий из секретного ключа схемы цифровой подписи, соответствующего открытого ключа и его сертификата ключа, используемый в автономных системах электронных платежей с электронными бумажниками. Конфиденциальный набор ключей выдается специальным органом (центром выдачи конфиденциального набора ключей), создаваемым для этих целей, вслепую так, что впоследствии центр выдачи конфиденциального набора ключей не сможет идентифицировать клиента, которому был выдан данный конфиденциальный набор ключей. Тем самым обеспечивается неотслеживаемость клиентов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Автономная система электронных платежей

Конфикер [Conficker] —

Вредоносная программа, создающая bot-сети. Представляет собой мощную высокотехнологичную платформу для решения различных задач, в том числе может использоваться с целью сбора банковской информации. Поразил десятки миллионов компьютеров во всем мире. Распространяется с 2008 года с загружаемых носителей, по электронной почте, через социальные сети по технологии сетевого «червя». В системе червь хранится в виде dll-файла со случайным именем. Отключает ряд служб: автоматическое обновление Windows, Windows Security Center, Windows Defender и Windows Error Reporting, а также блокирует доступ к сайтам ряда производителей антивирусов. Периодически червь случайным образом генерирует список сайтов, к которым обращается для получения исполняемого кода. При

получении с сайта исполняемого файла червь сверяет электронно-цифровую подпись и, если она совпала, исполняет файл. Кроме того, червь реализует P2P-механизм обмена обновлениями, что позволяет ему рассылать обновления удаленным копиям, минуя управляющий сервер. Также известен как Downup, Downadup и Kido *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Сетевой червь.

См. также: Антибот, Бот-сеть.

Концепция диспетчера доступа [reference monitor concept] —

1. Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

2. Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

Син.: Концепция монитора ссылок.

См. также: Диспетчер доступа.

Концепция защиты информации —

Система взглядов и общих технических требований по защите информации. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

См. также: Защита информации, Требование по защите информации.

Концепция монитора ссылок —

См. Концепция диспетчера доступа.

Корпоративная информационная система [enterprise information system] —

Информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Син.: Корпоративная система.

См. также: Информационная система общего пользования, Участники электронного взаимодействия.

Корпоративная политика информационной безопасности [corporate information security policy] —

Документ, отражающий позицию руководства по обеспечению информационной безопасности в соответствии с требованиями основной деятельности организации и правовыми и регулирующими нормами.

Примечание. Документ, описывающий высокоуровневые требования информационной безопасности, которые должны соблюдаться в организации. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и*

средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012].

См. также: Обеспечение информационной безопасности организации.

Корпоративная система —

См. Корпоративная информационная система.

Корректирующие действия [corrective action] —

Мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупредить их повторное возникновение. *[ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен в действие: 01.02.2008]*.

Син. Корректирующие меры.

См. также: Предупреждающие действия.

Корректирующие меры [corrective action] —

Меры по устранению причин несоответствий требованиям СУИБ в целях предотвращения их повторений. *[BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements Дата принятия: 14.10.2005 Перевод: ООО «GlobalTrust Solutions»]*.

Син. Корректирующие действия.

См. также: Превентивные меры.

Корреляционная атака [correlation attack] —

Атака на криптосистему, основанная на корреляционном методе. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

См. также: Корреляционный метод.

Корреляционный метод [correlation cryptanalysis] —

Метод криптографического анализа, использующий статистические зависимости между внутренними состояниями криптосистемы (как автомата) и значениями входной и выходной последовательностей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

См. также: Корреляционная атака.

Корреляция функций [correlation of functions] —

См. Коэффициент корреляции функций.

Крипто API [crypto API (application programming interface)] —

Криптографический интерфейс прикладного программирования, определяющий порядок обращения прикладных программ к библиотеке функций/программ, реализующих элементарные криптографические функции и криптографические операции. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптографическая функция.

Криптоанализ [cryptanalysis] —

Анализ криптографической системы и/или ее входов и выходов с целью получения конфиденциальных переменных и/или чувствительных данных, включая открытый текст. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Криптография.

Ниже: Квантовый криптоанализ.

См. также: Криптоаналитик, Метод криптографического анализа (криптоанализа), Правило Керкгоффса, Предположения криптоанализа.

Криптоаналитик [cryptanalyst] —

Специалист, занимающийся анализом криптографическим криптосистем. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптоанализ.

Криптограмма [cryptogram] —

Шифрованное сообщение, оформленное по действующим правилам пользования системой шифрования. Содержит, кроме шифрованного текста, адрес, грифы срочности и др. служебную информацию. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Шифрованное сообщение.

Криптографическая защита [cryptographic protection] —

Защита данных при помощи криптографического преобразования данных. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

См. также: Защита данных, Криптографическая операция, Криптографические средства, Криптографическая защита информации, Шифровальные (криптографические) средства (средства криптографической защиты информации).

Криптографическая защита информации [cryptographic protection of information] —

Защита информации с помощью ее криптографического преобразования. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Защита информации, Криптографическая защита, Криптографическая операция.

Криптографическая операция [cryptographic operation] —

Термин, принятый в компьютерной криптографии и введенный в стандарте ISO/IEC15408-99 для обозначения криптографических алгоритмов и криптографических протоколов. Под криптографической операцией понимаются: зашифрование и расшифрование данных или ключей, алгоритм формирования цифровой подписи, алгоритм проверки цифровой подписи, вычисление кода аутентичности сообщения, вычисление значения хеш-функции, протокол выработки ключей и др. В более ранних стандартах

использовался термин криптографический механизм. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптографический алгоритм, Криптографический протокол.

Криптографическая система [cryptographic system (cryptosystem)] —

Система обеспечения безопасности информации криптографическими методами в части конфиденциальности, целостности, аутентификации, невозможности отказа и неотслеживаемости. В качестве подсистем может включать системы шифрования, системы идентификации, системы имитозащиты, системы цифровой подписи и др., а также ключевую систему, обеспечивающую работу остальных систем. В основе выбора и построения криптографической системы лежит условие обеспечения криптографической стойкости. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Квантовая криптографическая система, Система шифрования, Система идентификации, Система имитозащиты, Система цифровой подписи, Пороговая криптографическая система, Система идентификации.

См. также: Криптографическая стойкость, Криптографическая функция, Криптографические средства, Протокол распределения ключей.

Криптографическая стойкость [cryptographic security] —

Фундаментальное понятие криптографии — свойство криптосистемы (криптопротокола), характеризующее ее (его) способность противостоять атакам противника и/или нарушителя, как правило, имеющим целью получить секретный ключ или открытое сообщение. Развиваются два основных подхода к определению и оценке стойкости — теоретическая стойкость и практическая стойкость. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Теоретическая стойкость (криптосистемы), Практическая стойкость (криптосистемы).

См. также: Атака на криптосистему, Метод криптографического анализа (криптоанализа), Модель открытого текста, Открытое сообщение, Слабый ключ.

Криптографическая функция [cryptographic function] —

Функция, необходимая для реализации криптографической системы. К таким функциям относятся: генерация ключей, генерация псевдослучайных последовательностей, функция шифрования, вычисление и проверка значений кода аутентичности сообщения и цифровой подписи, вычисление значения хеш-функции и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Функция шифрования.

См. также: Криптографическая система, Криптографические средства.

Криптографическая хеш-функция [cryptographic hash function] —

Хеш-функция, сочетающая в себе свойства односторонней хеш-функции, хеш-функции с трудно обнаружимыми вторыми прообразами и хеш-функции с трудно обнаружимыми коллизиями. Особо выделяют криптографические хеш-

функции, задаваемые ключом, имеющие другое содержание. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Криптографическая хеш-функция, задаваемая ключом.

См. также: Алгоритм хеширования, Коллизия, Односторонняя хеш-функция, Хеш-функция с трудно обнаружимыми вторыми прообразами, Хеш-функция с трудно обнаружимыми коллизиями.

Криптографическая хеш-функция, задаваемая ключом [cryptographic hash function with key] —

Криптографическая хеш-функция, реализуемая алгоритмом имитозащищающего кодирования, или кодом аутентификации, и предназначенная для обеспечения невозможности для противника и/или нарушителя создавать новые или модифицировать передаваемые (или хранимые) сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая хеш-функция.

См. также: Код аутентификации, Алгоритм имитозащищающего кодирования.

Криптографически сильная псевдослучайная последовательность [cryptographically strong pseudorandom sequence] —

Псевдослучайная последовательность, вырабатываемая криптографически сильным генератором псевдослучайных последовательностей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Псевдослучайная последовательность.

См. также: Криптографически сильный генератор псевдослучайных последовательностей.

Криптографически сильный генератор псевдослучайных последовательностей [cryptographically strong pseudorandom bit generator] —

Математическая модель генератора псевдослучайных последовательностей, выходом которого являются псевдослучайные последовательности, эффективно неотличимые (с полиномиальной сложностью) статистическими тестами от идеальных случайных последовательностей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптографически сильная псевдослучайная последовательность, Идеальная случайная последовательность.

Криптографические средства [cryptographic tools, cryptographic mechanisms] —

В широком смысле — средства обеспечения безопасности информации, использующие криптографические функции. В узком смысле — средства, реализованные в виде документов, механических, электромеханических, электронных технических устройств или программ, предназначенные для выполнения функций криптографической системы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Аппаратные криптографические средства, Встраиваемые криптографические средства, Криптографические средства физического и канального уровня, Криптографическое средство защиты информации, Наложенные криптографические средства, Штатные криптографические средства.

См. также: Криптографическая функция, Криптографическая защита, Шифровальные (криптографические) средства (средства криптографической защиты информации).

Криптографические средства выше прикладного уровня [above the application layer cryptographic mechanisms] —

Программные криптографические средства, реализаванные таким образом, что все данные заранее преобразуются так, чтобы они могли быть переданы непосредственно с помощью существующего протокола прикладного уровня, и чтобы при этом были реализованы необходимые службы и обеспечивался необходимый уровень безопасности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Программные криптографические средства.

Криптографические средства прикладного уровня [application layer cryptographic mechanisms] —

Программные криптографические средства, реализованные таким образом, что модули, выполняющие криптографические функции, расположены только на прикладном уровне и не требуют никаких модификаций для программных модулей и интерфейсов для более низких уровней. Это означает, что для обеспечения функций безопасности должны быть модифицированы как прикладные протоколы, так и сами прикладные программы, использующие эти протоколы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Программные криптографические средства.

Криптографические средства сетевого уровня [network layer cryptographic mechanisms] —

Программные криптографические средства, реализованные таким образом, что модули, выполняющие криптографические функции, расположены только на сетевом уровне без каких бы то ни было модификаций для программных модулей и интерфейсов для уровня канала передачи данных и прикладного уровня. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Программные криптографические средства.

Криптографические средства транспортного уровня [transport layer cryptographic mechanisms] —

Программные криптографические средства, реализованные таким образом, что модули, выполняющие криптографические функции, расположены на транспортном уровне, который осуществляет контроль доставки информации и контроль ее целостности. Такая реализация имеет целью усиление безопасности сетевого программного интерфейса с помощью

введения дополнительных возможностей, а также обеспечения возможности прикладным программам избирательно использовать эти дополнительные возможности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Программные криптографические средства.

Криптографические средства физического и канального уровня [physical and data layer cryptographic mechanisms] —

Криптографические аппаратные средства, осуществляющие шифрование трафика (соединения) на физическом или канальном уровне, исполненные в виде скремблеров, шифрующих модемов, специализированных канальных адаптеров и т.п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Скремблер.

См. также: Безопасность связи, Конфиденциальность трафика, Сетевой трафик.

Криптографические функции-сервисы безопасности (cryptographic service) —

Функции-сервисы безопасности, обеспечиваемые криптографическими средствами. К ним относятся: конфиденциальность, аутентификация, обеспечение целостности, невозможность отказа от ранее совершенных действий и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Программные криптографические средства.

Криптографический алгоритм [cryptographic algorithm] —

Алгоритм, реализующий вычисление одной из криптографических функций. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

См. также: Криптографическая операция, Криптографическая функция, Криптографическое преобразование.

Криптографический анализ —

См. Криптоанализ.

Криптографический примитив [cryptographic primitive] —

Функция (семейство функций), которая используется как составной элемент при построении криптосистем (криптографических протоколов) и обладает определенным криптографическим свойством. Примеры криптографических примитивов: односторонняя функция, хеш-функция, генератор псевдослучайных последовательностей, семейство псевдослучайных функций. Иногда криптографическим примитивом называют такие объекты, как цифровая подпись, электронные деньги, сертификат ключа и т. п., если они используются при построении криптографического протокола. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Хеш-функция, Семейство псевдослучайных функций, Цифровая подпись, Электронные деньги, Сертификат ключа.

См. также: Стойкость криптографического примитива.

Криптографический протокол [cryptographic protocol] —

Протокол, предназначенный для выполнения функций криптографической системы, в процессе выполнения которого участники используют криптографические алгоритмы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Групповой протокол, Квантовый криптографический протокол, Прикладной криптографический протокол, Примитивный криптографический протокол, Протокол аутентификации сообщений, Протокол разделения секрета, Протокол с арбитром.

См. также: Криптографическая операция, Криптографический алгоритм, Полнота (протокола), Участник(протокола), Цикл (раунд) (криптографического протокола).

Криптографический синтез [cryptosynthesis] —

Условно выделяемая часть криптографии (криптологии), связанная с разработкой криптографических систем (криптографических протоколов). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптография.

Криптографическое контрольное значение —

Информация, получаемая в результате выполнения криптографического преобразования блока данных.

Примечание - Контрольное значение может быть получено путем выполнения одного или нескольких шагов и является результатом математической функции ключа и блока данных. Оно обычно используется для проверки целостности блока данных. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Син.: Контрольная сумма.

Криптографическое (криптологическое) предположение [cryptographic assumption] —

Предположение о вычислительной сложности какой-либо математической задачи, на основе которого доказывается теоретико-сложностная стойкость криптосистем и криптографических протоколов. Примерами криптографического предположения являются предположения о существовании односторонних функций, функций с секретом, о вычислительной сложности задачи дискретного логарифмирования, задачи факторизации чисел целых. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Теоретико-сложностная стойкость.

Криптографическое преобразование —

Преобразование данных при помощи шифрования и (или) выработки имитовставки. *[ГОСТ 28147-89 Системы обработки информации. Защита*

криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990].

См. также: Криптографический алгоритм.

Криптографическое средство защиты информации [Cryptographic information protection facility] —

1. Средство защиты информации, реализующее алгоритмы криптографического преобразования информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Выше: Криптографические средства, Средство защиты информации.

Криптографическое устройство [cryptographic device] —

Аппаратное криптографическое средство, выполненное в виде отдельного устройства. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Аппаратные криптографические средства.

Криптография [cryptography] —

1. Дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого, предотвращения их не обнаруживаемой модификации и/или их несанкционированного использования.

Примечание. Криптография устанавливает методы, используемые при шифровании и дешифровании. Любое вторжение в криптографические принципы, средства или методы, представляет собой криптоанализ. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Область научных, прикладных, инженерно-технических исследований и практической деятельности, которая связана с разработкой криптографических средств защиты информации от угроз со стороны противника и/или нарушителя, а также анализом и обоснованием их криптографической стойкости. В настоящее время основными задачами криптографии являются обеспечение конфиденциальности, целостности, аутентификации, невозможности отказа, неотслеживаемости. В отличие от организационных и других способов защиты информации, под криптографическими понимаются такие, которые используют математические методы преобразования защищаемой информации. Криптография, с некоторой долей условности, делится на: криптосинтез и криптоанализ; криптография включает криптологию. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Криптосинтез, Криптоанализ, Криптология (математическая криптография), Квантовая криптография, Компьютерная криптография.

См. также: Криптографическая операция.

Криптология (математическая криптография) [cryptology (mathematical cryptography)] —

Отрасль криптографии, математики и математической кибернетики, изучающая математические модели систем криптографических. Так же, как и криптография, условно делится на две части: криптосинтез и криптоанализ. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптография.

См. также: Криптосинтез, Криптоанализ.

Криптомаршрутизатор [cryptorouter] —

Программное средство (маршрутизатор), осуществляющее туннелирование исходящих и входящих пакетов, а также зашифрование исходящих и расшифрование входящих пакетов. Множество закрытых маршрутов всех взаимодействующих криптомаршрутизаторов образует виртуальную частную сеть в общей сети. Информация, пересылаемая криптомаршрутизатором, зашифрована на ключах парной связи между соответствующими криптомаршрутизаторами. Обмен ключами по сети отсутствует. Для закрытия информации и топологии внутренних подсетей применяется принцип инкапсуляции, то есть вложения передаваемых пакетов в другие, со скрытием внутренних адресов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Виртуальная частная сеть, Туннелирование.

Криптопровайдер [cryptoprovider] —

Программное средство, обеспечивающее работу пользователя с ключевым множеством криптосистемы без получения непосредственного доступа к нему. Криптопровайдер должен соответствовать действующим стандартам, реализовывать алгоритмы шифрования, алгоритмы формирования цифровой подписи, алгоритмы проверки цифровой подписи, обеспечивая защиту ключевого множества криптосистемы от непреднамеренной или случайной компрометации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Ключевое множество (криптосистемы), Криптосервер.

Криптопротокол [cryptoprotocol] —

См. Криптографический протокол.

Криптосервер [cryptoserver] —

Особо выделенная в сети рабочая станция, на которой создана доверенная среда и локализовано хранение информации о ключах, и выполнение криптографических операций. Обращение к криптосерверу осуществляется посредством вызовов функций, реализованных в его программном обеспечении. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптопровайдер.

Криптосинтез [cryptosynthesis] —

См. Криптографический синтез.

Криптофильтр [cryptofilter] —

Устройство, осуществляющее автоматическое шифрование пакетов, имеющее ровно два интерфейса и не имеющее своих сетевых адресов. Для обеспечения нормальной работы криптофильтр должен содержать: список сетевых адресов подсетей, с которыми может осуществляться связь; матрицу ключей парной связи между подсетями; список сетевых адресов компьютеров внутренней подсети, доступных извне для генерации пакетов и формирования ответов маршрутизатору; сетевой адрес маршрутизатора, подключенного к внешнему интерфейсу. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Критерии оценки (аудита) информационной безопасности —

Совокупность требований в области информационной безопасности, определенных стандартом Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» или его частью. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Критерий аудита информационной безопасности организации.

Критерии риска [risk criteria] —

Признаки, в соответствии с которыми оценивают значимость риска.

Примечание 1. Критерии риска основываются на целях организации и внешней и внутренней ситуации (контекста).

Примечание 2. Критерии риска могут быть взяты из стандартов, законов, политик и других требований. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Критерии фильтрации —

Параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т.п. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Правила фильтрации.

Критерий аудита информационной безопасности организации —

Совокупность принципов, положений, требований и показателей действующих нормативных документов, относящихся к деятельности организации в области информационной безопасности.

Примечание - Критерии аудита информационной безопасности используют для сопоставления с ними свидетельств аудита информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Аудиторская проверка информационной безопасности в организации, Заключение по результатам аудита информационной безопасности (аудиторское заключение), Свидетельства (доказательства) аудита информационной безопасности организации, Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям.

Критерий качества функционирования автоматизированной системы в защищенном исполнении при испытаниях на устойчивость —

Совокупность свойств и параметров, характеризующих работоспособность автоматизированной системы в защищенном исполнении. *[ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. Введен в действие: 01.07.2008]*.

Критерий обеспечения информационной безопасности организации —

Показатель, на основании которого оценивается степень достижения цели (целей) информационной безопасности организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Обеспечение информационной безопасности организации, Цель информационной безопасности (организации).

Критическая информационная инфраструктура Российской Федерации —

Совокупность автоматизированных систем управления КВО и обеспечивающих их взаимодействие информационно- телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

См. также: Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры

Российской Федерации, Безопасность критической информационной инфраструктуры.

Критическая информация [classified information] —

Определенные факты относительно намерений, способностей и действий, жизненно необходимых для эффективного управления и деятельности критически важных структур, эффективного выполнения стоящих стратегических задач. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Критический, Компрометация, Критически важные структуры, Некритичная информация.

Критически важная система информационной инфраструктуры —

Информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление или информационное обеспечение критическим объектом или процессом, или используется для официального информирования общества и граждан, нарушение или прерывание функционирования которой (в результате деструктивных информационных воздействий, а также сбоев или отказов) может привести к чрезвычайной ситуации со значительными негативными последствиями. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Син. Ключевая система информационной инфраструктуры.

См. также: Информационно-телекоммуникационная система.

Критически важные объекты —

Объекты, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики страны, субъекта или административно-территориальной единицы или к существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях длительный период времени. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Син.: Критически важный объект информационной инфраструктуры (КВО), Критический объект.

Критически важные структуры [critical structures] —

Объекты, системы и институты государства, целенаправленное воздействие на информационные ресурсы которых может иметь последствия, прямо затрагивающие национальную безопасность (транспорт, энергоснабжение, кредитно-финансовая сфера, связь, органы государственного управления, система обороны, правоохранительные органы, стратегические информационные ресурсы, научные объекты и научно-технические разработки,

объекты повышенной технической и экологической опасности, органы ликвидации последствий стихийных бедствий и иных чрезвычайных ситуаций). *[Доклад Генерального секретаря ООН от 10 июня 2000г.]*.

См. также: Критическая информация, Национальная безопасность.

Критически важный объект информационной инфраструктуры (КВО) —

Объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

Син.: Критически важные объекты.

См. также: Автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации.

Критически важный объект инфраструктуры Российской Федерации —

Часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

См. также: Критически важный объект информационной инфраструктуры (КВО), Национальная безопасность.

Критический [critical] **—**

Качественная характеристика, используемая, чтобы подчеркнуть важность ресурса, процесса или функции, которые должны быть постоянно доступными и действующими или доступными и действующими с наиболее раннего возможного момента времени после инцидента, чрезвычайной ситуации или бедствия. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

Критический маршрут выполнения функциональных объектов —

Маршрут, при выполнении которого существует возможность неконтролируемого нарушения установленных правил обработки информационных объектов. *[Руководящий документ Гостехкомиссии России*

«Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)].

Выше: Маршрут выполнения функциональных объектов.

Критический объект —

Объект или процесс, нарушение непрерывности функционирования которого может нанести значительный ущерб. Примечание. Ущерб может быть нанесен имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, а также выражаться в причинении вреда жизни или здоровью граждан. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009].*

Син.: Критически важные объекты.

Критичный компонент (информационно-телекоммуникационной системы) —

Компонент информационно-телекоммуникационной системы, нарушение непрерывности функционирования которого может нанести значительный ущерб организации. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009].*

Лазейка [loophole] **—**

Тип вторжения, при котором логический объект системы изменяется таким образом, что он разрешает нарушителю произвести неполномочное воздействие либо на команду, либо на заранее определенное событие, либо на последовательность таких событий. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].*

Выше: Виды вторжений.

Латинский квадрат [latin square] **—**

Матрица размеров n n, у которой каждая строка и каждый столбец являются перестановкой элементов некоторого конечного алфавита из n элементов. В криптографии латинский квадрат используются, например, для задания функции зашифрования при гаммировании. [Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].

См. также: Гаммирование.

Линейная атака [linear attack] **—**

Атака на криптосистему, основанная на линейном методе. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Атака на криптосистему.

Лицензиат —

Юридическое лицо или индивидуальный предприниматель, имеющие лицензию. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

Ниже: Лицензиат в области защиты информации.

См. также: Лицензия, Соискатель лицензии.

Лицензиат в области защиты информации —

Сторона, получившая право на проведение работ в области защиты информации. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

Выше: Лицензиат.

Лицензионные требования —

Совокупность требований, которые установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства Российской Федерации и направлены на обеспечение достижения целей лицензирования. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

Лицензионный договор —

По лицензионному договору одна сторона - обладатель исключительного права на результат интеллектуальной деятельности или на средство индивидуализации (лицензиар) предоставляет или обязуется предоставить другой стороне (лицензиату) право использования такого результата или такого средства в предусмотренных договором пределах.

Лицензиат может использовать результат интеллектуальной деятельности или средство индивидуализации только в пределах тех прав и теми способами, которые предусмотрены лицензионным договором. Право использования результата интеллектуальной деятельности или средства индивидуализации, прямо не указанное в лицензионном договоре, не считается предоставленным лицензиату. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Лицензиат.

Лицензирование —

Деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса,

а также по предоставлению в установленном порядке информации по вопросам лицензирования. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

Ниже: Лицензирование в области защиты информации.

См. также: Лицензирующие органы, Лицензиат, Лицензионные требования, Лицензионный договор, Лицензируемый вид деятельности, Лицензия, Место осуществления отдельного вида деятельности, подлежащего лицензированию, Соискатель лицензии.

Лицензирование в области защиты информации —

1. Деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Деятельность, заключающаяся в передаче или в получении прав на проведение работ в области защиты информации. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

Выше: Лицензирование.

См. также: Лицензия в области защиты информации.

Лицензируемый вид деятельности —

Вид деятельности, на осуществление которого на территории Российской Федерации и на иных территориях, над которыми Российская Федерация осуществляет юрисдикцию в соответствии с законодательством Российской Федерации и нормами международного права, требуется получение лицензии в соответствии с настоящим Федеральным законом, в соответствии с федеральными законами, указанными в части 3 статьи 1 настоящего Федерального закона и регулирующими отношения в соответствующих сферах деятельности. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

См. также: Лицензирование, Место осуществления отдельного вида деятельности, подлежащего лицензированию.

Лицензирующие органы —

Уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, а в случае передачи осуществления полномочий Российской Федерации в области лицензирования органам государственной власти субъектов Российской Федерации органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных*

видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011].

См. также: Лицензирование.

Лицензия [license] —

Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

Ниже: Лицензия в области защиты информации.

См. также: Лицензиат.

Лицензия в области защиты информации —

Оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

Выше: Лицензия.

См. также: Лицензиат в области защиты информации.

Лицо, ответственное за информационную безопасность [information security officer] —

Лицо, отвечающее за внедрение и поддержку программы обеспечения информационной безопасности. *[ГОСТ Р ИСО/ТО 13569-2007 Финансовые услуги. Рекомендации по информационной безопасности. Введен в действие: 01.07.2008]*.

См. также: Контроль обеспечения информационной безопасности организации.

Личная тайна [privacy] —

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. *[Конституция Российской Федерации. Принята на всенародном голосовании 12.12.1993]*.

2. Жизнь и здоровье, достоинство личности, личная неприкосновенность, честь и доброе имя, деловая репутация, неприкосновенность частной жизни, неприкосновенность жилища, личная и семейная тайна, свобода передвижения, свобода выбора места пребывания и жительства, имя гражданина, авторство, иные нематериальные блага, принадлежащие гражданину от рождения или в силу закона, неотчуждаемы и непередаваемы иным способом. Нематериальные

блага защищаются в соответствии с настоящим Кодексом и другими законами в случаях и в порядке, ими предусмотренных, а также в тех случаях и пределах, в каких использование способов защиты гражданских прав вытекает из существа нарушенного нематериального блага или личного неимущественного права и характера последствий этого нарушения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

3. Любые сведения о фактах, событиях в жизни человека, обстоятельствах его судьбы, разглашение которых человек считает нежелательным и предпринимает меры для того, чтобы эти сведения не стали известными другим лицам. *[База данных Российской судебной практики по информационному праву http://www.media-pravo.info/glossary/60]*.

Выше: Персональные ланные.

Личный ключ —

См. Закрытый ключ.

Лобовая атака [brute-force attack] —

Атака на криптосистему, основанная на методе полного (тотального) опробования ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

Логическая бомба [logic bomb] —

1. Обобщающий термин деструктивных программных комплексов, резидентно находящихся на компьютере «жертвы» и активирующихся по определенному логическому условию, например, достижение определенной даты или набора определенных состояний системы. Наиболее известным и распространенным является срабатывание логической бомбы на заранее заданный контекст (ключевое слово). Может быть самостоятельной программой или фрагментом кода в составе некоторого программного продукта (пакета программ), распространяемым программистами или производителем некоторого программного продукта (пакета программ). Используется для инициирования вирусной или иного рода программной атаки на систему компьютерную. Механизм разрушающего воздействия может быть сколь угодно различным. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

2. Программа, которая запускается при определённых временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных).

Многие вредоносные программы, такие как вирусы или черви, часто содержат логические бомбы, которые срабатывают в заранее определённое время или при выполнении определённых условий, например, в пятницу 13-го, день смеха или в годовщину Аварии на Чернобыльской АЭС (вирус CIH).

К логическим бомбам как правило относят код, который приводит к не сообщённым заранее последствиям для пользователей. Таким образом, отключение определённой функциональности или окончание работы условно-бесплатных программ, после завершения установленного периода, не считается логической бомбой. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Компьютерный вирус.

Ниже: Бомбы с часовыми механизмами.

Ложный объект [honey pot] —

Ложный информационный ресурс (база данных, WEB-сайт, хранилище файлов), предназначенный для имитации реального объекта, представляющего интерес для злоумышленника, создаваемый в качестве объекта прикрытия в соответствии с замыслом защиты. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Маскирование.

Локальная вычислительная сеть —

Вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

Выше: Компьютерная сеть.

Ниже: Виртуальная локальная вычислительная сеть.

Син.: Локальная сеть.

Локальная сеть [local area network] —

Компьютерная сеть пользователя, имеющая определенную внешнюю территориальную границу.

Примечание. Коммуникационные операции внутри локальной сети не являются предметом внешнего регулирования, но коммуникационные операции, осуществляемые через границу локальной сети, могут быть предметом регулирования. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Син.: Локальная вычислительная сеть.

Локальное (местное) управление компонентами межсетевого экрана —

Выполнение функций по сопровождению МЭ (компоненты) администратором МЭ на том же узле (платформе), на котором функционирует МЭ (компонента) с использованием интерфейса МЭ. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Администратор межсетевого экрана, Дистанционное управление компонентами межсетевого экрана, Централизованное управление компонентами межсетевого экрана.

Люки [backdoors] —

Не описанные в документации возможности работы с программным продуктом, позволяющие получить прямой доступ к фрагментам исполняемого кода и данным, которые не предусмотрены при обычном использовании этой программы. Как правило, специально оставляются разработчиком для обеспечения возможности восстановления работоспособности, либо оставляются по невнимательности после завершения процесса отладки. К появлению люков приводят также ошибки программирования, связанные с неправильным выделением памяти, некорректной обработкой прерываний и вводимых данных и др. Наличие люков позволяет создавать скрытые точки входа, дающие возможность проникать в компьютерную систему в обход механизмов защиты. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Вредоносное программное обеспечение
См. также: Бэкдоры, Скрытые точки входа.

Макровирусы [macro viruses] —

Программы на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и так далее). *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Выше: Компьютерный вирус.

Мандатное управление доступом [mandatory access control] —

Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности. Также иногда переводится как Принудительный контроль доступа. Это способ, сочетающий защиту и ограничение прав, применяемый по отношению к компьютерным процессам, данным и системным устройствам и предназначенный для предотвращения их нежелательного использования. Согласно требованиям ФСТЭК мандатное управление доступом или "метки доступа" являются ключевым отличием систем защиты Государственной Тайны РФ старших классов 1В и 1Б от младших классов защитных систем на классическом разделении прав по матрице доступа. Пример: субъект «Пользователь № 2», имеющий допуск уровня «не секретно», не может получить доступ к объекту, имеющему метку «для служебного пользования». В то же время, субъект «Пользователь № 1» с допуском уровня «секретно» право доступа к объекту с меткой «для служебного пользования» имеет. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: управление доступом.

См. также: Дискреционное управление доступом, Мандатный принцип контроля доступа, Метка конфиденциальности.

Мандатный принцип контроля доступа [mandatory access control] —

Показатель защищенности, определяющий правила разграничения доступа. При реализации мандатного принципа контроля доступа каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии. С помощью этих меток субъектам и объектам назначаются классификационные уровни, являющиеся комбинациями уровня иерархической классификации и иерархических категорий: а) субъект может читать объект, если уровень иерархической классификации в классификационном уровне субъекта не меньше, чем уровень иерархической классификации в классификационном уровне субъекта, и неиерархические категории в классификационном уровне субъекта включают в себя все неиерархические категории в классификационном уровне объекта; б) субъект осуществляет запись в объект, если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все неиерархические категории в классификационном уровне субъекта включены в неиерархические категории в классификационном уровне объекта. *[ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Введен в действие: 01.01.1996]*.

См. также: Дискретизационный принцип контроля доступа, Мандатное управление доступом, Метка конфиденциальности.

Манипулятивное воздействие —

Вид информационно-психологического воздействия, действие специальных средств (устройств) основанное на скрытом управлении, влиянии, обработке человека (группы людей, общества) с целью навязывания (изменения) необходимых идей, ценностей психофизического состояния, форм поведения и социальных установок. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Выше: Информационно-психологическое воздействие.

Маркировка [mark] —

Юридически зарегистрированный товарный знак или защищенный иным образом символ, который выпускается по правилам органа аккредитации или органа сертификации, указывающий на то, что орган достаточно уверен в системах или что соответствующие продукты или субъекты отвечают требованиям определенного стандарта. *[ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введен в действие: 01.10.2009]*.

См. также: Аккредитация, Сертификация.

Маршрут выполнения функциональных объектов —

Определенная алгоритмом последовательность выполняемых функциональных объектов. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)]*.

Ниже: Критический маршрут выполнения функциональных объектов, Фактический маршрут выполнения функциональных объектов.

См. также: Функциональный объект.

Маскиратор —

Средство защиты информации, реализующее математический алгоритм преобразования информации, не использующее секретного ключа или передающее (хранящее) его с сообщением. *[Мордвинов В.А., Фомина А.Б. Защита информации и информационная безопасность. / МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ «Информика», М., 2003/2004]*.

Маскирование [maskuerade] **—**

Стремление какого-либо логического объекта выглядеть в виде другого логического объекта. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды вторжений, Методы внешних вторжений.

См. также: Ложный объект.

Массовая информация —

Предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]***.**

Матрица доступа [access matrix] **—**

Таблица, отображающая правила разграничения доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Дискретизационный принцип контроля доступа, Дискреционное управление доступом.

Матрица рисков [risk matrix] **—**

Инструмент ранжирования и представления рисков путем присвоения рангов последствиям и возможностям. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Машинное моделирование [simulation] **—**

Реализуемый на вычислительной машине метод исследования, предполагающий замену реального процесса его математической моделью. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Модель.

Международная информационная безопасность —

1. Состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

2. Состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве. *[Доклад Генерального секретаря ООН от 10 июня 2000г]*.

Выше: Информационная безопасность.

См. также: Информационная война, Международный информационный терроризм, Международная информационная преступность, Основные направления международного сотрудничества Российской Федерации в области обеспечения информационной безопасности.

Международная информационная преступность [international cyber crime] —

Использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в противоправных целях. [*Доклад Генерального секретаря ООН от 10 июня 2000г.]*.

См. также: Международная информационная безопасность, Международный информационный терроризм.

Международный информационный терроризм —

Использование телекоммуникационных и информационных систем и ресурсов и воздействие на такие системы и ресурсы в международном информационном пространстве в террористических целях. *[Доклад Генерального секретаря ООН от 10 июня 2000г.]*.

См. также: Информационная война, Международная информационная безопасность, Международная информационная преступность, Терроризм в информационном пространстве.

Межконцевое шифрование —

Шифрование данных внутри или на стороне отправителя оконечной системы с соответствующим дешифрованием, выполняемое только внутри или на стороне получателя оконечной системы. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Шифрование.

Межсайтовая подделка запроса [Cross-Site Request Forgery (CSRF или XSRF)] —

Вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Для осуществления данной атаки, жертва должна быть авторизована на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны пользователя, который не может быть проигнорирован или подделан атакующим скриптом.

Основное применение CSRF - вынуждение выполнения каких-либо действий на уязвимом сайте от лица жертвы (изменение пароля, секретного вопроса для восстановления пароля, почты, добавление администратора и т.д.). Так же с помощью CSRF возможна эксплуатация пассивных XSS, обнаруженных на другом сервере. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Сетевая атака.

Син.: Подделка межсайтового запроса.

Межсайтовый скриптинг [Cross-Site Scripting (XSS)] —

Тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «внедрение кода».

Специфика подобных атак заключается в том, что вредоносный код может использовать авторизацию пользователя в веб-системе для получения к ней расширенного доступа или для получения авторизационных данных пользователя. Вредоносный код может быть вставлен в страницу как через уязвимость в веб-сервере, так и через уязвимость на компьютере пользователя. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Сетевая атака.

Межсетевой экран (сетевой экран) [firewall] —

1. Вид барьера безопасности, размещенного между различными сетевыми средами, состоящего из специализированного устройства или совокупности нескольких компонентов и технических приемов, через который должен проходить весь трафик из одной сетевой среды в другую и, наоборот, при этом пропускается только авторизованный трафик, соответствующий местной политике безопасности. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из)

АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

3. Комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определенные в конфигурации. Некоторые межсетевые экраны также позволяют осуществлять трансляцию адресов — динамическую замену внутрисетевых адресов или портов на внешние, используемые за пределами локальной сети. Различают собственно межсетевые экраны, контролирующие входящие и исходящие потоки данных между двумя или более различными сетями, и персональные межсетевые экраны, предназначенные для защиты одного пользовательского компьютера, подключенного к сети. Существует также разделение на межсетевые экраны, работающие на:

• сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;

• сеансовом уровне (также известные как stateful), отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающие спецификации TCP/IP, часто используемые в злонамеренных операциях — сканировании ресурсов, взломах через неправильные реализации TCP/IP, обрыв/замедление соединений, инъекция данных;

• уровне приложений, когда фильтрация происходит на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Администратор межсетевого экрана, Анализ трафика, Безопасность связи, Конфиденциальность трафика, Критерии фильтрации, Правила фильтрации, Трансляция адреса, Экранирование.

Менеджмент [management] **—**

Скоординированная деятельность по руководству и управлению. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Менеджмент информационной безопасности организации, Менеджмент (непрерывности) бизнеса, Менеджмент инцидента информационной безопасности, Менеджмент непрерывности бизнеса (МНБ), Менеджмент риска.

См. также: Система менеджмента.

Менеджмент (непрерывности) бизнеса —

Скоординированная деятельность по руководству и управлению бизнес-процессами организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Выше: Менеджмент.

Син.: Менеджмент непрерывности бизнеса (МНБ).

Менеджмент информационной безопасности организации [management] —

Скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Выше: Менеджмент.

См. также: Обеспечение информационной безопасности организации.

Менеджмент инцидента информационной безопасности [information security incident management] —

Процессы обнаружения, информирования, оценки, реагирования, рассмотрения и изучения инцидентов информационной безопасности. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

Выше: Менеджмент.

Ниже: Расследование инцидента, Реагирование на инцидент.

См. также: Центр управления безопасностью.

Менеджмент непрерывности бизнеса (МНБ) [business continuity management-BCM] —

Целостный управленческий процесс, идентифицирующий потенциальные угрозы для организации и их влияние на операции бизнеса, и обеспечивающий основу для повышения устойчивости организации с возможностью эффективного реагирования, что обеспечивает защиту интересов основных причастных сторон организации, ее репутации, бренда и деятельности по созданию ценностей. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

Выше: Менеджмент.

Син.: Менеджмент (непрерывности) бизнеса

См. также: Планирование непрерывности бизнеса, Минимальная цель обеспечения непрерывности бизнеса (МЦНБ)

Менеджмент риска [risk management] —

1. Скоординированные действия по руководству и управлению организацией в области риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

2. Полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Выше: Менеджмент.

Ниже: Менеджмент риска информационной безопасности организации Син.: Управление рисками, Риск-менеджмент.

См. также: Идентификация риска, Мера и средство контроля и управления, Структура менеджмента риска, Обмен информацией и консультирование (в области риск менеджмента).

Менеджмент риска информационной безопасности организации —

Скоординированные действия по руководству и управлению организацией в отношении риска информационной безопасности с целью его минимизации.

Примечание. Основными процессами менеджмента риска являются установление контекста, оценка риска, обработка и принятие риска, мониторинг и пересмотр риска. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Выше: Менеджмент риска.

См. также: Установление ситуации (контекста) (в области риск-менеджмента), Оценка риска информационной безопасности (организации), Обработка риска информационной безопасности организации, Принятие риска, Пересмотр.

Мера безопасности —

См. Защитная мера.

Мера и средство контроля и управления [control] —

Средство менеджмента риска, включающее в себя политики, процедуры, рекомендации, инструкции или организационные структуры, которые могут быть административного, технического, управленческого или правового характера.

Примечание. Термин «мера и средство контроля и управления» также используется как синоним терминов «защищая мера» (safeguard) или «контрмера» (countermeasure). *[ГОСТ Р ИСО/МЭК 27002-2012*

Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Введен в действие: 01.01.2014].

Син.: Защитная мера.

См. также: Менеджмент риска.

Мера обеспечения безопасности —

См. Защитная мера.

Мероприятие по защите информации [information protection measure] —

Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000].*

См. также: Защита информации.

Меры защиты [control] —

См. Меры обеспечения информационной безопасности.

Меры обеспечения безопасности —

Набор функций, определяющих возможности механизмов обеспечения безопасности сети электросвязи по непосредственной или косвенной реализации требований к безопасности. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007].*

См. также: Безопасность сети электросвязи, Механизм обеспечения безопасности сети электросвязи.

Меры обеспечения информационной безопасности [information security measure] —

Совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009].*

Ниже: Организационные меры обеспечения информационной безопасности.

См. также: Информационная безопасность, Объект обеспечения информационной безопасности.

Меры обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Правовые, организационные, программные и аппаратные способы, правила и процедуры использования механизмов защиты ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].*

См. также: Информационная безопасность Взаимоувязанной сети связи Российской Федерации, Механизм обеспечения информационной безопасности (защиты) Взаимоувязанной сети связи Российской Федерации, Обеспечение

информационной безопасности Взаимоувязанной сети связи Российской Федерации, Система обеспечения информационной безопасности сети связи Российской Федерации.

Место осуществления отдельного вида деятельности, подлежащего лицензированию —

Объект (помещение, здание, сооружение, иной объект), который предназначен для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении, соответствует лицензионным требованиям, принадлежит соискателю лицензии или лицензиату на праве собственности либо ином законном основании, имеет почтовый адрес или другие позволяющие идентифицировать объект данные. Место осуществления лицензируемого вида деятельности может совпадать с местом нахождения соискателя лицензии или лицензиата. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

См. также: Лицензирование.

Метка защиты [security label] —

Граничная метка, присваиваемая какому-либо ресурсу (в качестве которого может служить блок данных), которая именует или обозначает атрибуты защиты этого ресурса.

Примечание. Метка и/или присвоенное значение могут быть явными или неявными. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Метка конфиденциальности.

Метка конфиденциальности [sensitivity label] —

Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Мандатный принцип контроля доступа, Мандатное управление доступом, Метка защиты.

Метод анализа информации —

Совокупность правил, приемов и способов, операций по выделению, отбору, систематизации, преобразованию, переработке и обобщению различных сведений, фактов и данных, получаемых от конкретного источника. Метод анализа информации позволяет выделить наиболее существенную информацию, наметить пути получения новой информации, которая явно не содержится в имеющихся данных, прийти от единичных фактов к общим закономерностям. Известны сравнение, абстрагирование, аналогия, обобщение информации. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Метод «встреча посередине» [meet-in-the-middle attack] —

Метод криптографического анализа, состоящий из двух этапов. Первоначально ключ разбивается на две части, на первом этапе производятся вычисления для одной части ключа, результаты которых записываются в память, на втором этапе определяется ключ путем последовательного обращения к памяти. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Метод испытаний [test method] —

Правила применения определенных принципов и средств испытаний. [ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011].

См. также: Испытания.

Метод коллизий [cryptanalysis based on collision search] —

Метод криптографического анализа, основанный на возможности (при определенных условиях) использования коллизий. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

См. также: Коллизия.

Метод контроля [inspection method] —

Правила применения определенных принципов и средств контроля. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

См. также: Приемочный контроль.

Метод криптографического анализа (криптоанализа) [crypt-analytic method, method of cryptanalysis] —

Совокупность приемов и способов, направленных на исследование криптографической стойкости криптосистемы, объединенных одной или несколькими идеями (математическими, техническими или другими). Можно предположить, что и разработчик криптосистем, и противник и/или нарушитель используют одну и ту же совокупность методов криптографического анализа. В качестве наиболее важных характеристик метода криптографического анализа обычно рассматривают трудоемкость метода криптографического анализа и надежность метода криптографического анализа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптоанализ, Криптографическая стойкость, Модель открытого текста.

Ниже: Корреляционный метод, Метод «встреча посередине», Метод коллизий, Метод на основе парадокса дней рождения, Метод полного (тотального) опробования ключей, Метод последовательного опробования ключа, Метод протяжки вероятного слова, Метод, существенно использующий память, Метод эквивалентных ключей, Разностный метод, Статистический метод, Частотный метод.

Метод на основе парадокса дней рождения [birthday attack] —

Метод криптографического анализа, основанный на использовании парадокса дней рождения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Метод полного (тотального) опробования ключей [exhaustive key search, brute-force attack] —

Метод криптографического анализа, состоящий в переборе всех возможных ключей криптосистемы с отбраковкой ложных вариантов по некоторому критерию. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Метод последовательного опробования ключа [sequential key search] —

Метод криптографического анализа, состоящий в последовательном опробовании и отбраковке ключей криптосистемы в соответствии с некоторыми упорядочениями на множестве ключей. Как правило, применяются специально подобранные упорядочения ключевого множества, например, с учетом вероятностей появления ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Метод протяжки вероятного слова [moving probable word cryptanalysis] —

Метод криптографического анализа, состоящий в последовательном опробовании места в шифрованном тексте, соответствующего вероятному фрагменту открытого текста. При истинном варианте опробования возможно составление и решение уравнений относительно неизвестного ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Метод, существенно использующий память [memory using cryptanalysis] —

Метод криптографического анализа, основанный на использовании массива памяти, значительно превосходящего по объему память, необходимую для записи исходной задачи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Метод эквивалентных ключей [equivalent keys cryptanalysis] —

Метод криптографического анализа, основанный на возможности объединения ключей криптосистемы в классы эквивалентности и опробования только одного ключа из каждого класса. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

См. также: Эквивалентные ключи.

Методическое обеспечение автоматизированной системы [AS methodical support] —

Совокупность документов, описывающих технологию функционирования АС, методы выбора и применения пользователями технологических приемов для получения конкретных результатов при функционировании АС. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Автоматизированная система, Информационное обеспечение автоматизированной системы, Организационное обеспечение автоматизированной системы, Правовое обеспечение автоматизированной системы, Программное обеспечение автоматизированной системы, Техническое обеспечение автоматизированной системы.

Методы внешних вторжений —

Совокупность способов достижения поставленной цели, отличительной особенностью которых является нахождение источника воздействия во внешней среде. Внешние вторжения могут использовать следующие методы: подсоединение к линии (активное или пассивное); перехват излучений; маскирование под полномочных пользователей системы или под ее компоненты; обход механизмов аутентификации или управления доступом. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Вторжение.

Ниже: Маскирование, Перехват (информации).

Методы защиты информации —

Способы (приемы, меры, мероприятия) реализации элементов системы защиты информации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Классификация методов защиты информации.

Механизм (средство) заполнения трафика [traffic padding] **—**

Средство заполнения пауз между передаваемыми сообщениями или их частями для сокрытия передаваемой информации в общем потоке передаваемых данных. Наиболее эффективным способом заполнения трафика является шифрование всего трафика, включая заполняющую паузы информацию. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Заполнение трафика.

Механизм (средство) разграничения доступа [access control mechanism] **—**

Средство реализации идентификации, проверки полномочий пользователя и разрешения или отказа в доступе к объекту. Для этого могут использоваться различные средства: списки полномочий, системы идентификации, специальные режимы и особенности работы, метки, временные ограничения и выделенные маршруты. Наиболее надежно эти средства реализуются на основе системы управления ключами, дающими право

доступа к соответствующей информации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Контроль доступа, Система управления ключами, Минимум привилегий, Многоуровневая защита, Нарушение полномочий, Система разграничения доступа.

Механизм обеспечения безопасности сети электросвязи —

Взаимоувязанная совокупность организационных, аппаратных, программных и программно-аппаратных средств, способов, методов, правил и процедур, используемых для реализации требований к безопасности сети электросвязи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Безопасность сети электросвязи, Меры обеспечения безопасности.

Механизм обеспечения информационной безопасности (защиты) Взаимоувязанной сети связи Российской Федерации —

Аппаратно-программные и организационные средства системы обеспечения информационной безопасности ВСС РФ, реализующие, исходя из заданной политики информационной безопасности ВСС РФ, определенные уровни защиты информационной сферы ВСС РФ в соответствии с одним из перекрывающих друг друга этапов защиты: предотвращением, обнаружением и восстановлением (ликвидацией) последствия воздействия нарушителя информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Информационная безопасность Взаимоувязанной сети связи Российской Федерации, Меры обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации, Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации, Система обеспечения информационной безопасности сети связи Российской Федерации.

Механизм передачи информации —

Реализованный способ передачи информации от отправителя к получателю. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Канал связи.

Механизм проверки правомочности обращений [reference validation mechanism] **—**

Реализация концепции монитора обращений, обладающая следующими свойствами: защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования. *[Руководящий документ "Безопасность информационных*

технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)].

См. также: Монитор обращений.

МикроЭВМ [microcomputer] —

ЭВМ, относящаяся к классу вычислительных машин, центральная часть которых построена на одном или нескольких микропроцессорах и разработанных исходя из требования минимизации физического объема. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

Выше: Семейство ЭВМ.

Минимальная цель обеспечения непрерывности бизнеса (МЦНБ) [minimum business continuity objective - MBCO] —

Обеспечение минимального уровня услуг и (или) продуктов, которые являются приемлемыми для организации в достижении ее целей бизнеса во время нарушения. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014].*

См. также: Менеджмент непрерывности бизнеса (МНБ).

Минимум привилегий [least privilege] —

Один из основополагающих принципов организации системы защиты, гласящий, что каждый субъект должен иметь минимально возможный набор привилегий, необходимый для решения поставленных перед ним задач. Следование этому принципу предохраняет от нарушений, возможных в результате злого умысла, ошибки или несанкционированного использования привилегий. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009].*

См. также: Механизм (средство) разграничения доступа.

Мини-ЭВМ [minicomputer] —

ЭВМ, относящаяся к классу вычислительных машин, разрабатываемых из требования минимизации стоимости и предназначенных для решения достаточно простых задач.

Примечание. Как правило, мини-ЭВМ устанавливаются в обычных рабочих помещениях. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

Выше: Семейство ЭВМ.

Многократная цифровая подпись [multiple digital signature] —

Цифровая подпись, сформированная с использованием схемы цифровой подписи, и не являющаяся одноразовой цифровой подписью. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Цифровая подпись.

См. также: Одноразовая цифровая подпись.

Многоуровневая безопасность [multilevel security] —

См. Многоуровневая защита.

Многоуровневая защита [multilevel security] —

1. Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

2. Концепция (модель) доступа субъектов с различными правами к объектам различных уровней секретности. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

Син.: Многоуровневая безопасность.

См. также: Механизм (средство) разграничения доступа.

Многофакторная аутентификация [multi-factor authentication] —

Реализация контроля доступа, представляющая собой идентификацию пользователя на основе нескольких независимых факторов (биометрические данные, того, что он знает и того, чем он владеет, и т.п.). Представляет гибкий подход, позволяющий организации реализовать устойчивую систему управления доступом на основе использования различных методов аутентификации. Технологии многофакторной аутентификации включают: одноразовые пароли, аутентификацию на основе сертификатов, аутентификацию на основе контекста и др. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Аутентификация.

См. также: Многофакторная аутентификация.

Модель [model] —

Абстрактное представление реальности в какой-либо форме (например, в математической, физической, символической, графической или дескриптивной), предназначенное для представления определенных аспектов этой реальности и позволяющее получать ответы на изучаемые вопросы. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Модель защиты [protection model] —

Абстрактное (формализованное или неформализованное) описание комплекса средств программно-технических и (или) организационных мер защиты от несанкционированного доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Оценка защиты.

Модель нарушителя [intruder model] —

Абстрактное (формализованное или неформализованное) описание возможностей противника или нарушителя.

Модель нарушителя определяет:

- категории (типы) нарушителей, которые могут воздействовать на объект;

- цели, которые могут преследовать нарушители каждой категории, возможный количественный состав, - ---- используемые инструменты, принадлежности, оснащение, оружие и проч.;

- типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

См. также: Модель нарушителя информационной безопасности, Нарушитель.

Модель нарушителя информационной безопасности [information security intruder model] —

Описание и классификация нарушителей информационной безопасности, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз информационной безопасности со стороны указанных нарушителей. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Модель нарушителя, Нарушитель информационной безопасности.

Модель нарушителя правил разграничения доступа [security policy violator's model] —

Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Правила разграничения доступа, Нарушитель правил разграничения доступа.

Модель открытого текста [plain text model] —

Математическая модель, описывающая свойства реальных открытых текстов, вырабатываемых определенными источниками, либо естественными (осмысленный текст на каком-то языке), либо искусственными (межмашинный обмен, телеметрия и др.). Простейшими моделями открытого текста являются последовательность независимых испытаний и цепь Маркова. Модели открытого текста лежат в основе различных подходов к определению криптографической стойкости, а также методов криптографического анализа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Открытый текст.

Модель политики безопасности [security policy model] —

Формальное представление политики безопасности, разработанной для системы. Оно должно содержать формальное описание определяющих управление, распределение и защиту критической информации. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

Модель угроз (безопасности информации) [treat-risk model] —

Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. Примечание. Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Син.: Модель угроз информационной безопасности.

См. также: Угроза (безопасности информации).

Модель угроз информационной безопасности [information security threat-risk model] —

Описание источников угроз информационной безопасности; методов реализации угроз информационной безопасности; объектов, пригодных для реализации угроз информационной безопасности; уязвимостей, используемых источниками угроз информационной безопасности; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности активов информационных); масштабов потенциального ущерба. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Син.: Модель угроз (безопасности информации).

Модификация информации —

Целенаправленное изменение формы представления и содержания информации. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Нарушение целостности информации, Модификация (переработка) программы для ЭВМ или базы данных, Обнаружение манипуляции.

Модификация (переработка) программы для ЭВМ или базы данных [software modification] —

Любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык, за исключением адаптации. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Модификация информации, Адаптация программы для ЭВМ или базы данных.

Монитор обращений [reference monitor] —

Концепция абстрактной машины, осуществляющей политики управления доступом объекта оценки. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Механизм проверки правомочности обращений.

Мониторинг [monitoring] —

1. Систематическое или непрерывное наблюдение за объектом с обеспечением контроля и/или измерения его параметров, а также проведение анализа с целью предсказания изменчивости параметров и принятия решения о необходимости и составе корректирующих и предупреждающих действий. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Постоянное наблюдение за объектами и субъектами, влияющими на информационную безопасность организации банковской системы Российской Федерации, а также сбор, анализ и обобщение результатов наблюдений. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

3. Процесс систематического сбора информации о параметрах состояния некоторой технической системы, социально-экономической среды либо состояния выполнения различного рода соглашений. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Ниже: Мониторинг (в области риск-менеджмента), Мониторинг безопасности информации, Мониторинг информационной безопасности организации, Сетевой мониторинг.

См. также: Ведение контрольных журналов, Проверка безопасности.

Мониторинг (в области риск-менеджмента) [monitoring] —

Постоянная проверка, надзор, критическое наблюдение или определение состояния, с целью идентифицировать изменения относительно требуемого или ожидаемого уровня.

Примечание. Мониторинг можно применять к системе риск-менеджмента, процессу риск-менеджмента, риску или контролированию риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Выше: Монитроинг.

См. также: Контролирование риска.

Мониторинг безопасности информации [information security monitoring] —

1. Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие

требованиям безопасности информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Монитроинг.

Мониторинг информационной безопасности организации —

Постоянное наблюдение за процессом обеспечения информационной безопасности в организации с целью установить его соответствие требованиям по информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Выше: Монитроинг.

Син.: Контроль обеспечения информационной безопасности организации.

См. также: Обеспечение информационной безопасности организации, Лицо, ответственное за информационную безопасность, Оценка соответствия информационной безопасности организации установленным требованиям.

Мониторинговые атаки (объекта оценки) [monitoring attacks] **—**

Характерная категория методов нападения, которая включает пассивные методы и средства анализа, направленные на раскрытие чувствительных внутренних данных объекта оценки в условиях его функционирования в соответствии с руководствами. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

Выше: Атака.

См. также: Уязвимость (объекта оценки).

Мошенничество в сфере компьютерной информации —

Хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей *[Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изменениями на 5 мая 2014 года) (редакция, действующая с 16 мая 2014 года). Введен в действие 01.01.1997]*.

Выше: Компьютерное преступление.

См. также: Интернет-мошенничество.

Мультипрограммирование [multiprogramming] **—**

Режим обработки информации, при котором ресурсы вычислительной машины или системы обработки информации используются более чем одним

процессом обработки информации. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Наблюдатель [observer] —

Лицо, сопровождающее группу по аудиту, но не проводящее аудит.

Примечания:

1. Наблюдатель не входит в состав группы по аудиту и не влияет или не вмешивается в проведение аудита.

2. Наблюдателем может быть представитель проверяемой организации, контролирующего органа или другой заинтересованной стороны, который наблюдает за проведением аудита. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Аудитор, Группа по аудиту, Сопровождающий, Технический эксперт.

Набор статистических тестов [battery of tests] —

В криптографии — совокупность статистических критериев (тестов), предназначенная для проверки соответствия анализируемой последовательности гипотезе о независимости и равновероятности ее элементов. Каждый тест состоит в вычислении по анализируемой последовательности некоторой статистики, имеющей известное распределение для идеальной случайной последовательности, и использовании критерия согласия. Стандартными наборами статистических тестов являются набор тестов Д. Кнута, пакет DIEHARD (Дж. Марсальи), набор тестов NIST (Института стандартов США), пакет TestUOl (Л'Экуйера). В эти наборы входят тест автокорреляции, тест следующего бита, тест профиля линейной сложности, тест серий, универсальный тест Маурера, частотный тест и другие. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Тест автокорреляции, Тест следующего бита (предсказатель), Тест профиля линейной сложности, Тест серий, Тест частот цепочек, Универсальный тест Маурера, Частотный тест.

Наводка (наведенный в токопроводящих линейных элементах технических средств сигнал) —

Ток и напряжение в токопроводящих элементах, вызванные электромагнитным излучением, емкостными и индуктивными связями. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

Син.: Электромагнитные наводки.

См. также: Побочное электромагнитное излучение, Побочные электромагнитные излучения и наводки, Паразитное электромагнитное излучение.

Надежность [reliability] —

Характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение

определенного периода времени. Показателями надежности являются вероятность безотказной работы, среднее время наработки на отказ, среднее время восстановления. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Восстановление.

Налоговая тайна —

Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений:

1) являющихся общедоступными, в том числе ставших таковыми с согласия их обладателя - налогоплательщика;

2) об идентификационном номере налогоплательщика;

3) о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;

4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам);

5) предоставляемых избирательным комиссиям в соответствии с законодательством о выборах по результатам проверок налоговым органом сведений о размере и об источниках доходов кандидата и его супруга, а также об имуществе, принадлежащем кандидату и его супругу на праве собственности;

6) предоставляемых в Государственную информационную систему о государственных и муниципальных платежах, предусмотренную Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг";

7) о специальных налоговых режимах, применяемых налогоплательщиками, а также об участии налогоплательщика в консолидированной группе налогоплательщиков. *[Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 N 146-ФЗ (с изменениями на 28 декабря 2013 года). Введен в действие: 01.01.1999]*.

Выше: Служебная тайна.

Наложенные криптографические средства [additional cryptographic mechanisms] **—**

Криптографические средства, не связанные с функционированием операционной системы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографические средства.

Нападающий [attacker] **—**

Субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Син.: Нарушитель.

См. также: Противостоять.

Нарушение [disruption] —

Ожидаемый (например, ураган) или непредвиденный (например, нарушение/прекращение энергоснабжения, землетрясение или атака на системы/инфраструктуру информационно -коммуникационных технологий) инцидент, который нарушает обычный ход операций на площадке организации. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: План восстановления ИКТ после бедствия, Устойчивость.

Нарушение безопасности (информационной системы) [security violation] —

Нарушение установленных правил управления доступом, приведшее к нарушению свойств конфиденциальности, целостности и доступности. Может быть, как преднамеренное в результате неправомерных действий злоумышленника, так и в результате сбоя в работе отдельных программ или технических компонентов системы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Атака.

Нарушение информационной безопасности организации —

Случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Нарушитель информационной безопасности, Угроза информационной безопасности организации, Ущерб.

Нарушение полномочий [privilege violation] —

Попытка пользователя или программы выполнить неразрешенную операцию. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Список полномочий, Неправомочные действия, Полномочие.

Нарушение системы безопасности [security system violation] —

Успешное поражение средства управления безопасностью, которое завершается проникновением в систему. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Атака.

Нарушение целостности информации [information integrity violation] —

Утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения. Несанкционированная модификация информации может быть случайной (искажение) или умышленной (подделка). По отношению к целостности информации можно дифференцировать дополнительно следующие виды угроз: модификацию, искажение, подделку и уничтожение. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Модификация информации.

Нарушитель [dishonest party, attacker] —

1. Любое лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем и сетей, или снижения доступности ресурсов информационной системы и сетевых ресурсов для законных пользователей. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Участник протокола, нарушающий предписанные протоколом действия. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Нечестный участник, Нарушитель внутренний, Нападающий.

Ниже: Активный нарушитель, Пассивный нарушитель.

См. также: Модель нарушителя, Противник, Потенциал нападения.

Нарушитель безопасности сети электросвязи —

Физическое или юридическое лицо, преступная группа, процесс или событие, производящие преднамеренные или непреднамеренные воздействия на инфокоммуникационную структуру сети электросвязи, приводящие к нежелательным последствиям для интересов пользователей услугами связи, операторов связи и/или органов государственного управления. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Безопасность сети электросвязи, Меры обеспечения безопасности.

Нарушитель в (информационной) автоматизированной системе —

Субъект, имеющий доступ к работе со штатными средствами автоматизированной системы и средствами вычислительной техники как части автоматизированной системы.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты. *[Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Модель нарушителя.

Нарушитель информационной безопасности —

1. Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

3. Субъект, реализующий угрозы безопасности информационной организации банковской системы Российской Федерации, нарушая предоставленные ему полномочия по доступу к активам организации банковской системы Российской Федерации или по распоряжению ими *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Нарушитель, Модель нарушителя информационной безопасности.

Нарушитель информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Физическое или юридическое лицо, общественное объединение, ведомство, процесс, событие, способное произвести несанкционированные или

непреднамеренные действия (операции) над информационной сферой ВСС РФ, приводящие к нежелательным для пользователя или оператора связи ВСС РФ последствиям. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Информационная безопасность Взаимоувязанной сети связи Российской Федерации, Информационная сфера взаимоувязанной сети связи Российской Федерации.

Нарушитель правил разграничения доступа [security policy violator] —

Субъект доступа, осуществляющий несанкционированный доступ к информации. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Правила разграничения доступа, Модель нарушителя правил разграничения доступа.

Национальная безопасность —

Состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства. *[Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537]*.

См. также: Критически важные структуры, Критически важный объект инфраструктуры Российской Федерации, Обеспечение национальной безопасности, Стратегические национальные приоритеты, Угроза национальной безопасности.

Национальные интересы России в информационной сфере —

Выделяют четыре основные составляющие национальных интересов Российской Федерации в информационной сфере:

• соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

• информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

• развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение

накопления, сохранности и эффективного использования отечественных информационных ресурсов. На этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности;

• защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Ниже: Интересы государства в информационной сфере.

Национальные интересы Российской Федерации —

Совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства. *[Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537]*.

Национальный центр компьютерной безопасности США [National Computer Security Center (NCSC)] —

Организация, поддерживающая и стимулирующая распространение защищенных систем в учреждениях Федерального правительства. Является координирующим органом в области анализа и разработки систем с гарантированной защитой. Первичное название — Центр Компьютерной Безопасности министерства обороны США (DoD Computer Security Center). *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Не интерактивное доказательство с нулевым разглашением [noninteractive zero-knowledge proof] —

Доказательство с нулевым разглашением, выполняемое за один цикл (протокола): доказывающий посылает сообщение проверяющему, который на основе анализа этого сообщения либо принимает, либо отвергает доказательство. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Доказательство с нулевым разглашением.

Неавторизованный доступ —

См. Несанкционированный доступ.

Невозможность отказа [non-repudiation] —

1. Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Свойство криптографического протокола, состоящее в том, что его участники (все или некоторые) не могут отказаться от факта совершения определенных действий. Обеспечивается системой цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Неотказуемость.

См. также: Самоотказ, Функция-сервис обеспечения невозможности отказа.

Невозможность отказа от авторства [non-repudiation of origin] —

Сервис, предназначенный для защиты от отрицания автором факта создания или отправления им сообщения. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также Невозможность отказа.

Невырожденная функция [nondegenerate function] —

Функция, существенно зависящая от всех своих переменных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Негативные действия [adverse actions]—

Действия, выполняемые источником угрозы по отношению к активам. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Источник угрозы безопасности информации.

Недекларированные возможности —

1. Функциональные возможности средств вычислительной техники и программного обеспечения, не описанные или не соответствующие описанным в документации, которые могут привести к снижению или нарушению свойств безопасности информации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Функциональные возможности программного обеспечения, не описанные в документации. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

3. Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)]*.

См. также: Программная закладка.

Незарегистрированный пользователь [unauthorized user] —

Пользователь, не состоящий на учете в данной системе коллективного пользования. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Законный пользователь.

Неквалифицированная электронная подпись (усиленная неквалифицированная электронная подпись) [nonqualified electronic signature] —

Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]* .

Выше: Электронная подпись.

См. также: Неквалифицированная электронная подпись (усиленная неквалифицированная электронная подпись), Простая электронная подпись, Средства электронной подписи, Электронный документ.

Некритичная информация [unclassified information] —

Защищаемая информация, не отнесенная к какой-либо категории информации ограниченного доступа.

Примечание 1.: В директиве президента США от 9 мая 2008 г. введена новая категория «некритичная контролируемая информация», включающая такие подкатегории, как информация «только для официального использования», «чувствительная, но неклассифицируемая» и «чувствительная правоохранительная». Подлежит защите от модификации и уничтожения. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Критическая информация, Информация ограниченного доступа, Служебная информация ограниченного распространения.

Неотказуемость [non-repudiation] —

1. Способность удостоверять имевшее место событие или действие и их субьекты так, чтобы это событие или действие и субьекгы, имеющие к нему отношение, не могли быть поставлены под сомнение. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства*

обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007].

Син.: Невозможность отказа.

Неотслеживаемость [untracebility] —

Свойство, означающее невозможность получения противником и/или нарушителем сведений о действиях участников (протокола). Определяется для криптографических систем с большим количеством участников: систем электронных платежей, систем доступа к электронным информационным фондам и т. п. Родственные понятия — анонимность и несвязываемость. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Анонимность, Несвязываемость.

Неправомерное использование информации —

Передача, распространение (публикация), применение полученных легальным путем сведений в нарушение правил и полномочий (санкций), установленных для данных сведений и субъекта, предпринявшего такие действия. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Нарушение полномочий.

Неправомерное использование информационно-телекоммуникационных систем и информационных ресурсов —

Использование телекоммуникационных и информационных систем и ресурсов без соответствующих прав или с нарушением установленных правил, законодательства или норм международного права. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Нарушение полномочий, Неправомерное использование информационных ресурсов, Несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы.

Неправомерное использование информационных ресурсов —

Использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств либо норм международного права. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

См. также: Неправомерное использование информационно-телекоммуникационных систем и информационных ресурсов, Нарушение полномочий, Несанкционированное вмешательство в информационные ресурсы.

Неправомочные действия —

Действия в отношении ресурса информационного, совершаемые в нарушение правил и полномочий (санкций), установленных для данного ресурса *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Нарушение полномочий, Список полномочий.

Неправомочный доступ [illegal access] **—**

См. Несанкционированный доступ.

Непредвиденная ситуация —

Рисковое событие, связанное с неблагоприятными внешними событиями природного и техногенного характера, а также с действиями субъектов (групп субъектов), приводящими к невозможности функционирования организации или ее служб/подразделений в обычном, регламентируемом соответствующими стандартами режиме. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Чрезвычайная ситуация.

Непреднамеренная атака на отказ в обслуживании [unintentional Denial-of-Service] **—**

Отказ в обслуживании для какого-либо сервиса, наступивший в результате случайного стечения обстоятельств (резко возросший интерес в результате рекламы, внезапная и непредвиденная исключительная популярность и т. д.), создающий впечатление об успешно проведенной DoS атаке. Часто возникает в моменты пиковой активности в результате размещения интересной информации на новостных сайтах, а также в результате индексирования поисковыми системами популярных URL-ссылок на различные медиа-ресурсы с ограниченной пропускной способностью каналов доступа к ним. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

Выше: Атака на отказ в обслуживании.

Непреднамеренное воздействие на информацию —

1. Ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000 ГОСТ Р 51583-2000]*.

2. Ошибка пользователя информацией, сбой технических и программных средств информационных систем, а также природное явление или иное нецеленаправленное на изменение информации воздействие, связанное с

функционированием технических средств, систем или с деятельностью людей, приводящей к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Воздействие.

См. также: Защита информации от непреднамеренного воздействия.

Непреднамереные угрозы —

См. Случайные угрозы.

Непрерывность защиты [protection continuity] —

Принцип защиты, заключающийся в организации защиты объекта на всех стадиях его жизненного цикла: в период разработки, изготовления (строительства), испытаний, эксплуатации и утилизации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Принципы обеспечения безопасности.

Неприятие риска [risk aversion] —

Отношение к риску, выражаемое в избегании риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Принятие риска.

Несанкционированное вмешательство в информационные ресурсы —

Неправомерное воздействие на процессы формирования, обработки, преобразования, передачи, использования и хранения информации. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

См. также: Неправомерное использование информационных ресурсов.

Несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы —

Вмешательство в процессы сбора, обработки, накопления, хранения, отображения, поиска, распространения и использования информации с целью нарушения нормального функционирования систем или нарушение целостности, конфиденциальности и доступности ресурсов информационных и телекоммуникационных. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Неправомерное использование информационно-телекоммуникационных систем и информационных ресурсов.

Несанкционированное воздействие на информацию —

1. Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Изменение информации (ресурсов автоматизированной информационной системы), осуществляемое с нарушением установленных прав и (или) правил.

Примечание 1. Несанкционированное воздействие может быть осуществлено преднамеренно или непреднамеренно. Преднамеренные несанкционированные воздействия являются специальными воздействиями.

Примечание 2. Изменение может быть осуществлено в форме замены информации (ресурсов автоматизированной информационной системы), введения новой информации (новых ресурсов автоматизированной информационной системы), а также уничтожения или повреждения информации (ресурсов автоматизированной информационной системы). *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Воздействие.

См. также: Защита информации от несанкционированного воздействия (ЗИ от НСВ), Средство защиты информации от несанкционированного воздействия.

Несанкционированное изменение информации —

Изменение содержания информации при ее обработке, хранении или передаче с нарушением установленных прав и правил разграничения доступа. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Несанкционированное изменение маршрута сообщения —

Изменение маршрутной информации, содержащейся в передаваемом сообщении или в системе коммутации сети связи с нарушением установленных прав и правил разграничения доступа, приводящее к передаче сообщения или части сообщения по измененному адресу. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Несанкционированное изменение последовательности сообщений —

Смещение во времени или переупорядочение сообщений в процессе их обработки, хранения или передачи с нарушением установленных прав и правил разграничения доступа. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Несанкционированное изменение сообщения —

Изменение данных сообщения при его обработке, хранении или передаче, приводящее к невозможности достоверного выделения информации, содержащейся в данном сообщении. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации

Несанкционированный доступ [unauthorized access] —

Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

Примечание 1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.

Примечание 2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Выше: Доступ.

Син.: Неавторизованный доступ, Неправомочный доступ.

См. также: Вторжение (в автоматизированную информационную систему), Защита от несанкционированного доступа (Защита от НСД), Компрометация, Основные способы несанкционированного доступа, Несанкционированный доступ к информации, Способы несанкционированного доступа.

Несанкционированный доступ к информации [unauthorized access to information] —

1. Доступ к информации (ресурсам автоматизированной информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам автоматизированной информационной системы).

Примечания:

1. Несанкционированный доступ может быть осуществлен преднамеренно или непреднамеренно.

2. Права и правила доступа к информации и ресурсам информационной системы устанавливаются для процессов обработки информации, обслуживания автоматизированной информационной системы, изменения программных, технических и информационных ресурсов, а также получения информации о них. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

2. Нарушение регламентированного доступа к объекту защиты. *[Руководящий документ Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

3. Доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. *[Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

4. Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

См. также: Несанкционированный доступ, Защита информации от несанкционированного доступа (ЗИ от НСД), Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники, Специальный защитный знак (СЗЗ), Санкционированный доступ к информации.

Несанкционированный доступ к информационной сфере Взаимоувязанной сети связи Российской Федерации —

Доступ к информационной сфере ВСС РФс нарушением установленных прав и правил разграничения доступа. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Несанкционированный доступ к программным средствам —

Доступ к программам, записанным в памяти электронно-вычислительной машины или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Дата принятия: Введен в действие: 01.07.1999]*.

См. также: Защита программных средств.

Несанкционированный доступ к услугам электросвязи Взаимоувязанной сети связи Российской Федерации (сети связи общего пользования) —

Доступ к услугам электросвязи с нарушением установленных прав и правил разграничения доступа. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Несанкционированный повтор сообщения —

Повтор передачи заданному получателю ранее уже переданного сообщения с нарушением установленных прав и правил разграничения доступа. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Несвязываемость [unlinkability] —

Свойство, родственное неотслеживаемости и означающее, что противник и/или нарушитель не только не может установить, кто именно выполнил данное конкретное действие, но даже выяснить, были ли разные действия выполнены одним и тем же участником. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Анонимность, Неотслеживаемость.

Неформальный [informal] —

Выраженный на естественном языке. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Формальный, Полуформальный.

Нечестный участник [dishonest party] —

См. Нарушитель.

Норма эффективности защиты информации —

Значение показателя эффективности защиты информации, установленное нормативными и правовыми документами. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Контроль эффективности защиты информации, Показатель эффективности защиты информации.

Носитель данных [data medium]—

1. Материал, на котором или в котором данные могут быть записаны и из которого они могут быть извлечены. *[ISO/IEC 2382-1:1993.*

Информационная технология. Словарь. Часть 1. Основные термины и определения].

2. Материальный объект, предназначенный для записи и хранения данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Защита данных, Носитель информации.

Носитель документированной информации —

Материальный объект, предназначенный для закрепления, хранения (и воспроизведения) речевой, звуковой или изобразительной информации. *[ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения. Введен в действие: 01.03.2014]*.

См. также: Документированная информация.

Носитель защищаемой информации —

Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Защищаемая информация.

Носитель информации [data medium] **—**

Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Носитель данных, Защита информации.

Носитель сведений, составляющих государственную тайну —

Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов. Примечание. Реквизиты носителей сведений, составляющих государственную тайну, включают следующие данные:

• о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

• об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

• о регистрационном номере;

• о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены. *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Гриф секретности, Доступ к сведениям, составляющим государственную тайну.

Нотариальная тайна —

Нотариус обязан хранить в тайне сведения, которые стали ему известны в связи с осуществлением его профессиональной деятельности. Суд может освободить нотариуса от обязанности сохранения тайны, если против нотариуса возбуждено уголовное дело в связи с совершением нотариального действия. *[Закон РФ от 11.02.1993 N 4462-1 “Основы законодательства Российской Федерации о нотариате” (с изменениями на 21 декабря 2013 года). Введен в действие: 11.03.1993]*.

Выше: Профессиональная тайна.

Нотаризация (удостоверение подлинности) [notarization] —

1. Регистрация данных доверенным третьим лицом, которое обеспечивает последующее подтверждение правильности их характеристик, таких как содержимое, отправитель, время и получатель. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*. Регистрация данных защищенной третьей стороной, что в дальнейшем позволяет обеспечить точность характеристик данных.

Примечание. К характеристикам данных, например, относятся: содержание, происхождение, время и способ доставки. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*

Выше: Виды механизмов защиты.

Син.: Заверение (подлинности).

Нулевое разглашение [zero-knowledge property] —

Свойство протокола доказательства знания, обеспечивающее такое его выполнение, что никакая информация о доказываемом утверждении, кроме факта его истинности, не может быть получена нечестным проверяющим из переданных сообщений за время полиномиально зависящее от суммарной длины этих сообщений. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Нулевое разглашение относительно честного проверяющего.

См. также: Доказательство с нулевым разглашением.

Нулевое разглашение относительно честного проверяющего [honest-verifier zero-knowledge] —

Ослабленный вариант разглашения нулевого, при котором требуется, чтобы протокол интерактивного доказательства не давал никакой дополнительной информации о доказываемом утверждении лишь честному проверяющему, т. е. выполняющему действия, предписанные протоколом. С криптографической точки зрения данное свойство защищает доказывающего не от нечестного проверяющего, а от противника, который подслушивает сеанс выполнения протокола. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Нулевое разглашение.

Обезличивание персональных данных —

Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Выше: Обработка персональных данных.

Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Деятельность, направленная на предотвращение утечки защищаемой информации информационной сферы ВСС РФ, несанкционированных или непреднамеренных воздействий нарушителя на информационную сферу ВСС РФ, на обнаружение последствий от непредотвращенных воздействий нарушителя на информационную сферу ВСС РФ и на ликвидацию последствий воздействия нарушителя на информационную сферу ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Информационная безопасность Взаимоувязанной сети связи Российской Федерации, Меры обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации, Механизм обеспечения информационной безопасности (защиты) Взаимоувязанной сети связи Российской Федерации, Политика информационной безопасности Взаимоувязанной сети связи Российской Федерации, Проект информационной безопасности Взаимоувязанной сети связи Российской Федерации, Система обеспечения информационной безопасности сети связи Российской Федерации.

Обеспечение информационной безопасности организации —

Деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Критерий обеспечения информационной безопасности организации, Корпоративная политика информационной безопасности, Менеджмент информационной безопасности организации, Мониторинг информационной безопасности организации, Система обеспечения информационной безопасности, Объект обеспечения информационной безопасности, Роль обеспечения информационной безопасности в организации, Система документов по информационной безопасности в организации, Служба информационной безопасности организации.

Обеспечение национальной безопасности —

Основное содержание обеспечения национальной безопасности состоит в поддержании правовых и институциональных механизмов, а также ресурсных возможностей государства и общества на уровне, отвечающем национальным интересам Российской Федерации.

Состояние национальной безопасности Российской Федерации напрямую зависит от экономического потенциала страны и эффективности функционирования системы обеспечения национальной безопасности. *[Указ Президента РФ от 12.05.2009 N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"]*.

См. также: Национальная безопасность, Система обеспечения национальной безопасности.

Обладатель информации [owner of information] —

Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

См. также: Обладатель информации, составляющей коммерческую тайну.

Обладатель информации, составляющей коммерческую тайну —

Лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны. *[Федеральный закон от 29.07.2004 N 98-ФЗ “О коммерческой тайне” (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]*.

См. также: Передача информации, составляющей коммерческую тайну, Разглашение информации, составляющей коммерческую тайну, Режим коммерческой тайны.

Область аудита [audit scope] —

Содержание и границы аудита.

Примечание. Область аудита обычно включает в себя местонахождение, организационную структуру, виды деятельности и процессы, а также охватываемый период времени. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

Область аудита информационной безопасности —

Содержание и границы аудита информационной безопасности. Примечание. Область аудита информационной безопасности включает местонахождение, организационную структуру, виды деятельности проверяемой организации и процессы, которые подвергаются аудиту информационной безопасности, а также охватываемый период времени. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Область памяти [storage area] —

Память, выделенная для размещения одной или нескольких порций данных. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Область действия системы обеспечения информационной безопасности —

Совокупность информационных активов и элементов информационной инфраструктуры организации банковской системы Российской Федерации. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Обмен аутентификацией —

Механизм, предназначенный для подтверждения подлинности какого-либо логического объекта путем обмена информацией. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Обмен информацией и консультирование (в области риск менеджмента)[communication and consultation] **—**

Непрерывные и итерационные процессы, которые организация осуществляет для обеспечения, совместного использования или получения информации и ведения диалога с заинтересованными сторонами, касающегося управления рисками.

Примечание 1. Информация может касаться наличия, характера, формы, возможности, важности, приемлемости, оценивания и воздействия на риск.

Примечание 2. Консультирование — это двусторонний процесс квалифицированного обмена информацией между организацией и сторонами, заинтересованными по любому вопросу перед тем, как вынести решение или перед определением направления решения этого вопроса. Консультирование — это:

• процесс, который воздействует на принимаемое решение посредством влияния, а не административных полномочий;

• информация для принятия решений, а не совместное принятие решений. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Менеджмент риска.

Обнаружение вторжений [intrusion detection] **—**

Формальный процесс обнаружения вторжений, обычно характеризующийся сбором сведений об аномальном характере использования, а также о том, какая уязвимость была использована и каким образом, включая то, когда и как это произошло. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Вторжение, Система обнаружения вторжения, Предотвращение вторжений.

Обнаружение манипуляции [manipulation detection] —

Механизм, используемый для обнаружения возможной модификации блока данных (случайной или преднамеренной). *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Модификация информации.

Обнаруженные потенциальные уязвимости (объекта оценки) [encountered potential vulnerabilities] —

Потенциально слабые места объекта оценки, идентифицированные оценщиком при выполнении видов деятельности по оценке, которые могли бы быть использованы для нарушения функциональных требований безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Уязвимость (объекта оценки), Потенциальная уязвимость (объекта оценки).

Обновление ключей [key updating] —

Способ смены ключей, при котором новый ключ генерируется с помощью вычисления значения функции (обычно функции однонаправленной) от аргумента, определяемого предыдущим ключом и, возможно, другими данными. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Обработка данных [data processing] —

1. Систематизированное выполнение операций с данными.

Примечание 1. Примерами являются арифметические или логические операции с данными, слияние или сортировка данных, сборка или компиляция программ или операции с текстом, такие как редактирование текста, сортировка, соединение, хранение, восстановление, вывод на дисплей или печать.

Примечание 1а. Термин обработка данных не следует использовать как синоним термина обработка информации. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Процесс обработки данных, Центр обработки данных.

Обработка информации [information processing] —

1. Совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

2. Систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Выше: Информационная технология.

Ниже: Получение (добывание) информации.

См. также: Защищенность от несанкционированного доступа к информации при ее обработке средствами вычислительной техники, Система обработки информации, Средства обработки информации.

Обработка персональных данных [personal data processing] —

Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Ниже: Автоматизированная обработка персональных данных, Блокирование персональных данных, Обезличивание персональных данных, Предоставление персональных данных, Распространение персональных данных, Трансграничная передача персональных данных, Уничтожение персональных данных.

См. также: Оператор (персональных данных).

Обработка риска [risk treatment] —

Процесс выбора и осуществления мер по модификации риска. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Обработка риска информационной безопасности организации —

Процесс разработки и/или отбора и внедрения мер управления рисками информационной безопасности организации.
Примечание 1. Обработка риска может включать в себя:

• избежание риска путем принятия решения не начинать или не продолжать действия, создающие условия риска;

• поиск благоприятной возможности путем принятия решения начать или продолжать действия, могущие создать или увеличить риск;

• устранение источника риска;

• изменение характера и величины риска;

• изменение последствий;

• разделение риска с другой стороной или сторонами;

• сохранение риска как в результате сознательного решения, так и «по умолчанию».

Примечание 2. Обработки риска с негативными последствиями иногда называют смягчением, устранением, предотвращением, снижением, подавлением и коррекцией риска. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Менеджмент риска информационной безопасности организации.

Обработка риска нарушения информационной безопасности —

Процесс выбора и осуществления защитных мер, снижающих риск нарушения информационной безопасности, или мер по переносу, принятию или уходу от риска. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Обработка текстов [text processing] —

Использование вычислительной машины для ввода, редактирования, форматирования и печати текстов и документов. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Обратная социальная инженерия [reverse social engineering] —

1. Целью обратной социальной инженерии является цель заставить самому рассказать о своих паролях, информацию о компании. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. Об обратной социальной инженерии упоминают тогда, когда жертва сама предлагает злоумышленнику нужную ему информацию. Это может показаться абсурдным, но на самом деле лица, обладающие авторитетом в технической или социальной сфере, часто получают идентификаторы и пароли пользователей и другую важную личную информацию просто потому, что никто не сомневается в их порядочности. Например, сотрудники службы поддержки никогда не спрашивают у пользователей идентификатор или пароль; им не нужна эта информация для решения проблем. Однако, многие пользователи ради скорейшего устранения проблем добровольно сообщают эти конфиденциальные сведения. Получается, что злоумышленнику даже не нужно спрашивать об этом.

Примером обратной социальной инженерии может служить следующий простой сценарий. Злоумышленник, работающий вместе с жертвой, изменяет на ее компьютере имя файла или перемещает его в другой каталог. Когда жертва замечает пропажу файла, злоумышленник заявляет, что может все исправить. Желая быстрее завершить работу или избежать наказания за утрату информации, жертва соглашается на это предложение. Злоумышленник заявляет, что решить проблему можно, только войдя в систему с учетными данными жертвы. Теперь уже жертва просит злоумышленника войти в систему под ее именем, чтобы попытаться восстановить файл. Злоумышленник неохотно соглашается и восстанавливает файл, а по ходу дела крадет идентификатор и пароль жертвы. Успешно осуществив атаку, он даже улучшил

свою репутацию, и вполне возможно, что после этого к нему будут обращаться за помощью и другие коллеги. Этот подход не пересекается с обычными процедурами оказания услуг поддержки и осложняет поимку злоумышленника. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Социальная инженерия.

Общедоступная информация —

Общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

См. также: Открытая информация.

Общедоступные персональные данные [public personal data] —

Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. *["Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСБ РФ 21.02.2008 N 149/6/6-622)]*.

Выше: Персональные данные.

См. также: Информационная система, обрабатывающая общедоступные персональные данные.

Общие методы обеспечения информационной безопасности —

Общие методы обеспечения информационной безопасности разделяются на правовые, организационно-технические и экономические. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Ниже: Организационно-технические методы обеспечения информационной безопасности, Правовые методы обеспечения информационной безопасности, Экономические методы обеспечения информационной безопасности.

См. также: Объект обеспечения информационной безопасности.

Объединение рисков [risk aggregation] —

Объединение нескольких видов риска в один риск, выполняемое для более полного понимания совокупного риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Агрегирование риска.

Объект [object] **—**

1. Пассивная сущность в пределах объекта оценки, которая содержит или получает информацию и над которой субъекты выполняют операции. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Пассивный компонент системы, хранящий, принимающий или передающий информацию. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

3. Любая часть, элемент, устройство, подсистема, функциональная единица, аппаратура или система, которые можно рассматривать в отдельности.

Примечания:

1. Объект может состоять из технических средств, программных средств или их сочетания и может также в частных случаях включать технический персонал.

2. Ряд объектов, например, их совокупность или выборка, может рассматриваться как объект. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Ниже: Информационный объект

См. также: Защита объекта, Субъект

Объект доступа (в автоматизированной информационной системе) —

Единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Доступ (в автоматизированной информационной системе).

Объект информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Объект (объекты) ВСС РФ, воздействие на который [которые] может привести к реализации угрозы информационной безопасности ВСС РФ.

Примечание - управление объектом [объектами] в соответствии с заданной политикой информационной безопасности ВСС РФ в отношении специфических действий, относящихся к информационной безопасности ВСС РФ, осуществляется единым руководящим органом [администратором] системы обеспечения информационной безопасности ВСС РФ. *[ОСТ 45.127-99*

Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].

См. также: Информационная безопасность Взаимоувязанной сети связи Российской Федерации, Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Объект защиты информации —

Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Защищенность объекта защиты, Носитель информации, Информационный процесс, Цель защиты информации.

Объект информатизации [information target] —

Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

Ниже: Защищаемый объект информатизации.

См. также: Информационная безопасность объекта информатизации.

Объект обеспечения информационной безопасности —

Лицо, организация, информационный ресурс, средства и система передачи, приема, обработки и отображения информации в различных системах разведки, управления и сферах деятельности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Обеспечение информационной безопасности организации, Общие методы обеспечения информационной безопасности, Меры обеспечения информационной безопасности.

Объект оценки [target of Evaluation (TOE)] —

Совокупность программного, программно-аппаратного и/или аппаратного обеспечения, возможно сопровождаемая руководствами.

Примерами объекта оценки являются:

- прикладная программа;
- операционная система;
- прикладная программа в сочетании с операционной системой;
- прикладная программа в сочетании с операционной системой и рабочей станцией;
- операционная система в сочетании с рабочей станцией;
- интегральная схема смарт-карты;

- локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства;

- приложение базы данных за исключением программных средств удаленного клиента, обычно ассоциируемых с приложением базы данных. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Орган оценки, Система оценки, Уязвимость (объекта оценки), Внешняя сущность (для объекта оценки), Задание по безопасности, Требование безопасности (объекта оценки), Политика безопасности объекта оценки, Проблема безопасности (объекта оценки), Профиль защиты, Ресурс объекта оценки, Функциональные возможности безопасности объекта оценки, Роль.

Объект среды информационного актива —

Материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.). *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Информационный актив

Объект технического контроля [item under inspection] **—**

Подвергаемая контролю продукция, процессы ее создания, применения, транспортирования, хранения, технического обслуживания и ремонта, а также соответствующая техническая документация. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

См. также: Метод контроля.

Объекты авторских прав —

Объектами авторских прав являются произведения науки, литературы и искусства независимо от достоинств и назначения произведения, а также от способа его выражения:

- литературные произведения;

- драматические и музыкально-драматические произведения, сценарные произведения;

- хореографические произведения и пантомимы;

- музыкальные произведения с текстом или без текста;

- аудиовизуальные произведения;

- произведения живописи, скульптуры, графики, дизайна, графические рассказы, комиксы и другие произведения изобразительного искусства;

- произведения декоративно-прикладного и сценографического искусства;

- произведения архитектуры, градостроительства и садово-паркового искусства, в том числе в виде проектов, чертежей, изображений и макетов;

- фотографические произведения и произведения, полученные способами, аналогичными фотографии;

- географические, геологические и другие карты, планы, эскизы и пластические произведения, относящиеся к географии, топографии и к другим наукам;

- другие произведения.

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Автор результата интеллектуальной деятельности, Авторские права.

Объекты информатизации, аттестуемые по требованиям безопасности информации —

Автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров. *[Положение по аттестации объектов информатизации по требованиям безопасности информации. (утв. Председателем Гостехкомиссии 25.11.1994)]*.

См. также: Аттестация объектов информатизации.

Объекты информатизации, подлежащие обязательной аттестации —

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей тайну государственную, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации. *[Положение по аттестации объектов информатизации по требованиям безопасности информации" (утв. Гостехкомиссией РФ 25.11.1994)]*.

См. также: Аттестация объектов информатизации.

Объекты обеспечения информационной безопасности в области науки и техники —

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в области науки и техники являются:

• результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Российской Федерации;

• открытия, не запатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

• научно-технические кадры и система их подготовки;

• системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и другими). *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

См. также: Угрозы информационной безопасности в области науки и техники.

Объекты обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах —

Основными объектами обеспечения информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

• информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

• средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

• технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

• помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

См. также: Угрозы информационной безопасности в общегосударственных информационных и телекоммуникационных системах.

Объекты обеспечения информационной безопасности в правоохранительной и судебной сферах —

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

• информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

• информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

• информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи). *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Угрозы информационной безопасности в правоохранительной и судебной сферах.

Объекты обеспечения информационной безопасности в сфере внешней политики —

К наиболее важным объектам обеспечения безопасности информационной Российской Федерации в сфере внешней политики относятся:

• информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

• информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

• информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

• блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, ее мнения по социально значимым событиям российской и международной жизни. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*..

См. также: Угрозы информационной безопасности в сфере внешней политики

Объекты обеспечения информационной безопасности в сфере внутренней политики —

Наиболее важными объектами обеспечения информационной безопасности Российской Федерации в сфере внутренней политики являются:

• конституционные права и свободы человека и гражданина;

• конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Российской Федерации;

• открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Угрозы информационной безопасности в сфере внутренней политики.

Объекты обеспечения информационной безопасности в сфере духовной жизни —

К числу основных объектов обеспечения информационной безопасности Российской Федерации в сфере духовной жизни относятся:

• достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества, преподавания;

• свобода массовой информации;

• неприкосновенность частной жизни, личная и семейная тайна;

• русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов государств участников Содружества Независимых Государств;

• языки, нравственные ценности и культурное наследие народов и народностей Российской Федерации;

• объекты интеллектуальной собственности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Угрозы информационной безопасности в сфере духовной жизни.

Объекты обеспечения информационной безопасности в сфере обороны —

К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся:

• информационная инфраструктура центральных органов военного управления и органов военного управления видов ВС РФ и родов войск, объединений, соединений, воинских частей и организаций, входящих в ВС РФ, научно-исследовательских учреждений МО РФ;

• информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

• программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

• информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Угрозы информационной безопасности в сфере обороны.

Объекты обеспечения информационной безопасности в сфере экономики —

Воздействию угроз информационной безопасности Российской Федерации в сфере экономики наиболее подвержены:

• система государственной статистики;

• кредитно-финансовая система;

• информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

• системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

• системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

См. также: Угрозы информационной безопасности в сфере экономики.

Объекты обеспечения информационной безопасности в условиях чрезвычайных ситуаций —

Наиболее уязвимыми объектами обеспечения информационной безопасности Российской Федерации в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

См. также: Угрозы информационной безопасности в условиях чрезвычайных ситуаций, Чрезвычайная ситуация.

Объекты смежных прав —

Объектами смежных прав являются:

1) исполнения артистов-исполнителей и дирижеров, постановки режиссеров - постановщиков спектаклей (исполнения), если эти исполнения выражаются в форме, допускающей их воспроизведение и распространение с помощью технических средств;

2) фонограммы, то есть любые исключительно звуковые записи исполнений или иных звуков либо их отображений, за исключением звуковой записи, включенной в аудиовизуальное произведение;

3) сообщения передач организаций эфирного или кабельного вещания, в том числе передач, созданных самой организацией эфирного или кабельного вещания либо по ее заказу за счет ее средств другой организацией;

4) базы данных в части их охраны от несанкционированного извлечения и повторного использования составляющих их содержание материалов;

5) произведения науки, литературы и искусства, обнародованные после их перехода в общественное достояние, в части охраны прав публикаторов таких произведений. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Смежные права, Знак правовой охраны смежных прав.

Обязательные требования —

Обязательные для применения и исполнения требования в области технического регулирования, предъявляемые к продукции (работам, услугам), а также процессам, установленные нормативными правовыми актами Российской Федерации, нормативными правовыми актами федерального органа исполнительной власти, уполномоченного в области внешней разведки, принятыми в пределах его компетенции, и документами в области стандартизации, устанавливающими указанные требования. *[Постановление Правительства РФ от 21.04.2010 N 266 " Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения". Вступило в силу 12.05.2010]*.

Ниже: Требования по защите информации.

Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне —

Могут касаться: права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне; права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения; права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне. *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Допуск к государственной тайне.

Ограниченный доступ [restricted access] **—**

Доступ к информационному ресурсу, разрешаемый установленными для данного ресурса правилами доступа только определенному кругу лиц, обладающих соответствующими полномочиями. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Доступ.

См. также: Контроль доступа, Механизм (средство) разграничения доступа.

Однократный вход —

См. Единая авторизация.

Одноразовая цифровая подпись [one-time digital signature] —

Цифровая подпись, сформированная с использованием схемы цифровой подписи, в которой после проведения процедуры проверки правильности цифровой подписи необходимо осуществить смену ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Цифровая подпись.

См. также: Многократная цифровая подпись.

Одноразовый блокнот [one-time pad] —

Записанный на некотором материальном носителе (например, в специальных бумажных блокнотах) набор данных, используемых для получения управляющих последовательностей для однократного шифрования. Этот набор данных, обладающий определенными свойствами, должен обеспечивать совершенную стойкость (шифрсистемы) при однократном применении. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Одноразовый пароль [One-Time Password (OTP)] —

Пароль, действительный только для одного сеанса аутентификации. Действие одноразового пароля также может быть ограничено определённым промежутком времени. Преимущество одноразового пароля по сравнению со статическим состоит в том, что пароль невозможно использовать повторно. Таким образом, злоумышленник, перехвативший данные из успешной сессии аутентификации, не может использовать скопированный пароль для получения доступа к защищаемой информационной системе. Использование одноразовых паролей само по себе не защищает от атак, основанных на активном вмешательстве в канал связи, используемый для аутентификации (например, от атак типа «человек посередине»). *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Аутентификация на основе одноразовых паролей.

Одноразовый пароль по дополнительному каналу [One-Time Passwords Out-Of-Band (OTP OOB)] —

Технология усиления аутентификации, основанная на передаче одноразового пароля с использованием канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе, например, с помощью службы коротких сообщений SMS, электронной почты и т. п. Применяется для защиты от атак «противник в середине», создание подложного сайта и др. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*.

См. также: Одноразовый пароль, Аутентификация на основе одноразовых паролей.

Одноранговая сеть [Peer-to-Peer network, P2P] —

Децентрализованная оверлейная («надстоечная») компьютерная сеть, основанная на равноправии участников. В такой сети отсутствуют выделенные серверы, а каждый узел (peer) является как клиентом, так и сервером. Будучи сервером, каждая машина должна быть способной обрабатывать запросы от других машин в сети, отсылать то, что было запрошено. Каждая машина также должна выполнять некоторые вспомогательные и административные функции (например, хранить список других известных машин — «соседей» и поддерживать его актуальность). В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Любой узел данной сети не гарантирует свое присутствие на постоянной основе. Он может появляться и исчезать в любой момент времени. Одноранговые сети используются для обмена файлами (torrent), организации распределенных вычислений (компания Sony использует в игровых приставках PlayStation), в сетях с деньгами цифровыми (bitcoin), для управления бот-сетями и др. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Компьютерная сеть.

Син.: Пиринговая сеть.

Односторонняя аутентификация [one-way authentication] —

Аутентификация сторон, при которой одна из сторон проверяет, что взаимодействующая с ней сторона — именно та, за которую себя выдает. Односторонняя аутентификация реализуется протоколом идентификации с двумя участниками: доказывающим и проверяющим. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Аутентификация сторон.

Односторонняя подстановка [one-way permutation] —

Взаимно однозначная односторонняя функция. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Односторонняя хеш-функция [one-way hash function (OWHF)] —

Хеш-функция, для которой задача поиска прообразов заданных значений является вычислительно трудной. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Хеш-функция.

Опасная ситуация —

Обстоятельства, в которых люди, имущество или окружающая среда подвергаются опасности. *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]*.

См. также: Опасность.

Опасность [hazard] —

1. Источник потенциального вреда.

Примечание. Опасность может быть источником риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk*

Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].

2. Свойство объекта, характеризующее его способность наносить ущерб или вред другим объектам. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009].*

См. также: Источник риска, Опасная ситуация, Оценка опасности, Предупреждение об опасности, Ущерб.

Оперативная память [operating storage] —

Память, в которой размещаются данные, над которыми непосредственно производятся операции процессора.

Примечание. Оперативная память может иметь несколько иерархических уровней. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

Выше: Память.

См. также: Основная память.

Оператор (персональных данных) —

Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007].*

См. также: Обработка персональных данных.

Оператор связи (электрической или почтовой) —

Юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии. *[Федеральный закон от 07.07.2003 N 126-ФЗ “О связи” (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004].*

См. также Услуга связи, Пользователь услугами связи, Политика безопасности оператора связи.

Оператор информационной системы —

Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006].*

См. также: Информационная система.

Операционная система [operating system] —

1. Программное средство, которое управляет исполнением программ и которое может обслуживать выделение ресурсов, планирование, управление вводом-выводом и управление данными.

Примечание. Операционные системы обычно реализуются на чисто программном уровне, но возможно частичное воплощение в хардверных программных средствах или хардвере. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Совокупность системных программ, предназначенная для обеспечения определенного уровня эффективности системы обработки информации за счет автоматизированного управления ее работой и предоставляемого пользователю определенного набора услуг. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Ниже: Защищенная операционная система.

Операция записи данных [write operation] —

Операция занесения порции данных в память данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Память данных.

Операция устройства вычислительной машины [operation] —

Однозначно определенное действие, выполняемое устройством вычислительной машины и составляющее выполнение команды или реакцию на определенные условия. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Операция чтения данных [read operation] —

Операция получения порции данных из памяти данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Память данных.

Описание риска [risk description] —

Структурированное утверждение о риске, обычно содержащее описание четырех элементов: источников, событий, причин и последствий. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Источник риска, Последствие (в области риск-менеджмента), Событие.

Определение приемлемости уровня риска —

Процесс сравнения результатов анализа риска с критериями риска с целью определения приемлемости или допустимости уровня риска. Примечание. Определение приемлемости уровня риска помогает принять решения об обработке риска. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Син.: Оценивание риска.

См. также: Анализ риска (информационного), Критерии риска, Допустимый риск.

Орган по аккредитации —

Полномочный орган, проводящий аккредитацию.

Примечание. Обычно полномочия органа по аккредитации исходят от правительства. *[ГОСТ ИСО/МЭК 17011-2009 Оценка соответствия. Общие требования к органам по аккредитации, аккредитующим органы по оценке соответствия. Введен в действие: 01.07.2010]*.

См. также: Аккредитация.

Орган оценки [evaluation authority] —

Организация, устанавливающая стандарты и контролирующая качество оценок, проводимых организациями в пределах определенного сообщества, и обеспечивающая реализацию ИСО/МЭК 15408 для данного сообщества посредством системы оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Система оценки.

Орган по сертификации —

1. Юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

2. Юридическое лицо, аккредитованное в установленном порядке для выполнения работ по обязательной сертификации продукции. *[Постановление Правительства РФ от 21.04.2010 N 266 " Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения". Вступило в силу 12.05.2010]*.

См. также: Сертификация, Федеральные органы по сертификации.

Орган сертификации [certification body] —

Третья сторона, оценивающая и сертифицирующая СМИБ организации-клиента на соответствие действующим стандартам СМИБ и любой дополнительной документации, требуемой в рамках этой системы. *[ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и*

сертификацию систем менеджмента информационной безопасности. Введен в действие: 01.10.2009].

См. также: Документ сертификации, Сертификат.

Организационная защита информации —

Защита информации, осуществляемая путем принятия административных мер. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Защита информации.

Ниже: Организационно-технические мероприятия по защите информации, Организационно-технические методы обеспечения информационной безопасности, Организационные мероприятия по защите информации.

См. также: Техническая защита информации, Правовая защита информации, Физическая (непосредственная) защита информации.

Организационно-технические мероприятия по защите информации —

Совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации.

Примечание 1. Организационно-технические мероприятия по обеспечению защиты информации должны осуществляться на всех этапах жизненного цикла объекта информатизации.

Примечание 2. Организационные меры предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Организационная защита информации.

См. также: Организационные меры обеспечения информационной безопасности.

Организационно-технические методы обеспечения информационной безопасности —

К организационно-техническим методам обеспечения безопасности информационной относят:

• создание и совершенствование системы информационной безопасности;

• усиление правоприменительной деятельности органов власти, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

• разработка, использование и совершенствование средств ЗИ и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

• создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также

изменение штатных режимов функционирования систем и средств информатизации и связи;

• выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств ЗИ при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по ЗИ;

• сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств ЗИ;

• совершенствование системы сертификации телекоммуникационного оборудования и обеспечения программного систем автоматизированных обработки информации по требованиям информационной безопасности;

• контроль над действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности;

• формирование системы мониторинга показателей и характеристик информационной безопасности в наиболее важных сферах жизни и деятельности общества и государства. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Организационная защита информации, Общие методы обеспечения информационной безопасности.

Организационное обеспечение автоматизированной системы [AS organizational support] —

Совокупность документов, устанавливающих организационную структуру, права и обязанности пользователей и эксплуатационного персонала АС в условиях функционирования, проверки и обеспечения работоспособности АС. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Автоматизированная система, Информационное обеспечение автоматизированной системы, Методическое обеспечение автоматизированной системы, Правовое обеспечение автоматизированной системы, Программное обеспечение автоматизированной системы, Техническое обеспечение автоматизированной системы.

Организационные мероприятия по защите информации —

Мероприятия по защите информации, предусматривающие установление временных, территориальных и пространственных ограничений на условия использования и режима работы объекта защиты. *[ОСТ В1 00464-82 Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. Введен в действие: 01.01.1998]*.

Выше: Организационная защита информации

Организационные меры обеспечения информационной безопасности [information security measure] —

1. Совокупность действий, определяемых нормативно-правовой документацией организации, по обеспечению информационной безопасности без применения технических средств защиты. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009]*.

2. Меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Выше: Организационная защита информации, Меры обеспечения информационной безопасности.

Организация [organization] —

1. Государственная или частная компания, корпорация, фирма, предприятие, управление или учреждение или их часть, или их комбинация, имеющая собственные функции и администрацию и способная обеспечить информационную безопасность. *[ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введен в действие: 01.10.2009]*.

2. Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений.

Примечания:

1. К организации относятся: компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, предприятие розничной торговли, ассоциация, а также их подразделения или комбинация из них.

2. Распределение обычно бывает упорядоченным.

3. Организация может быть государственной или частной. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

3. Юридическое лицо, которое имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде, а также имеющее самостоятельный баланс или смету и зарегистрированное в установленном

порядке. *[ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. Стандарты организаций. Общие положения. Введен в действие: 01.07.2005]*.

См. также: Информационная безопасность организации, Политика

Осведомленность об идентификационных данных [Identity Awareness] —

Технология централизованного управления доступом пользователей к ресурсам компании и Интернет приложениям, помогающая организации управлять индивидуальными политиками безопасности, включающими отдельных внутренних и внешних пользователей, группы пользователей и отдельные устройства. Позволяет организации осуществлять эффективный контроль за приложениями и контроль доступа через создание четких политик безопасности, основанных на идентификационных данных. Централизованное управление и мониторинг позволяют контролировать выполнение политик с одной унифицированной консоли. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Управление приложениями.

Основная память [main storage] —

Оперативная память центрального процессора или ее часть, представляющая единое пространство памяти. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Оперативная память.

Основные направления международного сотрудничества Российской Федерации в области обеспечения информационной безопасности —

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

• запрещение разработки, распространения и применения «информационного оружия»;

• обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

• координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

• предотвращение несанкционированного доступа к информации конфиденциальной в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Международная информационная безопасность.

Основные способы несанкционированного доступа —

К основным способам несанкционированного доступа относятся:

• непосредственное обращение к объектам доступа;

• создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;

• модификация средств защиты, позволяющая осуществить несанкционированный доступ;

• внедрение в технические средства средств вычислительной техники или автоматизированной системы программных или технических механизмов, нарушающих предполагаемую структуру и функции средства вычислительной техники или автоматизированной системы и позволяющих осуществить несанкционированный доступ. *[Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Син.: Способы несанкционированного доступа.

См. также: Несанкционированный доступ.

Основные технические средства и системы (ОТСС) —

Технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. В контексте настоящего документа к ним относятся технические средства и системы автоматизированных систем различного уровня и назначения на базе средств вычислительной техники, средства и системы связи и передачи данных, используемые для обработки конфиденциальной информации. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

См. также: Защищаемые помещения, Вспомогательные технические средства и системы (ВТСС).

Осознание необходимости обеспечения информационной безопасности —

Понимание руководством организации банковской системы Российской Федерации необходимости самостоятельно на основе принятых в этой организации ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по обеспечению безопасности информационной, а также поддерживать эту деятельность адекватно прогнозу.

Примечание. Осознание безопасности информационной является внутренней побудительной причиной для руководства банковской системы Российской Федерации инициировать и поддерживать деятельность по обеспечению безопасности информационной, в отличие от побуждения или принуждения, когда решение об инициировании и поддержке деятельности по обеспечению безопасности информационной определяется соответственно либо возникшими проблемами организации, либо внешними факторами, например,

требованиями законов. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Остаточная уязвимость (объекта оценки) [residual vulnerability] —

Слабое место объекта оценки, которое не может быть использовано в среде функционирования объекта оценки, но которое может быть использовано для нарушения функциональных требований безопасности нарушителем с более высоким потенциалом нападения, чем предполагается в среде функционирования объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Уязвимость (объекта оценки), Требование безопасности (объекта оценки), Потенциал нападения.

Остаточный риск [residual risk] —

1. Риск, сохраняющийся после воздействия на риск.

Примечание 1. Остаточный риск может содержать в себе неидентифицированный риск.

Примечание 2. Остаточный риск может быть также известен как «удержанный риск». *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Риск, остающийся после его обработки. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

3. Риск, остающийся после предпринятых защитных мер. [ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]

Выше: Риск.

См. также: Остаточный риск нарушения информационной безопасности.

Остаточный риск нарушения информационной безопасности —

Риск, остающийся после обработки риска нарушения информационной безопасности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Риск нарушения информационной безопасности.

См. также: Остаточный риск.

Отказ в обслуживании (несанкционированное блокирование доступа к информации) [Denial of Service, DoS] —

1. Прекращение санкционированного доступа к ресурсам системы или задержка операций и функций системы, приводящее в итоге к потере

доступности для авторизованных пользователей. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Создание условий, препятствующих доступу к информации (ресурсам системы информационной) субъекту, имеющему право на него.

Примечание 1. Несанкционированное блокирование доступа осуществляется нарушителем безопасности информации, а санкционированное — администратором.

Примечание 2. Создание условий, препятствующих доступу к информации (ресурсам системы информационной), может быть осуществлено по времени доступа, функциям по обработке информации (видам доступа) и (или) доступным ресурсам информационным. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Атака на отказ в обслуживании.

Отказоустойчивая система [faulttolerant system] —

Компьютерная система, которая при возникновении отказа сохраняет свои функциональные возможности в полном или уменьшенном объеме. Отказоустойчивость обычно обеспечивается сочетанием избыточности системы и наличия процедур обнаружения и устранения ошибок. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Живучесть.

Отклонение услуги —

Предотвращение санкционированного доступа к ресурсам или задержка операций, критичных ко времени. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды вторжений.

Открытая информация —

Информация, не имеющая ограничений по доступу к ней всех заинтересованных лиц. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также.: Общедоступная информация.

Открытое распределение ключей [public key distribution] —

Протокол совместной выработки пользователями секретного (общего) ключа путем обмена сообщениями по открытому каналу связи. Протокол должен исключать возможность получения информации о ключе посторонними, а также любым участником до завершения им действий, предусмотренных протоколом. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Протокол распределения ключей, Протокол (алгоритм) обмена ключами Диффи–Хеллмана.

Открытое сообщение [plaintext, cleartext] —

В широком смысле — данные, представленные в виде последовательности над конечным множеством (буквы, цифры и др. символы) или непрерывного сигнала (звуки, изображения и др.), подлежащие зашифрованию. В более узком смысле — аналогичные данные, обладающие доступным семантическим (смысловым) содержанием и предназначенные для хранения, преобразования или передачи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*

См. также: Шифрованное сообщение, Открытый текст.

Открытый ключ [public key] —

Несекретный ключ асимметричной шифрсистемы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ.

См. также: Закрытый ключ, Секретный ключ.

Открытый код [open source] —

Подход к проектированию, разработке и распространению программного обеспечения, предполагающий свободную доступность исходного кода. Полноценная лицензия для распространения программного обеспечения с открытым кодом должна удовлетворять таким условиям как: свободное последующее распространение; доступный исходный код; возможность модификации; сохранение целостности оригинального исходного кода и возможность свободного распространения производного кода; отсутствие дискриминационных ограничений по отношению к физическим или юридическим лицам; отсутствие дискриминационных ограничений по отношению к сферам использования; применяться ко всем пользователям без необходимости заключения дополнительных соглашений; не быть привязана к конкретному продукту; не ограничивать другое программное обеспечение; быть технологически нейтральной. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Открытый стандарт [open standard] —

Стандарт, обладающий общедоступной спецификацией, допускающий безвозмездное использование и свободную реализацию всеми желающими. Открытые стандарты охватывают различные элементы информационно-коммуникационных технологий— форматы представления данных, протоколы обмена данными, языки программирования, архитектурные аспекты программных систем и технических средств и т. д. Открытые стандарты обеспечивают интероперабельность, мобильность и масштабируемость соответствующих им компьютерных систем и/или программного обеспечения. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Выше: Стандарт.

См. также: Закрытый стандарт.

Открытый текст [plaintext] —

1. Смысловые данные, семантическое содержимое которых доступно. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Открытое сообщение, представленное в виде последовательности над конечным алфавитом. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Модель открытого текста, Открытое сообщение, Шифрованный текст (шифртекст).

Отнесение сведений к государственной тайне и их засекречивание —

Введение в предусмотренном законом «О государственной тайне» порядке для сведений, составляющих государственную тайну, ограничений на их распространение и на доступ к их носителям. *[Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Государственная тайна, Рассекречивание сведений и их носителей.

Отношение к риску [risk attitude] —

Подход организации к оценке и, в конечном счете, к использованию благоприятных возможностей, удержанию, принятию или избеганию риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Оценка риска.

Отображение, не размножающее искажений [mapping free of error propagation] —

См. Отображение, не распространяющее искажений

Отображение, не распространяющее искажений [mapping free of error propagation] —

Отображение множества всех слов конечных длин в алфавите X в множество всех слов конечных длин в алфавите Y, сохраняющее длины слов, для которого расстояние Хемминга между образами любых слов одинаковой длины не превосходит расстояния Хемминга между исходными словами. Вместе с описанными искажениями типа замены букв, иногда рассматривают искажения типа пропуска букв, вставки букв и др. (с соответствующей заменой метрики). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Отображение, не размножающее искажений.

См. также: Преобразование, не распространяющее искажений.

Отрицание [repudiation] —

Отрицание одним из участвующих в коммуникации субъектов своего участия во всей или части коммуникации. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая*

эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].

Отчетность (ресурсов информационной системы) [accountability] —

Состояние ресурсов информационной системы, при котором обеспечиваются идентификация и регистрация действий с ними. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006].*

Син.: Подотчетность (ресурсов автоматизированной информационной системы).

См. также: Ресурс (информационной системы).

Отчетность о риске [risk reporting] —

Форма обмена информацией, предусматривающая информирование соответствующих внутренних и внешних сторон, заинтересованных путем предоставления информации о текущем состоянии риска и управлении им. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

См. также: Управление рисками.

Официальный стандарт [official standard] —

Стандарт, спецификация которого одобрена официальным национальным или международным органом стандартизации и опубликована под его эгидой. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009].*

Выше: Стандарт.

Охраняемые сведения —

Сведения, составляющие государственную или иную охраняемую законом тайну. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)].*

См. также: Сведения конфиденциального характера, Государственная тайна.

Оценивание риска [risk evaluation] —

1. Процесс сравнения результатов анализа риска установленными критериями риска для определения, является ли риск и/или его величина приемлемыми или допустимыми.

Примечание. Оценивание риска способствует принятию решения относительно воздействия на риск. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

2. Основанная на результатах анализа риска процедура проверки, устанавливающая, не превышен ли допустимый риск. *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]*.

Син.: Определение приемлемости уровня риска.

См. также: Анализ риска (информационного), Критерии риска, Допустимый риск, Воздействие на риск.

Оценка [evaluation] —

Оценка профиля защиты, задания по безопасности или объекта оценки по определенным критериям *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Задание по безопасности, Профиль защиты, Объект оценки.

Оценка защиты [security evaluation] —

Экспертиза компьютерной системы с целью определения степени ее соответствия стандарту безопасности, установленной модели защиты и техническим условиям. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Модель защиты.

Оценка информационного риска [information risk assessment] —

Общий процесс анализа информационного риска и его оценивания. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Син.: Оценка риска.

См. также: Анализ риска (информационного), Оценивание риска.

Оценка опасности —

Определение степени возможного деструктивного воздействия. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Опасность.

Оценка риска [risk assessment] —

1. Общий процесс идентификации риска, анализа риска и оценивания риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Процесс, объединяющий идентификацию риска, анализ риска и оценивание риска. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

3. Выявление угроз безопасности информации, уязвимостей информационной системы, оценка вероятностей реализации угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной системы, используемой для обработки этой информации. *[Р 50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Син.: Оценка информационного риска.

См. также: Отношение к риску, Анализ риска (информационного), Оценивание риска.

Оценка риска информационной безопасности (организации) —

Общий процесс идентификации, анализа и определения приемлемости уровня риска информационной безопасности организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Менеджмент риска информационной безопасности организации, Определение приемлемости уровня риска, Анализ риска (информационного).

Оценка риска нарушения информационной безопасности —

Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения безопасности информационной, связанных с использованием информационных активов организации банковской системы Российской Федерации на всех стадиях их жизненного цикла. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Оценка риска.

Оценка соответствия [evaluation] —

Прямое или косвенное определение соблюдения требований, предъявляемых к объекту. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

См. также: Сертификат соответствия, Технический регламент.

Оценка соответствия информационной безопасности организации установленным требованиям —

Деятельность, связанная с прямым или косвенным определением выполнения или невыполнения в организации установленных требований информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Мониторинг информационной безопасности организации.

Оценка соответствия требованиям по защите информации [computer security evaluation] —

Прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Оценка соответствия информационной безопасности организации установленным требованиям.

Оценочный уровень доверия [evaluation assurance level] —

1. Набор требований доверия, представляющий некоторое положение на предопределенной шкале доверия и составляющий пакет доверия. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Пакет компонентов доверия, представляющий некоторое положение на предопределенной в нем шкале доверия.

Примечание. Пакет компонентов доверия определяется в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Пакет.

Пакет [package] —

Именованная совокупность функциональных требований безопасности или требований доверия к безопасности.

Примечание. Примером пакета может служить "Оценочный уровень доверия 3". [*ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Требование безопасности (объекта оценки), Оценочный уровень доверия.

Пакет прикладных программ [application program package] —

Система прикладных программ, предназначенная для решения задач определенного класса. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]* .

См. также: Прикладная программа.

Пакетная фильтрация [packet filtering] —

Процесс пропускания или блокирования пакетов в сети на основе значений адресов отправителя и получателя, портов или протоколов. Пакетная фильтрация, как правило, является частью программного обеспечения firewall, защищающего локальную сеть от нежелательных вторжений. В программном обеспечении firewall, пакетная фильтрация выполняется программой, называемой пакетным фильтром. Пакетный фильтр проверяет заголовок каждого пакета с помощью специального набора правил, на основе которых

принимает решение о блокировании передачи пакета (DROP) или разрешении его передачи (ACCEPT). Существует три способа конфигурирования пакетного фильтра для реализации установленных правил фильтрации. В первом методе фильтр разрешает только те пакеты, которые признаются безопасными, запрещая все остальные. Это наиболее безопасный метод, но он может вызвать неудобства, связанные с излишним блокированием легитимных пакетов. Во втором методе, фильтр запрещает только те пакеты, которые признаются опасными, разрешая все остальные. Это менее безопасный метод, но он причиняет меньше неудобств при работе с Web браузером. В третьем методе, если фильтр встречает пакет, для которого правилами не предусмотрено никаких инструкций, то он помещает его в карантин, либо пользователь может сам определить необходимые инструкции о том, что делать с пакетом. Это может быть неудобным, так как вызывает появление значительного диалога при работе с Web браузером. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Фильтрация.

См. также: Межсетевой экран (сетевой экран).

Память [memory] —

Все адресное пространство хранения в блоке обработки и все другие внутренние устройства хранения, которые используются, чтобы исполнять инструкции. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Ниже: Внешняя память, Оперативная память.

См. также: Загрузка в память, Область памяти.

Память данных [storage] —

Функциональная часть вычислительной машины или системы обработки информации, предназначенная для приема, хранения и выдачи данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Запоминающее устройство, Операция записи данных, Операция чтения данных.

Паразитное излучение —

Побочное излучение, возникающее в результате самовозбуждения электронного устройства из-за паразитных связей в генераторных и усилительных приборах или каскадах. Ведет к образованию неконтролируемого канала утечки информации. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Паразитное электромагнитное излучение.

Паразитное электромагнитное излучение —

Электромагнитное излучение, являющееся результатом паразитной генерации в электрических цепях технических средств обработки информации. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации.*

Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008].

См. также: Побочные электромагнитные излучения и наводки.

Параметр схемы ЭЦП [domain parameter] —

Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Схема цифровой подписи.

Пароль [password] —

1. Конфиденциальная информация аутентификации, обычно состоящая из строки знаков. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Идентификатор субъекта доступа, который является его (субъекта) секретом. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

3. Последовательность символов, задающая ключ или служащая для получения доступа к средствам криптографическим, вычислительным средствам и пр. Часто п. обладают лингвистическими особенностями, способствующими их запоминанию. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Пароль доступа.

См. также: Взламывание пароля.

Пароль доступа [password] —

Идентификатор субъекта доступа, который является его (субъекта) секретом. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Син.: Пароль.

Пассивная атака [passive attack] —

Атака на криптосистему или криптографический протокол, при которой противник и или нарушитель наблюдает и использует передаваемые шифрованные сообщения, но не влияет на действия законных пользователей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

См. также: Активная атака.

Пассивная угроза [passive threat] —

Угроза несанкционированного раскрытия информации без изменения состояния системы.

Примечание. К пассивным угрозам относятся те, которые при их реализации не приводят к какой-либо модификации любой информации, содержащейся в системе (системах), и где работа и состояние системы не изменяются. Одной из реализаций пассивной угрозы является использование перехвата для анализа информации, передаваемой по каналам связи. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды угроз, Угроза.

Пассивный нарушитель [passive adversary, eavesdropper] —

Нарушитель, который ограничивается сбором и анализом информации о ходе выполнения криптографического протокола, но не вмешивается в него. Полный анализ результатов неоднократного выполнения криптографического протокола не позволяет обнаружить присутствие пассивного нарушителя. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Нарушитель.

См. также: Активный нарушитель.

Пассивный противник [passive adversary, eavesdropper] —

Противник, который может получать некоторую информацию о выполнении криптографического протокола или работы криптографической системы, но не вмешивается в их работу. В случае протоколов полный анализ результатов неоднократного их выполнения не позволяет обнаружить присутствие пассивного противника. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Противник.

См. также: Активный противник.

Патентные права —

Интеллектуальные права на изобретения, полезные модели и промышленные образцы являются патентными правами.

Автору изобретения, полезной модели или промышленного образца принадлежат следующие права:

1) исключительное право;

2) право авторства. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

Ниже: Право авторства.

См. также: Изобретение, Контрафакт.

Передача информации, составляющей коммерческую тайну —

Передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности. *[Федеральный закон от*

29.07.2004 N 98-ФЗ “О коммерческой тайне” (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004].

См. также: Контрагент, Обладатель информации, составляющей коммерческую тайну, Предоставление информации, составляющей коммерческую тайну

Перекрытие гаммы [repeated use of a key sequence] —

Полное или частичное повторное использование гаммы (управляющей последовательности) при зашифровании двух или более различных открытых текстов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

См. также: Гамма (шифра).

Пересмотр [review] —

Деятельность, предпринимаемая для определения пригодности, адекватности и результативности предмета рассмотрения для достижения установленных целей.

Примечание. Процедуры пересмотра можно применять к структуре риск-менеджмента, процессу риск-менеджмента, риску или контролированию рисков. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

См. также: Менеджмент риска информационной безопасности организации.

Перехват (информации) —

Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006].*

Выше: Методы внешних вторжений.

См. также: Побочные электромагнитные излучения и наводки.

Перечень сведений, составляющих государственную тайну —

Совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством. *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993].*

См. также: Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.

Персональная ЭВМ [personal computer] —

Настольная микроЭВМ, имеющая эксплуатационные характеристики бытового прибора и универсальные функциональные возможности. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

Выше: Семейство ЭВМ.

Персональные данные [personal data] —

Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. [Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]

Выше: Сведения конфиденциального характера, Конфиденциальная информация.

Ниже: Личная тайна, Общедоступные персональные данные.

См. также: Безопасность персональных данных, Директива о приватности, Информационная система персональных данных, Обработка персональных данных, Оператор (персональных данных).

Пиринговая сеть [Peer-to-Peer network, P2P] —

См. Одноранговая сеть.

План аудита [audit plan] —

Описание деятельности и мероприятий по проведению аудита. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Программа аудита.

План восстановления ИКТ после бедствия [ICT disaster recovery plan - ICT DRP] —

Четко определенный и документально оформленный план по восстановлению возможностей ИКТ в случае возникновения нарушения.

Примечание. В некоторых организациях его называют планом обеспечения непрерывности ИКТ. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: Восстановление ИКТ после бедствия, Нарушение, Заданное время восстановления (ЗВВ), Заданная точка восстановления (ЗТВ).

План менеджмента риска [risk management plan] —

Краткое, схематичное описание деятельности и мероприятий в пределах структуры менеджмента риска, устанавливающих подход, элементы менеджмента и ресурсы, применяемые для менеджмента риска.

Примечание 1. Элементы менеджмента обычно включают в себя процедуры, методы, распределение ответственности, последовательность действий и сроки их исполнения.

Примечание 2. План менеджмента риска может быть применен к конкретной продукции, процессу и проекту, к части или всей организации. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: План управления рисками.

План обеспечения непрерывности бизнеса (ПНБ) [business continuity plan - BCP] —

Документированные процедуры, которым следует организация при осуществлении реагирования, восстановления, возобновления и возвращения к заранее определенному уровню операций после нарушения.

Примечание. Обычно он охватывает ресурсы, услуги и мероприятия, необходимые для обеспечения непрерывности критических функций бизнеса. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: Планирование непрерывности бизнеса.

План работ по обеспечению информационной безопасности —

Документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению информационной безопасности организации банковской системы Российской Федерации, их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

План управления рисками [risk management plan] —

Руководящий документ в системе риск-менеджмента, определяющий подход, элементы управления и ресурсы, используемые в управлении риском.

Примечание 1. Элементы управления обычно включают процедуры, практики, распределение обязанностей и ответственности, последовательность и время деятельности.

Примечание 2. План управления рисками может применяться для конкретного продукта, процесса и проекта, а также к части или ко всей организации. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*

См. также: Управление рисками.

Планирование непрерывности бизнеса [business continuity planning] —

Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов.

Примечание. Данный процесс должен также обеспечивать восстановление бизнеса с учетом заданных очередностей и интервалов времени и дальнейшее восстановление всех функций бизнеса в рабочее состояние. Ключевые элементы этого процесса должны обеспечивать применение и тестирование необходимых планов и средств и включение в них информации, бизнес-

процессов, информационных систем и сервисов, речевой связи и передачи данных, персонала и физических устройств. *[ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Введен в действие: 01.07.2008]*.

См. также: План обеспечения непрерывности бизнеса (ПНБ), Менеджмент непрерывности бизнеса (МНБ).

Платежный терминал [cash-in terminal] —

См. Банкомат.

Платежный терминал самообслуживания [self-service cash-in terminal] —

См. Банкомат.

Побочное электромагнитное излучение —

1. Электромагнитное излучение, наблюдаемое при работе технических средств обработки информации. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

2. Электромагнитное излучение, возникающее при работе технических средств обработки информации. *[ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

См. также: Паразитное электромагнитное излучение, Наводка, Побочные электромагнитные излучения и наводки.

Побочные электромагнитные излучения и наводки —

1. Электромагнитные излучения средств технических обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также наводки электромагнитные этих сигналов на токопроводящие линии, конструкции и цепи питания. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной информации. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Побочное электромагнитное излучение, Наводка.

Поведенческий блокиратор —

См. Антивирусные базы данных.

Повторное использование объекта [object reuse] —

Повторное использование пространства памяти, которое может содержать фрагменты данных от объекта, содержавшегося на этом месте ранее. Для обеспечения безопасности пространство, выделяемое под объекты, должно быть после использования очищено специальными мерами. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Подверженность риску [exposure] —

Степень подверженности организации и/или заинтересованных сторон воздействию события. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Подделка информации [forgery] —

Умышленная несанкционированная модификация информации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также Модификация информации.

Подделка межсайтового запроса [Cross-Site Request Forgery (CSRF или XSRF), one-click attack или session riding] —

Вид эксплойта, который передает на web-сайт неавторизованные команды от имени пользователя, которому web-сайт доверяет. В отличие от межсайтового скриптинга (XSS), который использует доверие, которое есть у пользователя к какому-либо сайту, CSRF использует доверие, которое имеется у сайта к браузеру пользователя. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Син.: Межсайтовая подделка запроса.

Подделка цифровой подписи [forgery] —

Реализация атаки на систему цифровой подписи. Состоит в создании противником и/или нарушителем, не владеющим секретным ключом, пары (сообщение, подпись), которая будет принята как корректная алгоритмом проверки цифровой подписи. В зависимости от того, для каких сообщений противник и/или нарушитель может подделывать подписи, различают подделку подписи универсальную цифровой, экзистенциальную подделку цифровой подписи и выборочную подделку цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Выборочная подделка цифровой подписи, Универсальная подделка цифровой подписи, Экзистенциальная подделка цифровой подписи.

Подлинность [authenticity] —

Свойство, гарантирующее, что субьект или ресурс идентичен заявленному. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

Син.: Аутентичность.

Подлинность (ресурсов автоматизированной информационной системы) —

Состояние ресурсов автоматизированной информационной системы, при котором обеспечивается реализация информационной технологии с использованием именно тех ресурсов, к которым субъект, имеющий на это право, обращается. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Подлинность.

Подлинность специального защитного знака —

Соответствие внешнего вида и наличие в СЗЗ совокупности характерных признаков, предусмотренных техническими условиями. *[Руководящий документ Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

Выше: Идентификация специального защитного знака.

См. также: Специальный защитный знак (СЗЗ).

Подлинный документ —

Документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом документе или выявленные иным путем, подтверждают достоверность его происхождения. *[ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения. Введен в действие: 01.03.2014]*.

Выше: Документ.

См. также: Реквизит документа.

Подмена [substitution] —

Атака на криптосистему, состоящая в перехвате противником и/или нарушителем сообщения, и замене его другим сообщением. При этом выбор последнего может зависеть от перехваченного сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

Подотчетность [auditability] —

1. Ответственность субьекта за его действия и решения. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Свойство, обеспечивающее однозначное прослеживание действий любого логического объекта. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Подотчетность (ресурсов автоматизированной информационной системы) —

Состояние ресурсов автоматизированной информационной системы, при котором обеспечиваются их идентификация и регистрация. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Син.: Отчетность (ресурсов информационной системы).

Подписанное сообщение [signed message] —

Набор элементов данных, состоящий из сообщения и дополнения, являющегося частью сообщения. *[ГОСТ Р34.10-2012 Информационная технология. Криптографическая защита информации. Процессы*

формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013].

См. также: Дополнение.

Подпрограмма [subprogram] **—**

Программа, являющаяся частью другой программы и удовлетворяющая требованиям языка программирования к структуре программы. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992].*

Подтвердить [confirm] **—**

Декларировать, что что-то детально проверено с независимым определением достаточности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].*

Позвенное шифрование —

Индивидуальное прикладное применение шифрования к данным на каждом звене системы обмена данных.

Примечание. Позвенное шифрование подразумевает, что данные, передаваемые через логический объект ретранслятора, должны иметь формат открытого текста. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].*

Выше: Шифрование.

См. также: Открытый текст.

Показатели устойчивости автоматизированной системы в защищенном исполнении —

Максимальные значения характеристик воздействующих факторов (импульсных электромагнитных полей, токов, напряжений), при которых значения параметров, определяющих устойчивость автоматизированной системы в защищенном исполнении, не выходят за пределы, установленные нормативными документами на систему конкретного типа. *[ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. Введен в действие: 01.07.2008].*

См. также: Устойчивость автоматизированной системы в защищенном исполнении к преднамеренному силовому электромагнитному воздействию.

Показатель защищенности информации —

Количественная или качественная характеристика безопасности информации, определяющая уровень требований, предъявляемых к конфиденциальности, целостности и доступности этой информации и реализуемых при ее обработке. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006].*

См. также: Защищенность информации, Безопасность информации (данных).

Показатель защищенности средств вычислительной техники [protection criterion of computer system] —

Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)].*

См. также: Защищенность средств вычислительной техники.

Показатель эффективности защиты информации —

Мера или характеристика для оценки эффективности защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008].*

См. также: Контроль эффективности защиты информации, Норма эффективности защиты информации, Эффективность защиты информации.

Поколение ЭВМ [computer generation] —

Классификационная группа ЭВМ, объединяющая ЭВМ по используемой технологии реализации ее устройств, а также по уровню развития функциональных свойств и программного обеспечения и характеризующая определенный период в развитии промышленности средств вычислительной техники. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

Поле данных [data field] —

Неразрывная область памяти, имеющая определенное назначение и обычно снабженная именем или идентификатором. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992].*

Полиморфные (зашифрованные) вирусы [polymorphic viruses] —

1. Вирусы, предпринимающие специальные меры для затруднения их поиска и анализа. Не имеют сигнатур, то есть не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001].*

2. Вирусы, использующие помимо шифрования кода специальную процедуру расшифровки, изменяющую саму себя в каждом новом экземпляре вируса, что ведет к отсутствию у него байтовых сигнатур. Расшифровщик не является постоянным - он уникален для каждого экземпляра вируса. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/].*

3. Вирус, предпринимающий специальные меры для затруднения своего обнаружения и анализа. Не имеет сигнатур, т. е., не содержит ни одного постоянного участка кода.

В большинстве случаев два образца одного и того же вируса-полиморфика не будут иметь ни одного совпадения. Достигается это за счет шифрования основного тела вируса и существенной модификации от копии к копии модуля-расшифровщика. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Компьютерный вирус.

Политика [policy] —

Общее намерение и направление, официально выраженное руководством. *[ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Введен в действие: 01.01.2014]*.

См. также: Организация.

Политика безопасности информации [information security policy] —

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Достоверная вычислительная база, Модель политики безопасности.

Политика безопасности (информации в организации) [organizational security policies] —

1. Совокупность правил, процедур или руководящих принципов в области безопасности для некоторой организации.

Примечание. Политика может быть также отнесена к какой-либо определенной среде функционирования. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

3. Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Син.: Политика безопасности организации.

См. также: Информационная безопасность организации.

Политика безопасности информационно-телекоммуникационных технологий (политика безопасности ИТТ) [ICT security policy] —

Правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

См. также: Безопасность информационно-телекоммуникационных технологий.

Политика безопасности объекта оценки [TOE security policy] —

Совокупность правил, регулирующих управление активами, их защиту и распределение в пределах объекта оценки. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Объект оценки.

Политика безопасности оператора связи —

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области обеспечения безопасности, которыми должен руководствоваться оператор связи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Оператор связи (электрической или почтовой), Безопасность связи.

Политика безопасности организации [organizational security policies] —

См. Политика безопасности (информации в организации).

Политика в области менеджмента риска [risk management policy] —

Заявление высшего руководства об общих намерениях, руководящих принципах и направлениях деятельности организации в области менеджмента риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Политика управления рисками.

См. также: Управление рисками.

Политика информационной безопасности (организации) [organizational information security policies] —

Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Примечание. Политики должны содержать:

• предмет, основные цели и задачи политики безопасности;

• условия применения политики безопасности и возможные ограничения;

• описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;

• права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;

• порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Информационная безопасность организации, Цель информационной безопасности (организации).

Политика информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Система мероприятий, направленных на обеспечение информационной безопасности ВСС РФ.

Примечание. Указанные мероприятия включают совокупность требований и правил по информационной безопасности ВСС РФ для объекта информационной безопасности ВСС РФ, выработанных в целях противодействия заданному множеству угроз информационной безопасности ВСС РФ с учетом ценности защищаемой информационной сферы и стоимости, системы обеспечения информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Политика сетевой безопасности [network security policy] —

Совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как должна обеспечиваться защита ее сетевой инфраструктуры и сервисов. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Домен безопасности, Безопасность информационной сети, Шлюз безопасности.

Политика управления рисками [risk management policy] —

Декларация общих намерений и направлений деятельности организации в отношении риск-менеджмента. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Стн.: Политика в области менеджмента риска.

См. также: Управление рисками.

Политика функции безопасности [security function policy] —

Совокупность правил, описывающих конкретный режим безопасности, реализуемый функциональными возможностями безопасности объекта оценки, и выраженных в виде совокупности функциональных требований безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Функциональные возможности безопасности объекта оценки, Требование безопасности (объекта оценки).

Полное шифрование жесткого диска [full disk encryption] —

Технология обеспечения автоматической защиты для всей информации на жестких дисках, включая данные пользователей, файлы операционной системы, временные и уничтоженные файлы. Для усиления защиты данных от несанкционированного доступа применяется многофакторная аутентификация при начальной загрузке, позволяющая идентифицировать пользователя, а шифрование защищает от потери данных при краже дисков. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*.

Полномочие —

Предоставление прав, гарантирующих доступ к ресурсам в соответствии с правами на доступ.

Примечание: Предусматривает два аспекта: рассматриваемые права являются правами на выполнение некоторой активности (такой как доступ к данным); и эти права предоставлены некоторому логическому объекту, агенту или процессу. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Список полномочий, Права доступа.

Полнота (протокола) [completeness property] —

Свойство криптографического протокола, означающее, что при выполнении честными участниками протокол решает ту задачу, для которой он создан. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Положение о применимости [statement of applicability] —

Документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации.

Примечание. Цели и меры управления основываются на результатах и выводах процессов оценки и обработки рисков, на требованиях законодательных или нормативных актов, на обязательствах по контракту и бизнес-требованиях организации по отношению к информационной безопасности. *[ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология.*

Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен в действие: 01.02.2008].

Син.: Ведомость применимости, Декларация о применимости.

Полуформальный [semiformal] —

Выраженный на языке с ограниченным синтаксисом и определенной семантикой. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Формальный, Неформальный.

Получение (добывание) информации —

Действия, связанные со сбором, обработкой и анализом фактов, связанных со структурой, свойствами и взаимодействием объектов и явлений, извлекаемых из поступающих сигналов и знаков. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

Выше: Обработка информации.

Пользователь [user] —

Любая сущность (человек-пользователь или внешний объект, находящиеся вне объекта оценки и взаимодействующие с ним) вне объекта оценки, которая взаимодействует с объектом оценки. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Внешний объект ИТ, Внешняя сущность (для объекта оценки), Уполномоченный пользователь (объекта оценки), Роль.

Пользователь автоматизированной системы [AS user] —

Лицо, участвующее в функционировании АС или использующее результаты ее функционирования. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Законный пользователь, Незарегистрированный пользователь, Пользователь (потребитель) информации.

Пользователь (потребитель) информации —

Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации, либо с их нарушением. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Пользователь автоматизированной системы, Законный пользователь, Незарегистрированный пользователь.

Пользователь сертификата ключа проверки электронной подписи [user of signature verification key certificate] —

Физическое лицо, использующее полученные в центре удостоверяющем сведения о сертификате ключа подписи для проверки принадлежности электронной подписи владельцу сертификата ключа проверки электронной подписи. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Владелец сертификата ключа проверки электронной подписи, Сертификат ключа проверки электронной подписи.

Пользователь сети —

Физические или юридические лица, имеющие доступ к ресурсам сети через терминал или другие средства связи, и процессы, выполняемые на различных ресурсах сети. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Сеть.

Пользователь системы обработки информации [user] **—**

Юридическое или фактическое лицо, применяющее систему обработки информации. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Система обработки информации.

Пользователь услугами связи —

Лицо, заказывающее и (или) использующее услуги связи. *[Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004]*.

Ниже: Абонент.

См. также: Услуга связи, Оператор связи.

Помехоустойчивость шифра [noise stability of a cipher] **—**

Способность шифра противостоять действию случайных помех (в отличие от целенаправленных действий противника), возникающих при передаче шифрованного сообщения по каналу связи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Шифр.

Пороговая криптографическая система [threshold cryptographic scheme] **—**

Криптографическая система, в которой секретный ключ распределен между n участниками так, что для функционирования системы необходима и достаточна совместная работа любых t участников, где $t < n$ — заданное число. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*

Выше: Криптографическая система.

Пороговая схема разделения секрета [threshold secret sharing scheme] **—**

Схема разделения секрета с n участниками для структуры доступа, в которой правомочными являются все коалиции, содержащие не менее t участников для некоторого t, а все коалиции с меньшим числом частников —

неправомочны. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема разделения секрета.

Последовательность псевдослучайных чисел [pseudo-random number sequence] —

Последовательность чисел, полученная в результате выполнения некоторого арифметического (вычислительного) процесса, используемая в конкретном случае вместо последовательности случайных чисел. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Последовательность случайных чисел.

Последовательность случайных чисел [random number sequence] —

Последовательность чисел, каждое из которых не может быть предсказано (вычислено) только на основе знания предшествующих ему чисел данной последовательности. *[ГОСТ Р34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Случайное число, Последовательность псевдослучайных чисел.

Последствие (в области риск-менеджмента) [consequence] —

Результат события, влияющий на цели.

Примечание 1. Событие может привести к ряду последствий.

Примечание 2. Последствие может быть определенным или неопределенным, и может иметь положительные и отрицательные влияния на цели.

Примечание 3. Последствия могут выражаться качественно или количественно.

Примечание 4. Первоначальные последствия могут усиливаться за счет эффекта домино. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Событие.

Поставщик трафика —

Одна из специализаций внутри организованных преступных группировок, занимающихся технологиями интернет-мошенничества; обозначает участника, который обеспечивает поток новых заражений компьютеров, принадлежащих лицам-клиентам системы дистанционного банковского обслуживания. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Интернет-мошенничество, Дроп, Заливщик, Дроповод-нальщик, Кардселлер, Кодер (программист), Поставщик трафика.

Постоянная антивирусная защита —

Запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность

совершаемые другими программами действия. Постоянная антивирусная защита проверяет не только файлы на различных носителях информации, но и оперативную память компьютера. Основная задача постоянной антивирусной защиты компьютера: обеспечивать максимальную безопасность при минимальном замедлении работы проверяемых на вредоносные действия программ. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Антивирусная программа.

Син.: Антивирусный монитор.

См. также: Антивирусная защита по требованию.

Постулаты Голомба [Golomb postulates] —

Сформулированные С. Голомбом постулаты для двоичных псевдослучайных последовательностей, используемых в криптографических приложениях. Согласно им последовательность должна удовлетворять определенным ограничениям на встречаемость знаков, мультиграмм и автокорреляционную функцию последовательности. Последовательности, удовлетворяющие постулатам Голомба, иногда называют псевдошумовыми. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Потенциал нападения [attack potential] —

1. Мера усилий, затрачиваемых при атаке на объект оценки, выраженная в показателях компетентности, ресурсов и мотивации нарушителя. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Нарушитель.

Потенциальная уязвимость (объекта оценки) [potential vulnerability] —

Предполагаемая, но не подтвержденная слабость объекта оценки.

Примечание — Предположение основывают на теоретически допустимой схеме нападения для нарушения функциональных требований безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Уязвимость (объекта оценки), Обнаруженные потенциальные уязвимости (объекта оценки).

Потенциально нежелательные программы [Potentially Unwanted Programs (PUPs), unwanted software] —

В отличие от вредоносных, не предназначены специально для того, чтобы нанести вред. Однако с их помощью можно нарушать компьютерную безопасность.

К потенциально нежелательным относятся программы рекламного характера, программы порнографического характера и другие потенциально нежелательные программы.

Программы рекламного характера (Adware) связаны с показом пользователю рекламной информации.

Программы порнографического характера (Pornware) связаны с показом пользователю информации порнографического характера.

Другие потенциально нежелательные программы (Riskware) – это чаще всего полезные программы, которыми многие пользуются. Однако если злоумышленники получат доступ к таким программам или внедрят их на компьютер пользователя, они могут использовать их функции, чтобы нарушать безопасность. Среди них программы-клиенты IRC, программы автодозвона (Dialers), программы для загрузки файлов, мониторы активности компьютерных систем, утилиты для работы с паролями, интернет-серверы служб FTP, HTTP или Telnet.

Другие потенциально нежелательные программы различают по функциям.

Client-IRC (Клиенты интернет-чатов) - пользователи устанавливают эти программы, чтобы общаться в ретранслируемых интернет-чатах (Internet Relay Chats). Злоумышленники используют их для распространения вредоносных программ.

Dialer (Программы автодозвона,«звонилки») - могут устанавливать телефонные соединения через модем в скрытом режиме.

Downloader (Программы-загрузчики) - могут загружать файлы с веб-страниц в скрытом режиме.

Monitor (Программы-мониторы) - позволяют наблюдать за активностью на компьютере, на котором установлены (смотреть, какие приложения работают, как они обмениваются данными с приложениями на других компьютерах).

PSWTool (Восстановители паролей) - позволяют просматривать и восстанавливать забытые пароли. С этойже целью их скрыто внедряют на компьютеры пользователей злоумышленники.

RemoteAdmin (Программы удаленного администрирования) - широко используются системными администраторами; позволяют получать доступ к интерфейсу удаленного компьютера, чтобы наблюдать за ним и управлять им. С этой же целью их скрыто внедряют на компьютеры пользователей злоумышленники для наблюдения за удаленными компьютерами и управления ими.

Потенциально нежелательные программы удаленного администрирования отличаются от троянских программ удаленного администрирования Backdoor. Троянские программы обладают функциями,

которые позволяют им самостоятельно проникать в систему и устанавливать себя; потенциально нежелательные программы этими функциями не обладают.

Server-FTP (FTP-серверы) - выполняют функции FTP-сервера. Злоумышленники внедряют их накомпьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу FTP.

Server-Proxy (Прокси-серверы) - выполняют функции прокси-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.

Server-Telnet (Telnet-серверы) - выполняют функции Telnet-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу Telnet.

Server-Web (Веб-серверы) - выполняют функции веб-сервера. Злоумышленники внедряют их на компьютер пользователя, чтобы открыть к нему удаленный доступ по протоколу HTTP.

RiskTool (Инструменты для работы на локальном компьютере) - дают пользователю дополнительные возможности при работе на своем компьютере (позволяют скрывать на своем компьютере файлы или окна активных приложений, закрывать активные процессы).

NetTool (Сетевые инструменты) - дают пользователю компьютера, на котором установлены, дополнительные возможности при работе с другими компьютерами в сети (позволяют перезагружать их, находить открытые порты, запускать установленные на них программы).

Client-P2P (Клиенты пиринговых сетей) - позволяют работать в пиринговых (Peer-to-Peer) сетях. Могут использоваться злоумышленниками для распространения вредоносных программ.

Client-SMTP (SMTP-клиенты) - отправляют электронные сообщения в скрытом режиме. Злоумышленники внедряют их на компьютер пользователя, чтобы от его имени рассылать спам.

WebToolbar (Веб-панели инструментов) - добавляют в интерфейс других приложений панели инструментов для использования поисковых систем.

FraudTool (Псевдопрограммы) - выдают себя за другие программы. Например, существуют псевдоантивирусы; они выводят сообщения об обнаружении вредоносных программ, но на самом деле ничего не находят и не лечат.

Потенциально нежелательные программы устанавливаются одним из следующих способов:

• Их устанавливает сам пользователь, отдельно или в составе другой программы (например, производители включают программы рекламного характера в бесплатное или условно-бесплатное программное обеспечение).

• Их устанавливают злоумышленники, например, включают их в пакеты с другими вредоносными программами, используют «уязвимости» веб-браузера или троянские программы-загрузчики и установщики. *[Блог Алексея Лукина http://alexeyworld.com/blog/unwanted_programs.18.aspx]*.

См. также: Вредоносное программное обеспечение.

Поточная шифрсистема [stream ciphering system] —

Система шифрования, в которой функция зашифрования реализуется поточным алгоритмом зашифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система шифрования.

Ниже: Управляющий модуль поточной шифрсистемы, Шифрующий модуль поточной шифрсистемы.

См. также: Поточный алгоритм зашифрования.

Поточный алгоритм зашифрования [stream encryption algorithm, stream cipher] —

Алгоритм зашифрования, реализующий при каждом фиксированном значении ключа последовательность обратимых отображений (вообще говоря, различных), действующую на последовательность блоков открытого текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006]*.

Выше: Алгоритм зашифрования.

См. также: Поточная шифрсистема, Развертывание ключа.

Почтовая бомба [mail bomb] —

1. Блокирование работы компьютерной программы, выполняющей функции клиента или сервера электронной почты, посредством отправки сообщения, просмотр которого вызывает ее «зависание». *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*

2. Один из простейших видов сетевых атак. Злоумышленником посылается на компьютер пользователя или почтовый сервер компании одно огромное сообщение, упакованное в архив, или множество (десятки тысяч) почтовых сообщений, что приводит к выводу системы из строя. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Компьютерный вирус, Сетевая атака.

См. также: Электронная почта.

Права доступа —

Совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (информации, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации. Права доступа определяют набор действий (например, чтение, запись, выполнение), разрешённых для выполнения субъектам (например, пользователям системы) над объектами данных. Для этого требуется некая система для предоставления субъектам различных прав доступа к объектам. Это система разграничения доступа субъектов к объектам, которая рассматривается в качестве главного средства защиты от несанкционированного доступа к информации. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Доступ, Полномочие, Система разграничения доступа, Контроль доступа в информационной системе, Управление доступом, Правила разграничения доступа, Тип доступа.

Правдоподобность появления (события) (в области риск-менеджмента) [likelihood] —

Характеристика возможности и частоты появления события.

Примечание 1. В менеджменте риска термин "правдоподобность" используют как характеристику возможности появления события, которая может быть определенной или неопределенной, измеримой или неизмеримой, объективной или субъективной, иметь качественную или количественную оценку и может быть выражена математически (как вероятность или частота за установленный период времени).

Примечание 2. Английский термин "правдоподобность" не имеет прямого эквивалента в некоторых языках, вместо которого в этом случае применяют термин "вероятность". В английском языке термин "вероятность" часто применяют как чисто математический термин. Таким образом, в области управления риском в части терминологии термин "вероятность" использован в более широком смысле, чем в других языках, кроме английского. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012].*

Син.: Возможность (в области риск-менеджмента).

См. также: Вероятность (в области риск-менеджмента), Событие.

Правила разграничения доступа [security policy] —

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)].*

Ниже: Правила разграничения доступа (в автоматизированной информационной системе).

См. также: Нарушитель правил разграничения доступа, Права доступа, Санкционированный доступ к информации.

Правила разграничения доступа (в автоматизированной информационной системе) [security policy] —

Правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006].*

Выше: Правила разграничения доступа.

Правила фильтрации —

Перечень условий по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Межсетевой экран может строиться с помощью экранирующих агентов, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию. Использование экранирующих агентов позволяет предоставить

дополнительную защитную функцию - сокрытие от субъекта истинного объекта. В то же время, субъекту кажется, что он непосредственно взаимодействует с объектом. Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Фильтрация, Критерии фильтрации.

Правило Керкгоффса [Kerckhoffs assumption] —

Общепринятое в криптографии предположение проведения криптоанализа, впервые сформулированное голландским криптографом Н. Керкгоффсом («компрометация системы не должна причинять неудобств корреспондентам»). В современном понимании это правило означает, что описание криптосистемы (криптопротокола) может быть полностью известно противнику и/или нарушителю, а криптографическая стойкость основана только на том, что не известен ключ (секретный). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптоанализ.

Право автора на имя —

Право использовать или разрешать использование произведения под своим именем, под вымышленным именем (псевдонимом) или без указания имени, то есть анонимно. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

Выше: Авторские права.

Право авторства —

Право признаваться автором произведения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

Выше: Авторские права, Патентные права.

Право доступа —

Автор произведения изобразительного искусства вправе требовать от собственника оригинала произведения предоставления возможности осуществлять право на воспроизведение своего произведения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

Выше: Авторские права.

Право на обнародование своего произведения —

Право осуществить действие или дать согласие на осуществление действия, которое впервые делает произведение доступным для всеобщего сведения путем его опубликования, публичного показа, публичного исполнения, сообщения в эфир или по кабелю либо любым другим способом. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

Выше: Авторские права.

Правовая защита информации —

Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации.

См. также: Техническая защита информации, Физическая (непосредственная) защита информации, Организационная защита информации, Комплексная защита информации, Правовое обеспечение информационной безопасности, Правовые методы обеспечения информационной безопасности.

Правовое обеспечение автоматизированной системы —

Совокупность правовых норм, регламентирующих правовые отношения при функционировании АС и юридический статус результатов ее функционирования.

Примечание. Правовое обеспечение реализуют в организационном обеспечении АС. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Автоматизированная система, Информационное обеспечение автоматизированной системы, Методическое обеспечение автоматизированной системы, Организационное обеспечение автоматизированной системы, Программное обеспечение автоматизированной системы, Техническое обеспечение автоматизированной системы.

Правовое обеспечение информационной безопасности —

Нормативные правовые акты, регламентирующие отношения в информационной сфере, и нормативные методические документы по обеспечению информационной безопасности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895) (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Правовая защита информации, Правовые методы обеспечения информационной безопасности.

Правовые методы обеспечения информационной безопасности —

Разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Общие методы обеспечения информационной безопасности.

См. также: Правовое обеспечение информационной безопасности.

Правонарушение в информационном пространстве —

Использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

См. также: Преступления в сфере компьютерной информации.

Практическая стойкость (криптосистемы) [practical security (of the cryptosystem)] **—**

Вычислительная сложность алгоритма (см. временная сложность алгоритма, емкостная сложность алгоритма, сложность коммуникационная), реализующего наилучшую в определенном смысле атаку на криптосистему. Чаще всего под практической стойкостью понимают временную сложность выполнения успешной атаки на криптосистему наиболее быстрым из известных алгоритмов при реальных предположениях о свойствах криптосистемы и ее применении, а также о вычислительных машинах, на которых она будет реализовываться. Такой подход, с учетом перспектив развития вычислительных машин, позволяет оценить время, в течение которого данная криптосистема будет обеспечивать защищенность информации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая стойкость.

См. также: Атака на криптосистему, Временная сложность алгоритма, Емкостная сложность алгоритма, Коммуникационная сложность (протокола).

Превентивные меры [preventive action] **—**

Меры по устранению причин потенциальных несоответствий требованиям СУИБ, с целью предотвращения их возникновения.

Примечание. Меры по предотвращению несоответствий часто являются более экономически оправданными, нежели корректирующие меры. *[BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements Дата принятия: 14.10.2005 Перевод: ООО «GlobalTrust Solutions»]*.

Син. Предупреждающие действия.

См. также: Корректирующие меры.

Преднамеренное силовое электромагнитное воздействие на информацию —

Несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Воздействие.

См. также: Защита информации от преднамеренного воздействия.

Преднамеренные угрозы —

Преднамеренные угрозы могут быть различных видов: от небрежного анализа, использующего легко доступные средства управления, до изощренных вторжений с использованием специальных сведений о системе. Реализуемая преднамеренная угроза может рассматриваться как «вторжение». *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды угроз.

См. также: Вторжение.

Предоставление информации [distribution of information] —

Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Выше: Информационная технология.

Предоставление информации, составляющей коммерческую тайну —

Передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций. [Федеральный закон от 29.07.2004 N 98-ФЗ “О коммерческой тайне” (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004].

См. также: Коммерческая тайна, Передача информации, составляющей коммерческую тайну.

Предоставление персональных данных [provision personal data] —

Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Выше: Обработка персональных данных.

Предотвращение вторжений [intrusion prevention] —

Формальный процесс активного реагирования с целью предотвращения вторжений. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология.*

Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012].

См. также: Вторжение, Система обнаружения вторжения, Обнаружение вторжений, Система предотвращения вторжений.

Предположение о черном ящике [black box assumption] —

Предположение криптоанализа, означающее, что алгоритм шифрования неизвестен, и возможно лишь наблюдение выхода алгоритма при любом заданном входе. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Черный ящик.

Предположения криптоанализа [cryptanalytic assumptions] —

Совокупность условий и допущений, при которых проводится анализ криптографической системы. Фактически предположения разработчика и законного пользователя описывают модель противника и/или нарушителя, т. е. его цели, возможности и имеющиеся исходные данные. Предположения противника и/или нарушителя обычно описывают свойства криптосистемы и особенности ее реализации и применения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Нарушитель, Противник, Криптоанализ.

Предпочтительный риск [risk appetite] —

Тип риска и его уровень, к которому организация стремится или готова поддерживать. *[ГОСТ Р51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Выше: Риск.

Син.: Риск-аппетит.

Предупреждающие действия [preventive action] —

1. Действие, предпринятое для устранения потенциального несоответствия или другой потенциально нежелательной ситуации. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Действия, необходимые для устранения причин потенциальных несоответствий требованиям СМИБ, с целью предотвратить их повторное появление.

Примечание. Обычно затраты на проведение мероприятий по предотвращению несоответствий более экономичны, чем на корректирующие действия. *[ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен в действие: 01.02.2008]*.

Син. Превентивные меры.

См. также: Корректирующие действия.

Предупреждение об опасности [alert] —

“Немедленное" оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или

человеческой ошибки. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Опасность.

Преобразование, не распространяющее искажений [transform free of error propagation] —

Отображение, не распространяющее искажений, множества слов из некоторого алфавита в себя. Все обратимые отображения такого типа описаны А. А. Марковым. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Отображение, не распространяющее искажений

Преобразование перемешивания [mixing transform] —

Преобразование, с помощью которого разработчики криптосистем стремятся обеспечить свойство перемешивания. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Свойство перемешивания.

Преобразование рассеивания [diffusion transform] —

Преобразование, с помощью которого разработчики криптосистем стремятся обеспечить свойство рассеивания. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Свойство рассеивания.

Преобразование усложнения [confusion transform] —

Преобразование, с помощью которого разработчики криптосистем стремятся обеспечить свойство усложнения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Свойство усложнения.

Прерывание [interruption] —

Операция процессора, состоящая в регистрации предшествующего прерыванию состояния процессора и установлении нового состояния.

Примечание. Прерывание является реакцией процессора на некоторые условия, возникшие в процессоре или вне его. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Преступления в сфере компьютерной информации —

Преступления, указанные в главе 28 Уголовного кодекса Российской Федерации:

• Неправомерный доступ к компьютерной информации (ст.272);
• Создание, использование и распространение вредоносных компьютерных программ (ст.273);

• Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст.274). *[Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (с изменениями на 5 мая 2014 года) (редакция, действующая с 16 мая 2014 года). Введен в действие 01.01.1997]*.

Выше: Компьютерное преступление.

См. также: Правонарушение в информационном пространстве.

Преступное/мошенническое программное обеспечение [crimeware] —

1. Обобщенный термин для описания всех вредоносных программ, имеющих целью незаконное получение денег или конфиденциальной информации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. Вид вредоносных программ, имеющих целью или облегчающих совершение противоправных действий. К таким действиям относятся кража личных идентификационных данных для совершения мошеннических действий в системах дистанционного банковского обслуживания и интренет-торговли, создание подложных сайтов интернет-магазинов и других поставщиков услуг, получение удаленного доступа к приложениям с целью внедрения вредоносного кода и т. п. Различают п. о. п., с помощью которого технические специалисты совершают противоправные действия (создание незаконных копий программ, использование вредоносных программ, бот-сетей) и п. о. п., которое помогает людям, не являющимся техническими специалистами, совершать преступления с помощью компьютера (создание вирусов, рассылка спама, реализация фишинговых атак и т. п.). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Вредоносное программное обеспечение, Удаленный доступ.

Претекстинг —

1. Действие, отработанное по заранее составленному сценарию (претексту). В результате цель должна выдать определённую информацию или совершить определённое действие. Этот вид атак применяется обычно по телефону. Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации: дата рождения, сумма последнего счёта и др.), с тем, чтобы обеспечить доверие цели. К этому же виду относятся атаки и по онлайн-мессенджерам, например, по ICQ. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. Набор действий, проведенный по определенному, заранее готовому сценарию (претексту). Данная техника предполагает использование голосовых средств, таких как телефон, Skype и т.п. для получения нужной информации. Как правило, представляясь третьим лицом или притворяясь, что кто-то нуждается в помощи, злоумышленник просит жертву сообщить пароль или авторизоваться на фишинговой веб-странице, тем самым заставляя совершить необходимое действие или предоставить определенную информацию. В большинстве случаев данная техника требует каких-либо изначальных данных о объекте атаки (например, персональных данных: даты рождения, номера телефона, номеров счетов и др.) Самая распространенная стратегия - использование поначалу небольших запросов и упоминание имен реальных людей в организации. В дальнейшем, в процессе разговора, злоумышленник объясняет, что он нуждаются в помощи (большинство людей могут и готовы

исполнить задачи, которые не воспринимаются как подозрительные). Как только доверительная связь установлена, мошенник может попросить что-то более существенное и важное. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Социальная инженерия.

Пригодная для использования уязвимость (объекта оценки) [exploitable vulnerability] —

Слабое место объекта оценки, которое может быть использовано для нарушения функциональных требований безопасности в среде функционирования объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Уязвимость (объекта оценки).

Приемочный контроль [acceptance inspection] —

Контроль продукции, по результатам которого принимается решение о ее пригодности к поставкам и/или использованию. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

См. также: Метод контроля, Комплекс технического контроля.

Прикладная программа [application program] —

1. Программное средство или программа, специально предназначенная для решения прикладных проблем определенного класса.

Примечание. Примером является программа для работы с электронными таблицами. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Программа, предназначенная для решения задачи или класса задач в определенной области применения системы обработки информации. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Пакет прикладных программ.

Прикладной криптографический протокол [application cryptographic protocol] —

Криптографический протокол, предназначенный для решения практических задач обеспечения функций-сервисов безопасности с помощью криптографических систем. Примеры: протокол конфиденциальной передачи сообщений, схема цифровой подписи, система электронных платежей, протокол голосования, протокол подписания контракта и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический протокол.

Ниже: Схема цифровой подписи, Система (протокол) электронных платежей, Протокол голосования, Протокол подписания контракта.

См. также: Функция-сервис безопасности.

Примитивный криптографический протокол [primitive cryptographic protocol] —

Криптографический протокол, который не имеет самостоятельного прикладного значения, но используется как базовый компонент при построении прикладных криптографических протоколов. Как правило, примитивный криптографический протокол решает какую-либо одну абстрактную задачу. Примеры: протокол обмена секретами, протокол привязки к биту, протокол подбрасывания монеты (по телефону) .*[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Протокол обмена секретами, Протокол подбрасывания монеты (по телефону), Протокол (схема) привязки к биту.

См. также: Прикладной криптографический протокол.

Принципы обеспечения безопасности —

1. Основными принципами обеспечения безопасности являются:

1) соблюдение и защита прав и свобод человека и гражданина;

2) законность;

3) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;

4) приоритет предупредительных мер в целях обеспечения безопасности;

5) взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности. *[Федеральный закон от 28.12.2010 N 390-ФЗ “О безопасности”. Введен в действие: 29.12.2010]*.

2. Для создания эффективной программы безопасности информационных и телекоммуникационных технологий фундаментальными являются следующие высокоуровневые принципы безопасности:

• менеджмент риска — активы должны быть защищены путем принятия соответствующих мер. Защитные меры должны выбираться и применяться на основании соответствующей методологии управления рисками, которая, исходя из активов организации, угроз, уязвимостей и различных воздействий угроз, устанавливает допустимые риски и учитывает существующие ограничения;

• обязательства — важны обязательства организации в области безопасности информационных и телекоммуникационных технологий и в управлении рисками. Для формирования обязательств следует разъяснить преимущества от реализации безопасности информационных и телекоммуникационных технологий;

• служебные обязанности и ответственность — руководство организации несет ответственность за обеспечение безопасности активов. Служебные

обязанности и ответственность, связанные с безопасностью информационных и телекоммуникационных технологий, должны быть определены и доведены до сведения персонала;

• цели, стратегии и политика — управление рисками, связанными с безопасностью информационных и телекоммуникационных технологий, должно осуществляться с учетом целей, стратегий и политики организации;

• управление жизненным циклом — управление безопасностью информационных и телекоммуникационных технологий должно быть непрерывным в течение всего их жизненного цикла. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Ниже: Непрерывность защиты.

См. также: Принципы правового регулирования отношений в сфере информации, технологий информационных и защиты информации.

Принципы правового регулирования отношений в сфере информации, технологий информационных и защиты информации —

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании систем информационных и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании систем информационных, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних технологий информационных перед другими, если только обязательность применения определенных технологий информационных для создания и эксплуатации государственных информационных систем не установлена федеральными законами. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28*

декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006].

См. также: Принципы обеспечения безопасности.

Принятие риска [risk acceptance] —

Обоснованное решение принять конкретный риск.

Примечание 1. Решение о принятии риска может быть принято без воздействия на риск или в процессе воздействия на риск.

Примечание 2. Необходимо проводить мониторинг и пересмотр принятого риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

См. также: Менеджмент риска информационной безопасности организации, Неприятие риска, Толерантность к риску.

Приоритет (процесса) [priority] —

Преимущественное право процесса обработки данных перед другими процессами на использование ресурсов, выражаемое числом, присвоенным этому процессу. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992].*

Причастная сторона [stakeholder] —

Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечание. Лицо, принимающее решение, также является причастной стороной. [ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012].

Син.: Заинтересованная сторона.

См. также: Третья сторона.

Проактивная защита —

См. Антивирусные базы данных.

Проблема безопасности (объекта оценки) [security problem] —

Изложение, которое в формализованном виде определяет характер и масштабы безопасности, которую должен обеспечивать объект оценки.

Примечание — Данное изложение содержит сочетание: угроз, которым должно быть обеспечено противостояние со стороны объекта оценки; политик безопасности организаций, осуществляемых объектом оценки, и предположений, которые определены для объекта оценки и его среды функционирования. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].*

См. также: Объект оценки.

Проблема повторной траты электронных денег [e-money double spending problem] —

Возможность неоднократного использования одних и тех же электронных денег нечестным покупателем. Возникает в автономных системах электронных платежей, так как в них транзакция платежа выполняется без участия банка. Для решения проблемы повторной траты электронных денег известны два способа. Первый — идентификация нарушителя post factum. Он основывается на специальной конструкции электронных денег, позволяющей банку при выполнении транзакции депозита обнаружить повторную трату и идентифицировать нарушителя. При этом честным клиентам банка гарантируется безусловная неотслеживаемость платежей. Второй способ предотвращает повторную трату электронных денег посредством электронных бумажников. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Автономная система электронных платежей, Электронный бумажник, Транзакция (протокол) депозита.

Провайдер сети —

Уполномоченная организация, выполняющая функции поставщика услуг сети для абонентского пункта и непосредственно для абонентов сети. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

См. также: Абонент сети, Абонентский пункт, Информационные сети общего пользования, Услуги сети.

Провайдер хостинга —

Лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет". *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Проверка безопасности —

Независимый просмотр, изучение системных журналов и наблюдение за функционированием информационных систем и объектов с целью определения достаточности средств контроля системы, соответствия принятой методике безопасности и процедурам обработки данных, обнаружения нарушений безопасности, выработки рекомендаций по изменению средств контроля и процедур безопасности. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Мониторинг.

Проверяемая организация [auditee] **—**

Организация, подвергающаяся аудиту. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Аудиторская проверка информационной безопасности в организации.

Проверяемое разделение секрета [verifiable secret sharing] **—**

См. Протокол разделения проверяемого секрета.

Программа (компьютерная) —

См. Программа для ЭВМ.

Программа аудита [audit programme] —

Совокупность мероприятий по проведению одного или нескольких аудитов, запланированных на конкретный период времени и направленных на достижение конкретной цели. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: План аудита, Программа аудита информационной безопасности.

Программа аудита информационной безопасности —

План деятельности по проведению одного или нескольких аудитов информационной безопасности (и других проверок информационной безопасности), запланированных на конкретный период времени и направленных на достижение конкретной цели. Примечание. Программа аудита информационной безопасности включает всю деятельность, необходимую для планирования, проведения, контроля, анализа и совершенствования аудитов информационной безопасности (и других проверок информационной безопасности). [Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)].

См. также: Программа аудита.

Программа для ЭВМ [program] —

1. Представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

2. Синтаксический блок, соответствующий правилам конкретного языка программирования и состоящий из объявлений и утверждений или инструкций, необходимых для выполнения определенных функций, задач или проблем. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

3. Данные, предназначенные для управления конкретными компонентами системы обработки информации в целях реализации определенного алгоритма. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Программирование [programming] —

Научная и практическая деятельность по созданию программ. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Программная закладка [program bug, malicious logic] —

1. Преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

2. Преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения. Примечание. Программная закладка может быть реализована в виде вредоносной программы или программного кода. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

3. Внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию. *[ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

4. Скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Примечание. Программная закладка может быть реализована в виде вредоносной программы или программного кода. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

5. Преднамеренно внесенные в обеспечение программное функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, приводящих к нарушению конфиденциальности, доступности или целостности обрабатываемой информации. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)]*.

См. также: Аппаратная закладка, Вредоносная программа, Недекларированные возможности, Специальная проверка.

Программное воздействие —

Несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ. *[ГОСТ Р 51275-2006 Защита информации. Объект*

информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008].

Выше: Воздействие.

См. также: Вредоносное программное обеспечение.

Программное обеспечение [software] —

1. Любая часть программ, процедур, правил и документации для систем обработки информации.

Примечание. Софтвер является результатом интеллектуальной деятельности, не зависящим от средства, на котором он записан. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

3. Наряду с аппаратными средствами, важнейшая составляющая информационных технологий, включающая компьютерные программы и данные, предназначенные для решения определённого круга задач и хранящиеся на машинных носителях. Программное обеспечение представляет собой либо данные для использования в других программах, либо алгоритм, реализованный в виде последовательности инструкций для процессора.

В компьютерном сленге часто используется слово софт (от software), которое в этом смысле впервые применил в статье в American Mathematical Monthly математик из Принстонского университета Джон Тьюки в 1958 году. В области вычислительной техники и программирования программное обеспечение — это совокупность всей информации, данных и программ, которые обрабатываются компьютерными системами. В информатике программное обеспечение — это наборы пакетов программ и операционных систем, которые могут устанавливаться на персональных компьютерах, серверах и суперкомпьютерах. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Аппаратное обеспечение.

Программное обеспечение автоматизированной системы [AS software] —

Совокупность программ на носителях данных и программных документов, предназначенная для отладки, функционирования и проверки работоспособности автоматизированной системы. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Автоматизированная система, Информационное обеспечение автоматизированной системы, Методическое обеспечение автоматизированной системы, Организационное обеспечение автоматизированной системы, Правовое обеспечение автоматизированной системы, Техническое обеспечение автоматизированной системы.

Программное обеспечение, содержащее рекламу [adware, advertising-supported software] —

Термином «adware» называют вредоносное программное обеспечение, основной целью которого является показ рекламы во время работы компьютера. Основным назначением деятельности по показу рекламы является получение прибыли и покрытие расходов на разработку программного обеспечения (например, конвертера видео или клиента системы мгновенных сообщений), таким образом, adware — это неявная форма оплаты за использование программного обеспечения, осуществляющаяся за счёт показа пользователю рекламной информации. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Программное пиратство [software piracy] —

Несанкционированное использование, копирование или распространение программных средств, являющихся авторским произведением. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Авторские права, Технические средства защиты авторских прав.

Программное средство защиты информации [software security module] —

Программа, входящая в комплект программного обеспечения и реализующая одну из функций защиты информации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Средство защиты информации.

Программное шифрование [software encryption] —

Шифрование, выполняемое только с применением программных криптографических средств. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Шифрование.

См. также: Программные криптографические средства.

Программные криптографические средства [software cryptographic mechanisms] —

Программные средства, реализующие одну или несколько криптографических функций-сервисов безопасности. Различают программные криптографические средства с выполнением в контексте пользователя и на уровне ядра или системном уровне операционной системы. Программные криптографические средства с выполнением в контексте пользователя, как правило, ориентированы на выполнение ограниченного множества криптографических функций и решают какую-либо одну конкретную задачу. Могут быть реализованы как в виде законченного программного продукта, интеграция которого заключается в обычной инсталляции данного продукта, так и в виде программных модулей, установка которых может требовать дополнительных процедур встраивания их в обеспечение программное. Программные криптографические средства с выполнением на уровне ядра или системном уровне ОС реализуются в виде системных функций, выполняемых

на уровне ядра, либо на системном уровне (драйверы, динамические библиотеки). Для унификации реализации и использования криптографических функций различными приложениями в этом случае разрабатывается специальный крипто API. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Криптографические средства выше прикладного уровня, Криптографические средства прикладного уровня, Криптографические средства сетевого уровня, Криптографические средства транспортного уровня.

См. также: Криптографические функции-сервисы безопасности.

Программный модуль [program module] —

Программа или функционально завершенный фрагмент программы, предназначенный для хранения, трансляции, объединения с другими программными модулями и загрузки в оперативную память. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Продукт [product] —

Совокупность программных, программно-аппаратных и/или аппаратных средств информационных технологий, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Проект информационной безопасности Взаимоувязанной сети связи Российской Федерации —

План, замысел, определяющий для разрабатываемой системы обеспечения информационной безопасности ВСС РФ требования к информационной безопасности ВСС РФ.

Примечание. Проект информационной безопасности ВСС РФ разрабатывается в виде документа, согласующего приемлемый уровень качества служб информационной безопасности в условиях заданного множества угроз информационной безопасности ВСС РФ, эффективность выбранных мер обеспечения информационной безопасности ВСС РФ и результирующую цену системы обеспечения информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации, Система обеспечения информационной безопасности сети связи Российской Федерации.

Проект СМИБ —

Структурированные действия, принимаемые организацией для внедрения системы управления информационной безопасностью. *[ГОСТ Р ИСО/МЭК*

27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. Введен в действие: 01.12.2013].

См. также: Система менеджмента информационной безопасности.

Проникновение [penetration] **—**

Успешное преодоление механизмов защиты системы. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Вторжение.

Пропускная способность скрытого канала [covert channel capacity] **—**

Количество информации, которое может быть передано по каналу скрытому в единицу времени или относительно какой-либо другой шкалы измерения. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Скрытый канал.

Простая электронная подпись —

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается. Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

1) простая электронная подпись содержится в самом электронном документе;

2) ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

2. Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;

2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Электронная подпись.

См. также: Квалифицированная электронная подпись (усиленная квалифицированная электронная подпись), Неквалифицированная электронная подпись (усиленная неквалифицированная электронная подпись), Средства электронной подписи, Электронный документ.

Простой шифр замены [substitution cipher] —

Шифр, в котором функция зашифрования состоит в замене блоков текста (сообщения) открытого блоками текста (сообщения) шифрованного в соответствии с ключом, представляющим собой подстановку на множестве блоков текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Коммутаторный ключ.

Пространство подписей [signature space] —

Множество всех значений цифровой подписи, которые могут быть сгенерированы данной схемой цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Схема цифровой подписи .

Противник [adversary] —

Внешний по отношению к участникам криптопротокола (криптографической системы) субъект (или коалиция субъектов), наблюдающий за передаваемыми сообщениями, и, возможно, вмешивающийся в работу участников, путем перехвата, искажения (модификации), вставки (создания новых), повтора и перенаправления сообщений, блокирования передачи и т. п. с целью нарушения одной или нескольких функций-сервисов безопасности. Может образовывать коалицию с нарушителем. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Активный противник, Пассивный противник.

См. также: Нарушитель.

Противостоять [counter] —

Характеризует противостояние некоторому нападению, при котором негативные последствия реализации некоторой конкретной угрозы уменьшаются, но не обязательно полностью ликвидируются. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Нападающий.

Протокол [protocol] —

1. Описание распределенного алгоритма, в процессе выполнения которого два участника (или более) последовательно выполняют определенные

действия и обмениваются сообщениями. Последовательность шагов протокола группируется в циклы (раунды). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

2. Согласованная процедура передачи данных между различными объектами вычислительной системы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

3. Стандарт для формата и содержания данных, передаваемых между компьютерами по компьютерной сети. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Ниже: Двусторонний протокол

См. также: Участник (протокола), Криптографический протокол.

Протокол (алгоритм) обмена ключами Диффи–Хеллмана [Diffie–Hellman algorithm] —

Один из первых протоколов открытого распределения ключей. Предназначен для формирования «общего секрета» (ключа, идентификационного номера и др.) сторонами, обменивающимися данными по открытому каналу с использованием открытых (общедоступных)ключей и секретных (индивидуальных)ключей. Вместе с алгоритмом шифрования RSA положил начало развитию асимметричных шифрсистем. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Открытое распределение ключей, Асимметричная шифрсистема.

Протокол аутентификации сообщений [message authentication protocol] —

Криптографический протокол, предназначенный для обеспечения целостности сообщений, под которой понимается гарантируемая получателю возможность удостовериться, что сообщение поступило от заявленного отправителя и в неискаженном виде. В случае, когда участники протокола доверяют друг другу и защищаются от противника, протоколы аутентификации сообщений строятся на основе кодов аутентичности сообщений. Если же участники друг другу не доверяют, то для аутентификации сообщений используется схема цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический протокол.

См. также: Код аутентичности сообщения, Схема цифровой подписи, Теория аутентификации Симмонса.

Протокол голосования [election scheme, voting scheme, voting protocol] —

Прикладной криптографический протокол, позволяющий проводить процедуру голосования, в которой избирательные бюллетени существуют только в электронной форме. Является криптографическим протоколом, т. к. обеспечивает тайный характер голосования. Основное свойство протокола голосования — универсальная проверяемость, т. е. предоставление возможности всякому желающему, включая сторонних наблюдателей, в любой момент времени проверить правильность подсчета голосов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Прикладной криптографический протокол.

Протокол идентификации [identification protocol] —

Протокол аутентификации сторон, участвующих во взаимодействии и не доверяющих друг другу. Различают протокол идентификации с односторонней аутентификацией или взаимной аутентификацией. Протоколы идентификации, как правило, основаны на известной обеим сторонам информации (пароли, личные идентификационные номера, ключи секретные или ключи открытые) и реализуются с использованием техники «запрос-ответ» или доказательства знания. В дополнение к протоколам идентификации могут использоваться некоторые физические приборы, с помощью которых проводится идентификация (магнитная или интеллектуальная пластиковая карта, прибор, генерирующий меняющиеся со временем пароли), а также биометрические параметры. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система идентификации.

Протокол обмена секретами [secret exchange protocol] —

Примитивный криптографический протокол с двумя участниками. Входные слова участников называются секретами. В протоколе обмен секретами организован таким образом, чтобы в случае его прерывания (по любой причине) знания участников о секретах друг друга были приблизительно одинаковыми. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Примитивный криптографический протокол.

Протокол подбрасывания монеты (по телефону) [coin flipping (by telephone) protocol] —

Примитивный криптографический протокол, позволяющий двум не доверяющим друг другу участникам сгенерировать общий случайный равновероятный бит. Главное свойство таких протоколов состоит в том, что если хотя бы один из участников является честным участником, то сгенерированный бит будет случайным, независимо от действий другого участника. Имеются обобщения на случай конечных битовых строк, а также на случай произвольного количества участников. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Примитивный криптографический протокол.

Протокол подписания контракта [contract signing protocol] —

Прикладной криптографический протокол, как правило, с двумя участниками, которые, обмениваясь сообщениями по каналам связи, должны подписать контракт, существующий только в электронной форме. Основное требование к криптографической стойкости протокола подписания контракта таково: при любом прерывании выполнения протокола шансы каждого из участников получить контракт, подписанный другим, и при этом не подписаться самому, ничтожно малы. Поэтому протокол подписания контракта должен включать в себя протокол обмена секретами. Имеются и другие требования к стойкости протокола, в частности, так называемая защита от

злоупотреблений (abuse). Последняя означает, что если выполнение протокола было прервано и контракт остался неподписанным, то ни один из участников не сможет доказать третьим лицам (арбитрам), что другой участвовал в выполнении протокола (а, следовательно, имел намерение подписать данный контракт). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Прикладной криптографический протокол.

См. также: Протокол обмена секретами.

Протокол разделения проверяемого секрета [verifiable secret sharing protocol] —

Протокол разделения секрета предназначенный для случая, когда участники не доверяют друг другу, в том числе и дилеру. Для защиты от нечестного дилера протокол разделения проверяемого секрета предоставляет каждому из остальных участников возможность проверить, что от дилера получена корректная доля секрета. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Протокол разделения секрета.

Протокол разделения секрета [secret sharing protocol] —

Криптографический протокол, реализующий схему разделения секрета в модели, где участники являются абонентами сети связи. В этой модели имеется дополнительный участник (дилер), которому известно значение секрета. Дилер генерирует доли секрета и рассылает их остальным участникам. Всякая правомочная коалиция участников может восстановить секрет, выполнив протокол восстановления секрета. Протокол разделения секрета могут найти применение в организации хранения конфиденциальной информации, например, ключей криптосистемы, а также как примитивные криптографические протоколы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический протокол.

Ниже: Протокол разделения проверяемого секрета.

См. также: Схема разделения секрета, Примитивный криптографический протокол.

Протокол распределения ключей [key distribution protocol] —

Протокол получения пользователями ключей, необходимых для функционирования криптографической системы. Различают следующие типы протокола распределения ключей: протоколы передачи (уже сгенерированных) ключей; протоколы совместной выработки общего ключа (распределение открытое ключей); схемы предварительного распределения ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Открытое распределение ключей, Квантовое распределение ключей.

Протокол с арбитром [arbitrated protocol] —

Криптографический протокол, в котором для разрешения споров между участниками требуется арбитраж. Протоколы с арбитром делятся на два класса.

В пессимистических протоколах арбитр должен участвовать в каждом сеансе выполнения протокола. В оптимистических протоколах участие арбитра требуется только в случае возникновения конфликтов между участниками. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический протокол.

См. также: Арбитр

Протокол (схема) привязки к биту [bit commitment protocol (scheme)] —

Примитивный криптографический протокол с двумя участниками (отправителем и получателем), посредством которого отправитель передает получателю бит информации (битовое обязательство) таким образом, что выполняются следующие два условия: 1) после передачи бита получателю (так называемого этапа привязки) отправитель уже не может изменить его значение; 2) получатель не может самостоятельно определить значение бита и узнает его только после выполнения отправителем так называемого этапа раскрытия. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Примитивный криптографический протокол.

Профессиональная тайна —

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности. Подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Выше: Сведения конфиденциального характера.

Ниже: Адвокатская тайна, Врачебная тайна, Журналистская тайна, Нотариальная тайна, Тайна связи.

Профилактика —

Систематические действия эксплуатационного персонала, цель которых — выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и вновь полученные программные средства на наличие компьютерных вирусов. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Введен в действие: 01.07.1999]*.

См. также: Ревизия.

Профиль защиты [protection profile] —

1. Независимое от реализации изложение потребностей в безопасности для некоторого типа объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности.*

Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].

2. Совокупность типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой автоматизированной информационной системе. Примечание. Профиль защиты может разрабатываться для автоматизированной информационной системы, средства вычислительной техники, а также их технических и программных средств. *[Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Демонстрируемое соответствие, Задание по безопасности, объект оценки, Проблема безопасности (объекта оценки).

Профиль риска [risk profile] —

Описание какого-либо набора рисков. Примечание. Такой набор может включать риски, которые относятся ко всей организации, ее части или определенные иным образом. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Процесс обработки данных [computational process] —

Система действий, реализующая определенную функцию в системе обработки информации и оформленная так, что управляющая программа данной системы может перераспределять ресурсы этой системы в целях обеспечения мультипрограммирования.

Примечания:

1. Процесс характеризуется состояниями, которые определяются наличием тех или иных ресурсов в распоряжении процесса и, следовательно, возможностью фактически выполнять действия, относящиеся к процессу.

2. Перераспределение ресурсов, выполняемое управляющей программой, влияет на продолжительность процесса обработки данных, но не на его конечный результат.

3. Процесс оформляют с помощью специальных структур управляющих данных, которыми манипулирует управляющий механизм.

4. В конкретных системах обработки информации встречаются разновидности процессов, которые различаются способом оформления и составом ресурсов, назначаемых процессу и отнимаемых от него, и допускается вводить специальные названия для таких разновидностей, например задача в операционной системе ОС ЕС ЭВМ. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Система обработки информации, Обработка данных.

Процесс проверки подписи [verification process] —

Процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки подписи и параметры схемы ЭЦП, результатом которого является заключение о правильности или ошибочности цифровой подписи. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Алгоритм проверки цифровой подписи, Ключ подписи, Параметр схемы ЭЦП, Цифровая подпись, Процесс формирования подписи, Свидетельство.

Процесс риск-менеджмента [risk management process] —

Систематическое применение политик, процедур и практик менеджмента к деятельности по обмену информацией, консультированию, установлению ситуации (контекста) и идентификации, анализу, оцениванию, воздействию на риск, мониторингу и пересмотру риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Мониторинг (в области риск-менеджмента).

Процесс формирования подписи [signature process] —

Процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Защищенное устройство создания подписи, Ключ подписи, Параметр схемы ЭЦП, Цифровая подпись, Процесс проверки подписи.

Процессор [processor] —

Функциональная часть вычислительной машины или системы обработки информации, предназначенная для интерпретации программ. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Процессор ввода-вывода [input-output processor] —

Процессор, выполняющий операции обмена данными между центральным процессором и периферийными устройствами. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Псевдослучайная последовательность [pseudo-random sequence] —

Последовательность, порожденная детерминированным устройством или программой. Важной задачей криптографии является построение псевдослучайной последовательности, обладающих свойствами, близкими к свойствам типичных реализаций идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Криптографически сильная псевдослучайная последовательность.

См. также: Идеальная случайная последовательность, Набор статистических тестов.

Психологическое воздействие —

Действие, направленное против человеческого разума, а также компьютерной поддержки процессов принятия человеком ответственных решений. Операции по психологическому воздействию подразделяются: на операции против населения; на операции против руководящего состава войск; на операции против живой силы противоборствующей стороны; на операции по модификации культуры. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Воздействие.

Развертывание ключа [key scheduling] —

В поточных шифрсистемах — выработка ключевой последовательности по короткому ключу. В блочных шифрсистемах— алгоритм вычисления цикловых (раундовых) ключей по разовому ключу. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Поточный алгоритм зашифрования, Алгоритм блочного шифрования.

Разглашение государственной тайны —

Преступление, наказуемое в соответствии со статьей 283 Уголовного кодекса РФ. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Государственная тайна, Система защиты государственной тайны.

Разглашение информации —

Несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Защита информации от разглашения.

Разглашение информации, составляющей коммерческую тайну —

Действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору. *[Федеральный закон от 29.07.2004 N 98-ФЗ “О коммерческой тайне” (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]*.

См. также: Обладатель информации, составляющей коммерческую тайну.

Разграничение доступа [access control] —

См. Управление доступом.

Разделение секрета [secret sharing] —

См. Схема разделения секрета.

Разностная атака [differential attack] —

Атака на криптосистему, основанная на разностном методе. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

Син.: Дифференциальная атака.

См. также: Разностный метод.

Разностная атака на основе искажений [differential fault attack] —

Атака на криптосистему, основанная на разностном методе искажений. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

Разностно-линейная атака [differential-linear attack] —

Атака на криптосистему, основанная на разностно-линейном методе. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Атака на криптосистему.

Син.: Дифференциально-линейная атака.

Разностный метод [differential cryptanalysis] —

Метод криптографического анализа (в основном применимый к блочным шифрсистемам), использующий неравномерность условного распределения разностей между блоками шифрованного текста при некоторых значениях разности между блоками открытого текста. Имеет ряд модификаций, например, усеченный, метод бумеранга и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Син.: Дифференциальный метод.

См. также: Разностная атака.

Разовый ключ [once-only key] —

Ключ, однократно используемый для шифрования в жизненном цикле (ключей). Обычно не подлежит хранению и является элементом составного ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ.

См. также: Главный ключ, Долговременный ключ, Иерархия ключей.

Разрушение информации [destruction] —

Полная потеря хранящихся в информационных системах или передаваемых по информационным сетям данных или их изменение, исключающее возможность правильной их интерпретации и восстановления. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Информация, Средства информационного воздействия.

Распределение риска [risk sharing] —

Форма воздействия на риск, включающая согласованный раздел риска между несколькими сторонами.

Примечание 1. Законодательные или нормативные требования могут ограничить, запретить или обязать проведение распределения риска.

Примечание 2. Распределение риска может производиться путем страхования или иной формой контракта.

Примечание 3. До какой степени распределяется риск, зависит от надежности и четкости договоров по разделу риска.

Примечание 4. Передача риска является формой распределения риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

См. также: Риск.

Распределенная атака на отказ в обслуживании [Distributed Denial-of-Service attack (DDoS)] —

Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищенной крупной компании или правительственной организации. Первым делом злоумышленник сканирует крупную сеть с помощью специально подготовленных сценариев, которые выявляют потенциально слабые узлы. Выбранные узлы подвергаются нападению, и злоумышленник получает на них права администратора. На захваченные узлы устанавливаются троянские программы, которые работают в фоновом режиме. Теперь эти компьютеры называются компьютерами-зомби, их пользователи даже не подозревают, что являются потенциальными участниками DDoS-атаки. Далее злоумышленник отправляет определенные команды захваченным компьютерам и те, в свою очередь осуществляют мощную DoS-атаку на целевой компьютер. В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере (слэшдот-эффект). Большой наплыв пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки. В число анализируемых шаблонов нестандартного трафика входят все известные на сегодняшний день методы атак, в том числе реализуемые и при помощи распределенных бот-сетей. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Атака на отказ в обслуживании.

Распространение информации [information dissemination] —

Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006].

Выше: Информационная технология.

Распространение персональных данных [personal data dissemination] —

Действия, направленные на раскрытие персональных данных неопределенному кругу лиц. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Выше: Обработка персональных данных.

Рассекречивание сведений и их носителей —

Снятие ранее введенных в предусмотренном Законом «О государственной тайне» порядке ограничений на распространение сведений, составляющих государственную тайну и на доступ к их носителям. *[Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Отнесение сведений к государственной тайне и их засекречивание.

Расследование инцидента —

Исследование компьютерной информации и иных сведений с целью установления обстоятельств инцидента (характера, временной шкалы и других фактов) и выявления причастных лиц. *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

Выше: Менеджмент инцидента информационной безопасности.

См. также: Реагирование на инцидент.

Расстояние единственности [unicity distance] —

В задаче нахождения неизвестного параметра криптографической системы (например, секретного ключа) по выходным данным криптосистемы (например, по начальному отрезку шифрованного текста) — минимальное количество выходных данных, с заданной вероятностью достаточное для однозначного определения искомого параметра. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Расстояние между булевыми функциями [function-to-function distance] —

Расстоянием между булевыми функциями от одинакового количества переменных называется величина равная расстоянию Хемминга между векторами значений этих функций. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Расшифрование [decryption, deciphering] —

Процесс обратный к зашифрованию, реализуемый при известном значении ключа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Зашифрование данных.

Расшифровка данных [data deciphering] —

Процесс преобразования зашифрованных данных в открытые при помощи шифра. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

См. также: Расшифрование, Зашифрование данных.

Реагирование на инцидент —

Совокупность действий, направленных на выявление компьютерной информ ации, имеющей отношение к инциденту, и сохранение ее целостности и юридическо й значимости, а также на сбор иных сведений, имеющих отношение к инциденту. *[Инструкция по реагированию на инциденты, связанные с системами дистанционного банковского обслуживания. Авт. М.А.Суханов. Рецензенты: С.А.Грудинов и В.А.Лукацкий. ООО "Группа информационной безопасности" (Group-IB). 2012]*.

Выше: Менеджмент инцидента информационной безопасности.

См. также: Группа реагирования на инциденты информационной безопасности (ГРИИБ).

Ревизия [certification] —

Проверка вновь полученных программ специальными средствами, проводимая путем их запуска в контролируемой среде. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Введен в действие: 01.07.1999]*.

См. также: Профилактика.

Регистр рисков [risk register] —

Запись информации об идентифицированных рисках. Примечание. Термин «журнал рисков» иногда используют вместо термина «регистр рисков». *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Идентификация риска.

Регистрация [audit] —

Фиксация данных о совершенных действиях (событиях). *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Режим выработки имитовставки [message authentication code mode] —

См. Режим выработки кода аутентичности сообщения.

Режим выработки кода аутентичности сообщения [message authentication code mode] —

Режим шифрования, применяемый для выработки кода аутентичности сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Син.: Режим выработки имитовставки.

См. также: Код аутентичности сообщения.

Режим коммерческой тайны —

Правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности. *[Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (с изменениями на 11 июля 2011 года). Введен в действие: 16.08.2004]*.

См. также: Доступ к информации, составляющей коммерческую тайну, Информация, составляющей коммерческую тайну, Коммерческая тайна, Обладатель информации, составляющей коммерческую тайну.

Режим пакетной обработки [batch processing] —

Режим выполнения совокупности задач, при котором все они выполняются системой обработки информации в основном автоматически без синхронизации с событиями вне этой СОИ, в частности, без связи с лицами, представившими задание для выполнения. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]* .

См. также: Диалоговый режим, Интерактивный режим, Режим разделения времени, Режим реального времени, Система обработки информации.

Режим разделения времени [time sharing] —

Мультипрограммирование, при котором ресурсы системы обработки информации предоставляются каждому процессу из группы процессов обработки информации, находящихся в СОИ, на интервалы времени, длительность и очередность представления которых определяется управляющей программой этой СОИ с целью обеспечения одновременной работы процессов этой группы в интерактивном режиме. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Диалоговый режим, Интерактивный режим, Режим пакетной обработки, Режим реального времени, Система обработки информации.

Режим реального времени [real time processing] —

Режим обработки информации, при котором обеспечивается взаимодействие системы обработки информации с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Диалоговый режим, Интерактивный режим, Режим пакетной обработки, Режим разделения времени, Система обработки информации.

Режим шифрования [encryption mode] —

Способ получения алгоритма зашифрования, исходя из блочного базового алгоритма зашифрования. Основными режимами шифрования являются: простая замена или электронная кодовая книга (ECB), сцепление блоков шифртекста (CBC), обратная связь по шифртексту (CFB), обратная связь по выходу (OFB). Выбор режима шифрования имеет целью обеспечение определенных свойств алгоритма шифрования (ограничение распространения

искажений, простота синхронизации и др.). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Алгоритм зашифрования.

Реквизит документа —

Элемент оформления документа. *[ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения. Введен в действие: 01.03.2014]*.

См. также: Гриф ограничения доступа к документу , Гриф секретности, Подлинный документ.

Рекомендации [guidelines] —

Описание, поясняющее действия и способы их выполнения, необходимые для достижения установленных целей. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*

Рекомендации в области стандартизации [standardization guidelines] —

Документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего стандарта. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Стандарт.

Рекуррентная последовательность [recurrent sequence] —

Последовательность, в которой каждый элемент однозначно определяется некоторым фиксированным числом ее предыдущих элементов с помощью функции, именуемой законом рекурсии. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ресурс [resource] —

1. Активы (организации), которые используются или потребляются в ходе выполнения процесса.

Примечания:

1. Ресурсы могут включать в себя такие разнообразные объекты, как персонал, оборудование, основные средства, инструменты, а также коммунальные услуги: энергию, воду, топливо и инфраструктуру сетей связи.

2. Ресурсы могут быть многократно используемыми, возобновляемыми или расходуемыми. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Актив организации банковской системы Российской Федерации, который используется или потребляется в процессе выполнения некоторой деятельности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Актив, Ресурс (информационной системы).

Ресурс (информационной системы) —

Средства, использующиеся в информационной системе, привлекаемые для обработки информации (например, информационные, программные, технические, лингвистические). *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Ниже: Защищаемые ресурсы (информационной системы).

См. также: Информационная система, Отчетность (ресурсов информационной системы), Подлинность (ресурсов автоматизированной информационной системы), Подотчетность (ресурсов автоматизированной информационной системы), Целостность ресурсов информационной системы .

Ресурс объекта оценки [TOE resource] —

Все, что может быть использовано или потреблено объектом оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Объект оценки.

Ресурс системы обработки информации [resource] —

Средство системы обработки информации, которое может быть выделено процессу обработки данных на определенный интервал времени.

Примечание. Основными ресурсами являются процессоры, области основной памяти, наборы данных, периферийные устройства, программы. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Син.: Компьютерный ресурс.

Риск [risk] —

1. Влияние неопределенности на цели.

Примечание 1. Влияние — это отклонение от того, что ожидается (положительное и/или отрицательное).

Примечание 2. Цели могут иметь различные аспекты (например, финансовые и экологические цели и цели в отношении здоровья и безопасности) и могут применяться на различных уровнях (стратегических, в масштабах организации, проекта, продукта или процесса).

Примечание 3. Риск часто характеризуется ссылкой на потенциально возможные события и последствия или их комбинации.

Примечание 4. Риск часто выражают в виде комбинации последствий событий (включая изменения в обстоятельствах) и их возможности.

Примечание 5. Неопределенность — это состояние, заключающееся в недостаточности, даже частичной, информации, понимания или знания относительно события, его последствий или его возможности. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk*

Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].

2. Влияние неопределенности на цели организации.

Примечание 1. Влияние неопределенности подразумевает отклонение от ожидаемого результата.

Примечание 2. Цели организации могут иметь различные аспекты (финансовые аспекты,аспекты, связанные с охраной здоровья, безопасностью и внешней средой) и могут применяться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта или процесса.

Примечание 3. Риск часто характеризуют ссылкой на потенциальные события, их последствия или их комбинацию, а также на то, как они могут влиять на достижение целей организации.

Примечание 4. Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и связанной с ними вероятностью их возникновения. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009]*.

3. Влияние неопределенностей на процесс достижения поставленных целей.

Примечание 1. Цели могут иметь различные аспекты: финансовые, аспекты, связанные со здоровьем, безопасностью и внешней средой, и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса.

Примечание 2. Риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а также на то, как они могут влиять на достижение целей.

Примечание 3. Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

4. Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов.

Примечание. Определяется как сочетание вероятности события и его последствий. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

5. Сочетание вероятности нанесения ущерба и тяжести этого ущерба. *[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]*.

6. Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Допустимый риск, Остаточный риск, Предпочтительный риск.

См. также: Источник риска, Критерии риска, Матрица рисков, Обработка риска, Описание риска, Отчетность о риске, Подверженность риску, Управление рисками, Профиль риска, Распределение риска, Уклонение от риска, Уровень риска.

Риск-аппетит [risk appetite] —

Тип риска и его величина, к которым организация стремится или готова удерживать на себе. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Син.: Предпочтительный риск.

Риск информационной безопасности [information security risk] —

1. Потенциальная возможность того, что уязвимость будет использоваться для создания угрозы активу или группе активов, приводящей к ущербу для организации. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Примечание. Он измеряется исходя из комбинации вероятности события и его последствия. *[ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Введен в действие: 01.12.2011]*.

Син.: Риск нарушения информационной безопасности.

См. также: Угроза (безопасности информации).

Риск-менеджмент [risk management] —

См. Управление рисками, Менеджмент риска.

Риск нарушения безопасности сети электросвязи —

Вероятность причинения ущерба сети электросвязи или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в сети электросвязи. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Безопасность сети электросвязи, Меры обеспечения безопасности, Механизм обеспечения безопасности сети электросвязи.

Риск нарушения информационной безопасности —

Риск, связанный с угрозой информационной безопасности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Допустимый риск нарушения информационной безопасности, Остаточный риск нарушения информационной безопасности.

Син.: Риск информационной безопасности.

См. также: Обработка риска нарушения информационной безопасности, Оценка риска нарушения информационной безопасности.

Роль [role] **—**

1. Предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и объектом оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Примечания.

1) К субъектам относятся лица из числа руководителей организации банковской системы Российской Федерации, ее персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.

2) Объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, ресурс информационный, услуга, процесс, система, над которыми выполняются действия. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Пользователь, Объект оценки.

Роль информационной безопасности в организации —

Совокупность определенных функций и задач обеспечения информационной безопасности организации, устанавливающих допустимое взаимодействие между субъектом и объектом в организации.

Примечания.

1. К субъектам относятся лица из числа руководителей организации, ее персонал или инициируемые от их имени процессы по выполнению действий над объектами.

2. Объектами могут быть техническое, программное, программно-техническое средство, информационный ресурс, над которыми выполняются действия. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Объект обеспечения информационной безопасности, Обеспечение информационной безопасности организации.

Рубежи защиты информации —

Совокупность методов и средств, обеспечивающая многоуровневую, иерархическую систему допуска к информации с помощью различных средств,

таких как физические, технические, программные и тому подобное. Иерархическая последовательность доступа к информации реализуется по принципу «чем выше уровень доступа, тем уже круг допущенных лиц». *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Система разграничения доступа, Механизм (средство) разграничения доступа.

Руткит [rootkit] —

1. Набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), для обеспечения:

- маскировки объектов (процессов, файлов, директорий, драйверов);
- контроля (событий происходящих в системе);
- сбора данных (параметров системы).

Термин Rootkit исторически пришёл из мира UNIX, и под этим термином понимается набор утилит или специальный модуль ядра, которые злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Этот набор, как правило, включает в себя разнообразные утилиты для «заметания следов» вторжения в систему, делает незаметными снифферы, сканеры, кейлоггеры, троянские программы, замещающие основные утилиты UNIX (в случае неядерного руткита). Rootkit позволяет взломщику закрепиться во взломанной системе и скрыть следы своей деятельности путём сокрытия файлов, процессов, а также самого присутствия руткита в системе.

В систему руткит может быть установлен различными способами: загрузка посредством эксплойта, после получения шелл-доступа (в таком случае, может использоваться средство типа wget или исходный FTP-клиент для загрузки руткита с удаленного устройства), в исходном коде или ресурсах программного продукта. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

2. Программы, использующие технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов этой операционной системы. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Вредоносное программное обеспечение.

См. также: Кейлоггер, Сниффер, Троянская программа.

Сайт в сети “Интернет” —

Совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет". *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

См. также: Доменное имя, Сетевой адрес.

Самоотказ —

Самоотрицание одного из логических объектов, участвующих в обмене данными, полного или частичного своего участия в этом обмене. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Невозможность отказа.

Санкционированный доступ к информации [authorized access to information] —

Доступ к информации, не нарушающий правил разграничения доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Правила разграничения доступа, Несанкционированный доступ к информации.

Сбалансированная последовательность [balanced sequence] —

Последовательность знаков конечного алфавита X, в которой все элементы из X встречаются одинаковое число раз. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Сбор и корреляция событий безопасности [Security Information and Event Management (SIEM)] —

Высокопроизводительная мощная система управления информацией о безопасности и событиях безопасности, позволяющая автоматизировать процесс анализа событий, поступающих от средств защиты информации и повысить эффективность управления сетевой инфраструктурой в целом. Сбор и корреляция событий безопасности объединяет две отличающиеся технологии и продукты категорий: управление информацией о безопасности (SIM) и управление событиями безопасности (SEM). Решения сбора и корреляции событий безопасности — это многокомпонентная платформа, объединяющая программное обеспечение, устройства или службы управления, обычно применяемые для анализа записей журналов протоколирования данных о безопасности с любых систем, идентификации необычного поведения на уровне пользователей и генерации сообщений. Технология сбора и корреляции событий безопасности обеспечивает анализ в реальном времени извещений о нарушениях безопасности, порожденных сетевым аппаратным обеспечением и приложениями, позволяет контролировать требования политик безопасности и нормативных документов, своевременно выявлять атаки и оперативно реагировать на инциденты. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Ведение контрольных журналов, Сетевой мониторинг.

Сбор сведений из открытых источников —

Применение техник социальной инженерии требует не только знания психологии, но и умения собирать о человеке необходимую информацию.

Относительно новым способом получения такой информации стал её сбор из открытых источников, главным образом из социальных сетей.К примеру, такие сайты, как livejournal, «Одноклассники», «ВКонтакте», содержат огромное количество данных, которые люди и не пытаются скрыть. Как правило, пользователи не уделяют должного внимания вопросам безопасности, оставляя в свободном доступе данные и сведения, которые могут быть использованы злоумышленником. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Социальная инженерия.

Сведения конфиденциального характера —

Сведения, входящие в следующий перечень, утвержденный Указом Президента Российской Федерации №188 от 6 марта 1997 г.:

• сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность (данные персональные), за исключением сведений, подлежащих распространению в СМИ, в установленных федеральными законами случаях;

• сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты;

• служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

• сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и так далее);

• сведения, связанные с коммерческой деятельностью, доступ к которым ограничен органами государственной власти;

• сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. *[Указ Президента РФ от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.)]*.

Ниже: Персональные данные, Профессиональная тайна, Служебная тайна, Коммерческая тайна.

См. также: Доступ к конфиденциальной информации, Конфиденциальная информация, Охраняемые сведения.

Сведения, не подлежащие отнесению к государственной тайне и засекречиванию —

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

• о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

• о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

• о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

• о фактах нарушения прав и свобод человека и гражданина;

• о размерах золотого запаса и государственных валютных резервах Российской Федерации;

• о состоянии здоровья высших должностных лиц Российской Федерации;

• о фактах нарушения законности органами государственной власти и их должностными лицами. *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Государственная тайна, Перечень сведений, составляющих государственную тайну.

Сведения особой важности —

1. К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей. *[Постановление Правительства РФ от 04.09.1995 N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" (ред. от 22.05.2008)]*.

См. также: Гриф секретности, Секретные сведения, Совершенно секретные сведения, Степень секретности сведений, составляющих государственную тайну.

Свидетельства (доказательства) аудита информационной безопасности организации —

Записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита информационной безопасности организации и могут быть проверены.

Примечание. Свидетельства аудита информационной безопасности могут быть качественными или количественными. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Выводы аудита информационной безопасности, Заключение по результатам аудита информационной безопасности (аудиторское заключение), Критерий аудита информационной безопасности организации.

Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям —

Записи, изложение фактов или другая информация, которые имеют отношение к критериям оценки соответствия (самооценки соответствия, аудита) безопасности информационной и могут быть проверены.

Примечание. Свидетельства оценки соответствия (самооценки соответствия, аудита) ИБ могут быть качественными или количественными. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Выводы аудита информационной безопасности, Заключение по результатам аудита информационной безопасности (аудиторское заключение), Критерий аудита информационной безопасности организации.

Свидетельство [witness] —

Элемент данных, представляющий соответствующее доказательство достоверности (недостоверности) подписи проверяющей стороне. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Процесс проверки подписи.

Свойство перемешивания [mixing property] —

Строго не формализуемое свойство функции зашифрования, выражающееся, в современном понимании, в существенном усложнении взаимосвязи статистических и аналитических характеристик элементов шифрованного текста по сравнению с подобными взаимосвязями элементов открытого текста. Термин «перемешивание» перенесен в криптографию К. Шенноном из теории вероятностей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Функция зашифрования, Свойство рассеивания, Свойство усложнения, Преобразование перемешивания.

Свойство рассеивания [diffusion property] —

Строго не формализуемое свойство функции зашифрования, состоящее в том, что каждый знак открытого текста влияет на большое число знаков шифрованного текста. Термин введен К. Шенноном. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Функция зашифрования, Свойство перемешивания, Свойство усложнения, Преобразование рассеивания.

Свойство усложнения [confusion property] —

Строго не формализуемое свойство функции зашифрования, означающее сложную зависимость между ключом и шифрованным текстом. Термин введен К.Шенноном. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Функция зашифрования, Свойство перемешивания, Свойство рассеивания, Преобразование усложнения.

Сеанс работы [session] —

Интервал времени, в течение которого пользователю выделены ресурсы системы обработки информации для выполнения его работ и связи с ним в интерактивном режиме. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Интерактивный режим.

Сеансовый ключ [session key] **—**

Ключ, специально сгенерированный для одного сеанса связи между двумя участниками (протокола). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ.

См. также: Шифрование сеанса.

Секрет производства (ноу-хау) —

Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Режим коммерческой тайны, Информация, составляющая коммерческую тайну, Обладатель информации, составляющей коммерческую тайну.

Секретная информация —

Информация, содержащая сведения, отнесенные к государственной тайне. *[ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

Выше: Информация ограниченного доступа.

См. также: Секретный документ, Система защиты секретной информации

Секретность данных [data privacy] **—**

Свойство данных, предполагающее необходимость их защиты от неавторизованного доступа. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Неавторизованный доступ.

Секретные сведения —

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности. *[Постановление Правительства РФ от 04.09.1995 N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" (ред. от 22.05.2008)]*.

См. также: Гриф секретности, Сведения особой важности, Совершенно секретные сведения, Степень секретности сведений, составляющих государственную тайну.

Секретный документ —

Документ на любом носителе, отнесенный к информационным ресурсам ограниченного доступа и содержащий сведения, составляющие государственную тайну, которые включены в утвержденный специальный перечень таких сведений. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Секретная информация.

Секретный ключ [secret key] —

Ключ, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной симметричной шифрсистемы или к использованию некоторых функций данной асимметричной шифрсистемы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключ.

Син.: Закрытый ключ.

См. также: Открытый ключ.

Семейство подстановок с секретом [trapdoor permutation family] —

Семейство функций с секретом, в котором каждая функция является подстановкой. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Функция с секретом.

Семейство псевдослучайных подстановок [pseudorandom permutation family] —

Семейство псевдослучайных функций, в котором каждая функция является подстановкой. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Семейство псевдослучайных функций.

Семейство псевдослучайных функций [pseudorandom function family] —

Семейство функций, обладающее следующим свойством. Функция, выбранная равновероятно случайно из семейства, алгоритмически неотличима от случайной функции. При этом каждая из функций, и выбранная из семейства псевдослучайных функций, и случайная функция, рассматривается как черный ящик, т. е. алгоритм может только получать значения функции на выбираемых им значениях аргумента. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический примитив.

См. также: Генератор псевдослучайных функций, Черный ящик.

Семейство ЭВМ [computer family] —

Группа ЭВМ, представляющих параметрический ряд, имеющих единую архитектуру и, в большинстве случаев, одинаковую конструктивно-технологическую базу и характеризующихся полной или ограниченной некоторыми условиями программной совместимостью. *[ГОСТ 15971-90*

Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].

Ниже: Бортовая ЭВМ, МикроЭВМ, Мини-ЭВМ, Персональная ЭВМ, Специализированная ЭВМ, Супер-ЭВМ, ЭВМ общего назначения.

Сервис шифрования почтовых сообщений [secure messaging encryption] —

Сервис обеспечения безопасности корпоративной электронной почты, основанный на шифровании исходящих сообщений. Как правило, в централизованных системах исходящие сообщения сначала отправляются с использованием зашифрованного соединения, например, по протоколу SSL/TLS, в центр обработки данных, где они проверяются на наличие вирусов и, в соответствии с принятой политикой безопасности, зашифровываются на ключе адресата, а затем отправляются в почтовый ящик адресата, либо выкладываются в общий портал для совместного использования. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Электронная почта.

Сертификат [certificate] —

Документ, выданный органом сертификации в соответствии с условиями его аккредитации и содержащий соответствующий символ или заявление об аккредитации. *[ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введен в действие: 01.10.2009]*.

См. также: Документ сертификации.

Сертификат защиты —

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Защищенные средства вычислительной техники, Сертификация на соответствие требованиям по безопасности информации.

Сертификат ключа [key certificate] —

Структура данных заранее определенного формата, включающая открытый ключ, идентификационную информацию владельца ключа, а также другую служебную информацию (время действия и предназначение ключа, тип используемых криптографических алгоритмов и др.), заверенная цифровой подписью уполномоченного лица доверенного центра сертификации (удостоверяющего центра). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический примитив.

Сертификат ключа проверки электронной подписи —

Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. Сертификат ключа проверки электронной подписи должен содержать следующую информацию:

1) даты начала и окончания срока его действия;

2) фамилия, имя и отчество (если имеется) - для физических лиц, наименование и место нахождения - для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

3) ключ проверки электронной подписи;

4) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

5) наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;

6) иная информация, предусмотренная частью 2 статьи 17 Федерального закона N 63, — для квалифицированного сертификата. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Ниже: Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат).

См. также: Владелец сертификата ключа проверки электронной подписи, Ключ проверки электронной подписи, Пользователь сертификата ключа проверки электронной подписи.

Сертификат соответствия —

Документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

См. также: Декларирование соответствия, Оценка соответствия, Сертификация.

Сертификат средств электронной подписи [electronic signature facility certificate] —

Документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной подписи установленным требованиям. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Средства электронной подписи.

Сертификационные испытания [certification test] —

Контрольные испытания продукции, проводимые с целью установления соответствия характеристик ее свойств национальным и (или) международным нормативно-техническим документам. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

Выше: Испытания.

См. также: Аттестационные испытания, Контрольные испытания, Типовые испытания.

Сертификация [certification] —

1. Форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

2. Действия третьей стороны, цель которых подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга соответствует определенным стандартам или другим нормативным документам. *[ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Введен в действие: 01.07.1999]*.

Ниже: Сертификация на соответствие требованиям по безопасности информации, Сертификация средств защиты информации, Сертификация средств технической защиты информации на соответствие требованиям по безопасности информации, Сертификация уровня защиты.

См. также: Маркировка, Орган по сертификации, Сертификат соответствия, Технический регламент, Стандарт, Система сертификации.

Сертификация на соответствие требованиям по безопасности информации —

Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Примечание. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Сертификация.

См. также: Сертификат защиты.

Сертификация средств защиты информации —

Осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции. Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите

государственной тайны (Функции Межведомственной комиссии по защите государственной тайны в соответствии с Указом Президента Российской Федерации от 30 марта 1994 г. N 614 временно возложены на Государственную техническую комиссию при Президенте Российской Федерации.). Участниками сертификации средств защиты информации являются:

• федеральный орган по сертификации;

• центральный орган системы сертификации (создаваемый при необходимости) — орган, возглавляющий систему сертификации однородной продукции;

• органы по сертификации средств защиты информации — органы, проводящие сертификацию определенной продукции;

• испытательные лаборатории — лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;

• изготовители-продавцы, исполнители продукции. *[Постановление Правительства РФ от 26.06.1995 N 608 "О сертификации средств защиты информации" (ред. от 21.04.2010)]*.

Выше: Сертификация.

См. также: Сертификация средств технической защиты информации на соответствие требованиям по безопасности информации, Система сертификации средств защиты информации.

Сертификация средств технической защиты информации на соответствие требованиям по безопасности информации —

Деятельность органа по сертификации по подтверждению соответствия средств технической защиты информации требованиям технических регламентов, положениям стандартов или условиям договоров. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Сертификация.

Сертификация уровня защиты [protection level certification] **—**

Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Выше: Сертификация.

См. также: Сертификат защиты.

Сетевая атака [network attack] **—**

1. Действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы. Примечание. Сетевой протокол — совокупность семантических и синтаксических правил, определяющих взаимодействие программы управления

сетью, находящейся в одной ЭВМ, с одноименными программами, находящимися в другой ЭВМ. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Компьютерная атака с использованием протоколов межсетевого взаимодействия. *[ГОСТ Р51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

Выше: Атака.

Ниже: Атака на отказ в обслуживании, Дифейсмент, Межсайтовая подделка запроса, Межсайтовый скриптинг, Сниффинг, Спуфинг, Почтовая бомба.

См. также: Безопасность связи, Сетевые компьютерные операции.

Сетевая безопасность [network security] —

См. Безопасность информационной сети.

Сетевое администрирование [network administration] —

Повседневная эксплуатация и управление сетевыми процессами и средствами, используемыми сетью. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Сетевой адрес —

1. Идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

2. Адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели международной организации по стандартизации взаимодействия открытых систем (ISO OSI). Сетевой протокол выполняет управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети. В этих протоколах решается возможность доступа к подсети, определяется маршрут передачи и осуществляется трансляция сообщения. Управление доступом на сетевом уровне позволяет отклонять нежелательные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня. Поэтому, в данных протоколах возможно выполнение требований по защите в части проверки подлинности сетевых ресурсов, источника и приемника данных, принимаемых сообщений, проведения контроля доступа к ресурсам сети. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от*

несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)].

См. также: Доменное имя, Сайт в сети “Интернет”.

Сетевой анализатор пакетов [network sniffer] —

Устройство или программное средство, используемое для сбора информации, проходящей через сети. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Выше: Анализ трафика.

Сетевой менеджмент [network management] —

Процесс планирования, разработки, реализации, эксплуатации, мониторинга и поддержки сети. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Ниже: Сетевой мониторинг.

Сетевой мониторинг [network monitoring] —

Процесс постоянного наблюдения и проверки зафиксированных данных о сетевой деятельности и операциях, включая контрольные журналы и предупреждения об опасности, и связанный с этим анализ. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Выше: Сетевой менеджмент.

См. также: Анализ трафика, Безопасность информационной сети, Ведение контрольных журналов, Инструментальные средства аудита, Сбор и корреляция событий безопасности, Сетевой сканер.

Сетевой сканер [network scanner] —

Программа, которая осуществляет сбор информации о сети для нахождения компьютеров и программ, потенциально уязвимых к атакам. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Син.: Сканер уязвимости программ.

См. также: Сетевой мониторинг.

Сетевой трафик [network traffic] —

Объём информации, передаваемой через компьютерную сеть за определенный период времени. Количество трафика измеряется как в пакетах, так и в битах, байтах и их производных: килобайт (Кб), мегабайт (Мб) и т. д.

Трафик различают на:

- входящий (информация, поступающая в сеть);
- исходящий (информация, поступающая из сети);
- внутренний (в пределах определенной сети, чаще всего локальной);

- внешний (за пределами определенной сети, чаще всего — интернет-трафик).

Программы, осуществляющие подсчёт сетевого трафика: TMeter, BWMeter, NetWorx, DU Meter, NetTraffic, NetBalancer. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Трафик

См. также: Анализ трафика.

Сетевой червь [network worm] —

1. Разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные компьютерные сети. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

2. К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, интернет-пейджеры, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных сетевых червей распространяются в виде файлов: вложений в электронные письма, ссылкой на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и пр.

Некоторые сетевые черви (так называемые "бесфайловые" или "пакетные" черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии сетевые черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые сетевые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, содержат троянские функции или заражают выполняемые файлы на локальном диске, т. е. имеют свойства троянской программы и/или компьютерного вируса. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Компьютерный вирус .

См. также: Зомби.

Сетевые анализаторы (снифферы) [network analyzer, sniffers] —

1. Устройство или программное средство, используемое для наблюдения и анализа информационного сетевого трафика.

Примечание. До проведения анализа информационного потока информация должна быть собрана определенным образом, например, путем

использования сетевого анализатора пакетов. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Выше: Анализ трафика.

См. также: Руткит, Сниффинг.

Сетевые компьютерные операции —

Операции, объектом воздействия в которых являются компьютерные системы (отдельные компьютеры), а средой проведения — линии коммутации, объединенные в компьютерные сети. Они включают компьютерную сетевую атаку, защиту компьютерных сетей и связанные с ними действия по использованию компьютерных сетей. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Безопасность связи, Сетевая атака.

Сеть [network] **—**

Семантическая структура, состоящая из сущностей и их взаимосвязей.

Примечание. В топологии сети или в абстрактной структуре сети соединенные сущности обозначаются точками на схеме, а взаимосвязи — линиями на схеме. в компьютерной сети соединенными сущностями являются компьютеры или оборудование коммуникации данных, а взаимосвязями — парные связи данных. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Ниже: Информационно-телекоммуникационная сеть, Компьютерная сеть, Пользователь сети.

См. также: Узел

Сеть связи [communication network] **—**

1. Технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи. *[Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004]*.

2. Совокупность электрических сетей связи и сетей почтовой связи. Сеть связи функционирует как взаимоувязанный производственно-хозяйственный комплекс, предназначенный для удовлетворения нужд граждан, органов государственной власти и управления, обороны, безопасности, охраны правопорядка физических и юридических лиц в услугах электрической и почтовой связи.

Примечание. Сети электрической связи реализуют передачу и прием любых знаков, сигналов, письменного текста, изображений, звуков по

проводной, радио-, оптической и другим электромагнитным системам. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Ниже: Защищаемая сеть связи, Средства связи, Системы передачи данных.

См. также: Безопасность сети электросвязи.

Сеть связи общего пользования —

Составная часть Взаимоувязанной сети связи Российской Федерации, открытая для пользования физическим и юридическим лицам, в услугах которой этим лицам не может быть отказано.

[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].

Выше: Информационно-безопасная (защищенная) сеть связи общего пользования (служба электросвязи).

Син.: Информационные сети общего пользования.

См. также: Система обеспечения безопасности сети связи общего пользования.

Сеть ЭВМ —

См. Компьютерная сеть.

Сигнал [signal] **—**

Физическое явление, наличие, отсутствие или изменение которого представляет данные. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Ниже: Информативный сигнал.

Силы ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре —

Уполномоченные подразделения федерального органа исполнительной власти в области обеспечения безопасности, физические лица и специально выделенные сотрудники организаций, осуществляющих эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры на правах собственности либо на иных законных основаниях, а также сотрудники предприятий - разработчиков аппаратных средств и программного обеспечения, используемых в автоматизированных системах управления КВО, принимающие на основании законодательства Российской Федерации участие в восстановлении штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

См. также: Средства ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре, Инцидент (компьютерный).

Силы обеспечения национальной безопасности —

Вооруженные Силы Российской Федерации, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства Российской Федерации. *[Указ Президента РФ от 12.05.2009 N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"]*.

Выше: Система обеспечения национальной безопасности.

См. также: Средства обеспечения национальной безопасности.

Силы обнаружения и предупреждения компьютерных атак —

Уполномоченные подразделения федерального органа исполнительной власти в области обеспечения безопасности, федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры, а также физические лица и специально выделенные сотрудники организаций, осуществляющих эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры на правах собственности либо на иных законных основаниях, принимающие участие в обнаружении и предупреждении компьютерных атак на критическую информационную инфраструктуру, мониторинге уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов на основании законодательства Российской Федерации. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

Выше: Единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов, Средства обнаружения и предупреждения компьютерных атак.

Симметричная шифрсистема [secret key cryptosystem, symmetric cryptosystem] —

Система шифрования, в которой симметричным образом используются секретные ключи зашифрования и ключи расшифрования. В симметричной шифрсистеме ключи зашифрования и расшифрования в большинстве случаев совпадают, а в остальных случаях один легко определяется по другому. Криптографическая стойкость симметричной шифрсистемы определяется трудоемкостью, с которой противник и/или нарушитель может вычислить любой из секретных ключей, и оценивается при общепринятом допущении, что противнику и/или нарушителю известны все элементы шифрсистемы, за

исключением ключа секретного (правило Керкгоффса). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Асимметричная шифрсистема, Правило Керкгоффса.

Синхропосылка [synchrosignal] —

1. Значения исходных открытых параметров алгоритма криптографического преобразования. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

2. Комбинация знаков, передаваемая по каналу связи и предназначенная для вхождения в связь аппаратуры шифрования или для синхронизации аппаратуры. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Вектор инициализации.

Система [system] —

1. Множество элементов и отношений между ними, рассматриваемых как единое целое.

Примечание. Такими элементами могут быть как материальные, так и логические объекты, а также результаты деятельности людей (например, организационные формы предприятий, математические методы и языки программирования). *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Ниже: Информационная система, Информационно-телекоммуникационная система.

См. также: Информационная технология.

Система аттестации объектов информатизации по требованиям безопасности информации —

Является составной частью единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации и подлежит государственной регистрации в установленном Госстандартом России порядке. Деятельность системы аттестации организует федеральный орган по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации, которым является Гостехкомиссия России. *[Положение по аттестации объектов информатизации по требованиям безопасности информации. (утв. Председателем Гостехкомиссии 25.11.1994)]*.

См. также: Аттестация объектов информатизации.

Система документов по информационной безопасности в организации —

Объединенная целевой направленностью упорядоченная совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Обеспечение информационной безопасности организации.

Система защиты государственной тайны —

Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях. *[Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне" (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Государственная тайна, Разглашение государственной тайны.

Система защиты информации —

Совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно — распорядительными и нормативными документами в области защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Защита информации, Объект защиты информации, Техника защиты информации.

Система защиты информации автоматизированной системы —

Совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

См. также: Система защиты информации.

Система защиты информации от несанкционированного доступа [system of protection from unauthorized access to information] —

Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Ниже: Служебная информация системы защиты информации от НС.

См. также: Защита информации от несанкционированного доступа (ЗИ от НСД).

Система защиты персональных данных —

Включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. *[Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Вступило в силу: 15.11.2012]*.

См. также: Безопасность персональных данных, Актуальные угрозы безопасности персональных данных.

Система защиты секретной информации [secret information security system] —

Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Секретная информация.

Система идентификации [identification system] —

Криптографическая система, выполняющая аутентификацию сторон в процессе информационного взаимодействия. Математическая модель системы идентификации включает протокол идентификации и ключевую систему. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая система.

Ниже: Протокол идентификации, Ключевая система.

Система имитозащиты [integrity system] —

Криптографическая система, выполняющая аутентификацию сообщений и предназначенная для защиты от несанкционированного изменения информации или навязывания ложной информации. В частности, система имитозащиты обеспечивает целостность информации. Математическая модель системы имитозащиты включает алгоритм имитозащищающего кодирования (это может быть алгоритм шифрования, код аутентификации, либо др. преобразование) и алгоритм принятия решения об истинности полученной информации, а также ключевую систему. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая система.

Ниже: Алгоритм имитозащищающего кодирования, Ключевая система.

См. также: Имитозащита.

Система информационной безопасности —

Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Система обеспечения информационной безопасности.

См. также: Защитная мера.

Система испытаний [test system] —

Совокупность средств испытаний, исполнителей и определенных объектов испытаний, взаимодействующих по правилам, установленным соответствующей нормативной документацией. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011].*

См. также: Испытания.

Система контроля [inspection system] —

Совокупность средств контроля, исполнителей и определенных объектов контроля, взаимодействующих по правилам, установленным соответствующей нормативной документацией. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011].*

См. также: Комплекс технического контроля, Метод контроля, Объект технического контроля.

Система контроля и управления доступом (СКУД) —

Совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП. Основная задача - управление доступом на заданную территорию (кого пускать, в какое время и на какую территорию),включая также:

- ограничение доступа на заданную территорию
- идентификация лица, имеющего доступ на заданную территорию

Дополнительные задачи:

- учёт рабочего времени;
- расчет заработной платы (при интеграции с системами бухгалтерского учёта);
- ведение базы персонала / посетителей;
- интеграция с системой безопасности, например:

с системой видеонаблюдения для совмещения архивов событий систем, передачи системе видеонаблюдения извещений о необходимости стартовать запись, повернуть камеру для записи последствий зафиксированного подозрительного события;

с системой охранной сигнализации (СОС), например, для ограничения доступа в помещения, стоящие на охране, или для автоматического снятия и постановки помещений на охрану.

с системой пожарной сигнализации (СПС) для получения информации о состоянии пожарных извещателей, автоматического разблокирования эвакуационных выходов и закрывания противопожарных дверей в случае пожарной тревоги.

На особо ответственных объектах сеть устройств СКУД выполняется физически несвязанной с другими информационными сетями. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Доступ, Контроль доступа, Контролируемая зона.

Система менеджмента [management system] —

1. Система для разработки политики и целей и достижения этих целей.

Примечание. Система менеджмента организации может включать в себя различные системы менеджмента, такие как система менеджмента качества, система финансового менеджмента или система экологического менеджмента. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

2. Система, включающая в себя политики, процедуры, рекомендации и связанные с ними ресурсы для достижения целей организации. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

См. также: Менеджмент.

Система менеджмента информационной безопасности [information security management system (ISMS)] —

1. Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Примечание. Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы. *[ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен в действие: 01.02.2008]*.

2. Часть менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Выше: Система обеспечения информационной безопасности См. также: Система управления безопасности информационной, Проект СМИБ.

Система обеспечения безопасности сети связи общего пользования —

Совокупность служб безопасности операторов сетей электросвязи ССОП и используемых ими механизмов обеспечения безопасности, взаимодействующая с органами управления сетями электросвязи, организация и функционирование которой осуществляется по нормам, правилам и обязательным требованиям, установленным в области связи. *[ГОСТ Р 52448-*

2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007].

См. также: Сеть связи общего пользования, Служба безопасности сети электросвязи, Политика безопасности оператора связи .

Система обеспечения информационной безопасности —

Совокупность системы информационной безопасности и системы менеджмента информационной безопасности организации банковской системы Российской Федерации. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Ниже: Система информационной безопасности, Система менеджмента информационной безопасности.

См. также: Область действия системы обеспечения информационной безопасности.

Система обеспечения информационной безопасности Российской Федерации —

Часть системы обеспечения национальной безопасности страны. Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с федеральным законодательством РФ участие в решении задач обеспечения информационной безопасности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

См. также: Государственная политика обеспечения информационной безопасности Российской Федерации.

Система обеспечения информационной безопасности сети связи Российской Федерации —

Совокупность правовых норм, организационных и технических мероприятий, служб информационной безопасности и механизмов защиты, органов управления и исполнителей, направленных на противодействие заданному множеству угроз информационной безопасности ВСС РФ с целью сведения до минимума возможного ущерба пользователю или оператору связи ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Ниже: Служба информационной безопасности Взаимоувязанной сети связи Российской Федерации.

См. также: Обеспечение информационной безопасности Взаимоувязанной сети связи Российской Федерации, Услуга информационной безопасности Взаимоувязанной сети связи Российской Федерации (сети связи общего пользования, службы электросвязи), Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Система обеспечения национальной безопасности —

Силы и средства обеспечения национальной безопасности. *[Указ Президента РФ от 12.05.2009 N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"]*.

Ниже: Силы обеспечения национальной безопасности, Средства обеспечения национальной безопасности.

См. также: Обеспечение национальной безопасности.

Система обнаружения вторжения [Intrusion Detection System (IDS)] —

1. Специализированная система, используемая для идентификации того факта, что была предпринята попытка вторжения, вторжение происходит или произошло, а также для возможного реагирования на вторжение в информационные системы и сети. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — Intrusion Detection System (IDS). Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Обычно архитектура СОВ включает:

- сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;
- подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров;
- хранилище, обеспечивающее накопление первичных событий и результатов анализа;
- консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Вторжение, Обнаружение вторжений, Средство обнаружения вторжений , Система предотвращения вторжений.

Система обработки данных [data processing system] —

Один или большее число компьютеров, периферийного оборудования и программных средств, которые выполняют обработку данных.

Примечание. Система обработки данных может также выполнять операции обработки информации. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Виртуальная машина, Экспертная система.

Система обработки информации [information processing system] —

1. Одна или большее число систем обработки данных и устройств, таких как офисное и коммуникационное оборудование, которые выполняют обработку информации. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации. *[ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Введен в действие: 01.02.2008]*.

Выше: Информационная система.

См. также: Пользователь системы обработки информации, Обработка информации, Процесс обработки данных, Технические средства системы обработки информации, Устройство управления системы обработки информации, Функциональное устройство системы обработки информации.

Система оценки [evaluation scheme] —

1. Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ИСО/МЭК 15408. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют РД "Критерии оценки безопасности информационных технологий". *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Орган оценки, Объект оценки.

Система предотвращения вторжений [Intrusion Prevention System (IPS)] —

1. Вид систем обнаружения вторжений, специально предназначенных для обеспечения активной возможности реагирования. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Системы IPS можно рассматривать как расширение Систем обнаружения вторжений (IDS), так как задача отслеживания атак остается одинаковой. Однако, они отличаются в том, что IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Возможные меры — блокировка потоков трафика в сети, сброс соединений, выдача сигналов оператору. Также IPS могут выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами.

Классификация:

- Сетевые IPS (Network-based Intrusion Prevention, NIPS): отслеживают трафик в компьютерной сети и блокируют подозрительные потоки данных.

- IPS для беспроводных сетей (Wireless Intrusion Prevention Systems, WIPS): проверяет активность в беспроводных сетях. В частности, обнаруживает неверно сконфигурированные точки беспроводного доступа к сети, атаки человек посередине, спуфинг mac-адресов. См. en:Wireless intrusion prevention system.

- Поведенческий анализ сети (Network Behavior Analysis, NBA): анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS атаки.

- Система предотвращения вторжений для отдельных компьютеров (Host-based Intrusion Prevention, HIPS): резидентные программы, обнаруживающие подозрительную активность на компьютере. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Система обнаружения вторжения, Вторжение, Предотвращение вторжений.

Система предотвращения утечек [Data Loss Prevention (DLP), Data Leak Prevention, Content Monitoring and Filtering (CMF), Information Protection and Control (IPC), Extrusion Prevention System (EPS)] —

Технические устройства (программные или программно-аппаратные) для предотвращения утечек конфиденциальной информации из информационной системы вовне. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется. Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента. Первый способ позволяет избежать ложных срабатываний (ошибок второго рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Пропуски конфиденциальной информации (ошибки первого рода) при этом методе

вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются. В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста. Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п. Хостовые компоненты также стараются отслеживать изменение сетевых настроек, инсталляцию программ для туннелирования, стеганографии и другие возможные методы для обхода контроля. DLP-система должна иметь компоненты обоих указанных типов плюс модуль для централизованного управления. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Защита и контроль информации.

Система (протокол) электронных платежей [electronic cash system, e-cash system] —

Система осуществления транзакций и взаиморасчетов между сторонами в электронной (безбумажной) форме. Различают: электронные системы перевода денежных средств с использованием электронных систем обмена данными (межбанковские переводы), и системы, в которых используются дематериализованные денежные аналоги. Последние различаются по степени дематериализации: электронные деньги, виртуальные деньги и цифровые деньги. Система (протокол) электронных платежей состоит из набора протоколов, из которых основными являются протоколы, реализующие транзакцию снятия со счета, транзакцию платежа и транзакцию депозита. Если для выполнения транзакции платежа необходимо участие банка-эмитента, осуществляющего выдачу в обращение дематериализованных денег, то система (протокол) электронных платежей называется централизованной системой электронных платежей, в противном случае — автономной системой электронных платежей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Прикладной криптографический протокол.

Ниже: Автономная система электронных платежей, Централизованная система электронных платежей Транзакция (протокол) платежа, Транзакция (протокол) снятия со счета.

См. также: Транзакция (протокол) снятия со счета, Транзакция (протокол) платежа, Транзакция (протокол) депозита, Электронные деньги, Виртуальные деньги, Цифровые деньги.

Система разграничения доступа [access control mechanism, security policy realization] —

1. Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

2. Оборудование или обеспечение программное, процедуры системы автоматизированной, процедуры администратора и их различные комбинации, которые обнаруживают, предотвращают доступ несанкционированный и разрешают законный доступ в системах автоматизированных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Права доступа, Защита от несанкционированного доступа (Защита от НСД), Механизм (средство) разграничения доступа, Управление доступом.

Система риск-менеджмента [risk management framework] —

Набор компонентов, обеспечивающих основы и организационную структуру для разработки, внедрения, мониторинга, пересмотра и постоянного улучшения риск-менеджмента в масштабе всей организации.

Примечание 1. Основы включают политику, цели, полномочия и обязательства по управлению риском.

Примечание 2. Организационная структура включает планы, взаимосвязи, ответственность, ресурсы, процессы и деятельность.

Примечание 3. Система риск-менеджмента встроена во все стратегические и операционные политики и практики организации. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Мониторинг (в области риск-менеджмента).

Система сертификации —

Совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

См. также: Сертификация.

Система сертификации средств защиты информации —

Совокупность участников сертификации, осуществляющих ее по установленным правилам. Системы сертификации создаются федеральными органами по сертификации. *[Постановление Правительства РФ от 26.06.1995 N 608 "О сертификации средств защиты информации" (ред. от 21.04.2010)]*.

См. также: Сертификация средств защиты информации.

Система стандартов по защите информации —

Совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты

информации. *[ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Введен в действие: 01.09.2013]*.

См. также: Стандарт.

Система управления информационной безопасностью (СУИБ) —

Та часть общей системы управления, основанной на оценке бизнес рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

Примечание. Система управления включает в себя организационную структуру, политики, действия по планированию, распределение ответственности, практики, процедуры, процессы и ресурсы. *[BS ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements Дата принятия: 14.10.2005 Перевод: ООО «GlobalTrust Solutions»]*

См. также: Система менеджмента безопасности информационной.

Система управления ключами [key management system] —

Подсистема ключевой системы, определяющая порядок регистрации ключей, их использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей. Целью управления ключами является нейтрализация таких угроз, как компрометация и несанкционированное использование ключей, например, использование ключа, срок действия которого истек. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Ключевая система.

См. также: Механизм (средство) разграничения доступа, Компрометация криптографических ключей.

Система управления конфигурацией [configuration list] —

Документ с выходными данными системы управления конфигурацией, в котором перечисляются все элементы конфигурации для конкретного продукта с указанием точной версии каждого элемента конфигурации, актуальной для конкретной версии продукта в целом.

Примечание. Данный список позволяет отличать элементы, относящиеся к оцененной версии продукта, от других версий этих элементов, относящихся к другим версиям данного продукта. Окончательный список управления конфигурацией является конкретным документом для конкретной версии конкретного продукта. (Данный список может быть документом в электронном виде в рамках инструментальных средств управления конфигурацией. В этом случае он может рассматриваться в качестве определенного представления системы управления конфигурацией или части системы, а не в качестве выходных данных системы. Вместе с тем, для практического использования при оценке список конфигурации будут предположительно поставляться как часть документации для оценки.) Список конфигурации определяет элементы, на которые распространяются требования по управлению конфигурацией.

[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].

См. также: Конфигурация, Список конфигурации, Управление конфигурацией.

Система установки ключей [key establishment system] —

Подсистема ключевой системы, определяющая алгоритмы и процедуры генерации, распределения, передачи и проверки ключей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Кючевая система.

Система цифровой подписи [digital signature cryptosystem] —

Криптографическая система, выполняющая аутентификацию источника данных или аутентификацию сообщения. Предназначена для защиты от отказа субъектов от некоторых из ранее совершенных ими действий. Например, отправитель может отказаться от факта передачи сообщения, утверждая, что его создал сам получатель, а получатель может модифицировать, подменить или создать новое сообщение, а затем утверждать, что оно получено от отправителя. Математическая модель системы цифровой подписи включает схему цифровой подписи и ключевую систему, в качестве которой обычно выступает инфраструктура открытых ключей. Для разрешения споров необходима процедура арбитража, с помощью которой третья сторона — арбитр — разрешает споры о подлинности цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая система.

Ниже: Схема цифровой подписи, Ключевая система.

См. также: Цифровая подпись, Аутентификация сообщения, Аутентификация сторон, Невозможность отказа, Арбитраж.

Система шифрования [cryptosystem, cipher] —

Криптографическая система, предназначенная для защиты информации от лиц, не имеющих права доступа к ней. Защита обеспечивается путем зашифрования информации. Математическая модель системы шифрования включает способ кодирования исходной и выходной информации, шифр и ключевую систему. Основными требованиями, определяющими качество системы шифрования, являются: криптографическая стойкость, имитостойкость, помехоустойчивость шифра и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая система.

Ниже: Асимметричная шифрсистема, Блочная шифрсистема, Симметричная шифрсистема, Поточная шифрсистема.

Син.: Шифрсистема.

См. также: Криптографическая стойкость, Имитостойкость, Помехоустойчивость шифра.

Систематический анализ скрытых каналов [systematic covert channel analysis] —

Анализ, при котором разработчик системы информационных технологий и автоматизированных систем должен идентифицировать скрытые каналы структурированным и повторяемым образом в противоположность идентификации скрытых каналов частным методом, применимым для конкретной ситуации.

Примечание. Идентификация скрытых каналов осуществляется, как правило, в соответствии с планом обеспечения безопасности. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также Исчерпывающий анализ скрытых каналов.

Системная программа [system program] —

1. Программа, не привязанная к конкретным прикладным задачам, которая поддерживает работу прикладных программ.

Примечание. Примером является операционная система. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

2. Программа, предназначенная для поддержания работоспособности системы обработки информации или повышения эффективности ее использования в процессе выполнения прикладных программ. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Сообщение системы.

Системный журнал [audit trail] —

Хронологически упорядоченная совокупность записей результатов деятельности субъектов и пользователей компьютерной системы, предназначенная для просмотра и анализа последовательности действий и событий для инспекции конечного результата и выявления попыток несанкционированного доступа. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Мониторинг, Ведение контрольных журналов.

Системный процесс [system process] —

Процесс обработки данных, в виде которого функционируют определенные компоненты управляющей программы. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Системы передачи данных [data transfer system] —

Разновидность сетей электросвязи, в которых передача информации осуществляется в цифровом виде и на основе специальных протоколов обмена информацией между отправителем и получателем. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Сеть связи.

Скамминг [skamming] —

От английского "scamming", что означает "жульничество", вид интернет - мошенничества. Заключается в привлечении клиентов, якобы брачными агентствами (на самом деле скам - агентствами), с целью выуживания у них денег брачными аферами. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

Выше: Интернет – мошенничество.

Сканер уязвимости программ [network security scanner] —

Программа, которая осуществляет проверку больших групп компьютеров в Интернете в поисках машин, уязвимых к тому или иному конкретному виду атаки. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Син.: Сетевой сканер.

Скимминг [skiming] —

От англ. skim — снимать сливки. Частный случай кардинга, при котором используется скиммер — инструмент злоумышленника для считывания, например, магнитной дорожки платёжной карты. При осуществлении данной мошеннической операции используется комплекс скимминговых устройств:

- инструмент для считывания магнитной дорожки платёжной карты — представляет собой устройство, устанавливаемое в картоприёмник, и картридер на входной двери в зону обслуживания клиентов в помещении банка. Представляет собой устройство со считывающей магнитной головкой, усилителем — преобразователем, памятью и переходником для подключения к компьютеру. Скиммеры могут быть портативными, миниатюрными. Основная идея и задача скимминга — считать необходимые данные (содержимое дорожки/трека) магнитной полосы карты для последующего воспроизведения её на поддельной. Таким образом, при оформлении операции по поддельной карте авторизационный запрос и списание денежных средств по мошеннической транзакции будут осуществлены со счета оригинальной, «скиммированной» карты;
- миниатюрная видеокамера, устанавливаемая на банкомат и направляемая на клавиатуру ввода в виде козырька банкомата либо посторонних накладок, например, рекламных материалов — используется вкупе со скиммером для получения ПИН держателя, что позволяет получать наличные в банкоматах по поддельной карте (имея данные дорожки и ПИН оригинальной).

Данные устройства питаются от автономных источников энергии — миниатюрных батарей электропитания, и, для затруднения обнаружения, как правило, изготавливаются и маскируются под цвет и форму банкомата.

Скиммеры могут накапливать украденную информацию о пластиковых картах, либо дистанционно передавать её по радиоканалу злоумышленникам, находящимся поблизости. После копирования информации с карты мошенники изготавливают дубликат карты и, зная ПИН, снимают все деньги в пределах лимита выдачи, как в России, так и за рубежом. Также мошенники могут использовать полученную информацию о банковской карте для совершения

покупок в торговых точках. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Кардинг.

Ниже: Шимминг.

Скомпрометированный ключ [compromised key] —

Секретный ключ, ставший доступным лицам, не имеющим допуска к ключам данной симметричной шифрсистемы или к использованию некоторых функций данной асимметричной шифрсистемы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Компрометация криптографических ключей, Секретный ключ.

Скремблер [scrambler] —

Устройство, осуществляющее преобразование сигнала путем изменений соотношений между временем, амплитудой и частотой, не выходящих за пределы используемого диапазона. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографические средства физического и канального уровня.

Скрытые точки входа [backdoors, trapdoors] —

1. Вредоносные программы, предназначенные для скрытого входа в систему в обход стандартной процедуры аутентификации и получения прямого доступа к данным. Термин trapdoors введен в работе Petersen and Turn. Proceedings of AFIPS Conference. 1967. В настоящее время используется более современный термин backdoors в связи с тем, что термин trapdoors приобрел несколько иной смысл в криптографии с открытым ключом. При компрометации системы вредоносным программным обеспечением оно может устанавливать несколько скрытых точек входа для облегчения последующего входа в систему. Скрытые точки входа также могут быть установлены в системе предварительно для облегчения атаки системы обеспечением программным вредоносным. Идея оставления скрытых точек входа принадлежит разработчикам компьютерной техники, предусматривающим возможность входа в систему для осуществления технической поддержки и ремонта компьютеров. Скрытые точки входа обычно используются для осуществления скрытого удаленного доступа. Для установки скрытых точек входа применяются троянские программы, сетевые черви и другие методы. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. Программы скрытого удаленного администрирования, также известные как "бэкдоры" (backdoors). Являются разновидностью троянских программ (trojans), предоставляющих злоумышленнику возможность несанкционированного удаленного управления зараженным компьютером.

Доступные злоумышленнику действия определяются функционалом подобной программы. Как правило, злоумышленник может принимать и отсылать файлы, запускать и уничтожать их, выводить различные сообщения, стирать информацию, перезапускать компьютер и т. п. Таким образом, "бэкдоры" могут быть использованы для обнаружения и передачи конфиденциальной информации, для запуска вирусов, уничтожения данных и пр.

"Бэкдоры" по своей сути являются достаточно мощными утилитами удаленного администрирования компьютеров. Своей функциональностью они во многом напоминают легально распространяемые коммерческие системы администрирования. Классифицировать их как вредные троянские программы позволяет одна лишь особенность: отсутствие предупреждения пользователя об инсталляции и последующем запуске.

При запуске "бэкдор" скрытно устанавливает себя в операционную систему и затем следит за ней, не выдавая пользователю никаких сообщений. Более того, запущенный "бэкдор" может отсутствовать в перечне активных приложений. В результате пользователь не знает о присутствии в системе троянской программы удаленного администрирования, в то время как его компьютер открыт для управления злоумышленником. *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

Выше: Вредоносное программное обеспечение
Син.: Бэкдоры, Программа скрытого удаленного администрирования
См. также: Люки, Троянская программа, Сетевой червь, Удаленный доступ.

Скрытый канал [covert channel] —

1. Специально созданный несанкционированный канал передачи сигналов, который позволяет пользователю скрытно нарушать многоуровневую политику разграничения доступа и требования подконтрольности использования объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Непредусмотренный разработчиком системы технологий информационных и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности. По механизму передачи информации скрытые каналы подразделяют на: скрытые каналы по памяти; скрытые каналы по времени; скрытые статистические каналы. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Ниже: Скрытый канал по времени, Скрытый канал по памяти, Скрытый статистический канал.

См. также: Глубина анализа скрытого канала, Идентификация скрытого канала, Пропускная способность скрытого канала, Угрозы безопасности, реализованные с помощью скрытых каналов.

Скрытый канал по времени [covert timing channel] —

Скрытый канал по времени предполагает, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени. Например, в многозадачной операционной

системе центральный процессор является разделяемым информационно-вычислительным ресурсом для прикладных программ. Модулируя время занятости процессора, приложения могут передавать друг другу нелегальные данные. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Выше: Скрытый канал.

См. также: Скрытый канал по памяти, Скрытый статистический канал.

Скрытый канал по памяти [covert storage channel] —

Основан на наличии памяти, в которую передающий субъект записывает информацию, а принимающий — считывает ее. Скрытость каналов по памяти определяется тем, что сторонний наблюдатель не знает того места в памяти, где записана скрываемая информация. К. с. по памяти предполагает использование ресурсов памяти, однако способ использования памяти не учитывается разработчиками системы защиты и поэтому не может выявляться используемыми средствами защиты. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Выше: Скрытый канал.

См. также: Скрытый канал по времени, Скрытый статистический канал.

Скрытый статистический канал [covert statistical channel] —

Использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре к. с. Например, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в системе компьютерной. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Выше: Скрытый канал.

См. также: Скрытый канал по времени, Скрытый канал по памяти.

Слабый ключ [weak key] —

Ключ криптосистемы, при котором заметно ухудшаются характеристики криптографической стойкости криптосистемы по сравнению со средними значениями тех же характеристик при ключе, случайно равновероятно

выбранном из ключевого множества криптосистемы. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптографическая стойкость.

Слепая цифровая подпись [blind digital signature] —

Цифровая подпись, сформированная с использованием схемы цифровой подписи вслепую. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Схема цифровой подписи вслепую.

Служба безопасности сети электросвязи —

Организационно-техническая структура оператора сети электросвязи, реализующая политику безопасности оператора связи и обеспечивающая функционирование системы обеспечения безопасности сети связи общего пользования. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Безопасность сети электросвязи, Меры обеспечения безопасности, Механизм обеспечения безопасности сети электросвязи, Система обеспечения безопасности сети связи общего пользования.

Служба информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Организационно-техническая структура системы обеспечения информационной безопасности ВСС РФ, реализующая решение определенной задачи, направленной на противодействие той или иной угрозе информационной безопасности ВСС РФ. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Выше: Система обеспечения информационной безопасности сети связи Российской Федерации.

См. также: Администратор (руководящий орган) системы обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации, Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Служба информационной безопасности организации —

Организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, направленной на противодействие угрозам информационной безопасности организации. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Обеспечение информационной безопасности организации.

Служба электросвязи —

Организационно-техническая структура на базе сети (или совокупности сетей) связи, обеспечивающая обслуживание пользователей с целью удовлетворения их потребностей в определенном наборе услуг электросвязи.

[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000].

Выше: Информационно-безопасная (защищенная) сеть связи общего пользования (служба электросвязи).

Служебная информация —

1. Информация, не содержащая сведений, составляющих государственную тайну, определяемая установленными в государстве ведомственными перечнями собственников информации, циркулирующая в органах государственной власти и управления, а также в государственных и коммерческих предприятиях и учреждениях, выполняющих государственные заказы, подлежащая защите (собственником этой информации) от иностранных технических разведок и от ее утечки при передаче по каналам и сетям связи. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

2. Сведения, появляющиеся в связи с реализацией функций государственной службы. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

3. Любая информация, в том числе информация ограниченного доступа, образующаяся в результате деятельности государственных и негосударственных предприятий, организаций или учреждений и реализации профессиональных функций персонала. Круг сведений, составляющих служебную информацию, охватывает все сферы деятельности органов государственной власти. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Служебная информация ограниченного распространения, Служебная тайна.

Служебная информация ограниченного распространения —

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью. Не могут быть отнесены к служебной информации ограниченного распространения:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая - - информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

- решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка "Для служебного пользования". *[Постановление Правительства РФ от 03.11.1994 N 1233 " Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии"]*.

См. также: Служебная информация, Безопасность персональных данных, Некритичная информация.

Служебная информация системы защиты информации от НСД —

Информационная база АС, необходимая для функционирования системы защиты информации от НСД (уровень полномочий эксплуатационного персонала АС, матрица доступа, ключи, пароли и т.д.). *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

Выше: Система защиты информации от несанкционированного доступа.

Служебная тайна —

1. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии в Граждански кодексом Российской Федерации и федеральными законами. *[Указ Президента РФ от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями от 23 сентября 2005 г.)]*.

2. Защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

Выше: Сведения конфиденциального характера.

Ниже: Налоговая тайна.

См. также: Служебная информация.

Случайное число [random number] —

Число, выбранное из определенного набора чисел таким образом, что каждое число из данного набора может быть выбрано с одинаковой вероятностью. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Последовательность случайных чисел.

Случайные угрозы —

Угрозы, которые возникают непреднамеренно. Примерами реальных случайных угроз могут служить отказы системы, операционные грубые ошибки и ошибки в программных комплектах. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды угроз.

Син. Непреднамереныые угрозы.

Смежные права —

Интеллектуальные права на результаты исполнительской деятельности (исполнения), на фонограммы, на сообщение в эфир или по кабелю радио- и телепередач (вещание организаций эфирного и кабельного вещания), на содержание баз данных, а также на произведения науки, литературы и искусства, впервые обнародованные после их перехода в общественное достояние. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008]*.

См. также: Знак правовой охраны смежных прав, Объекты смежных прав.

Сниффер [sniffer] —

См. Сетевые анализаторы.

Сниффинг [sniffing] —

Вид сетевой атаки, также называемый «пассивное прослушивание сети». Несанкционированное прослушивание сети и наблюдение за данными производятся при помощи специальной не вредоносной программы — пакетным сниффером, который осуществляет перехват всех сетевых пакетов домена, за которым идет наблюдение. Перехваченные таким сниффером данные могут быть использованы злоумышленниками для легального проникновения в сеть на правах фальшивого пользователя. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Сетевая атака.

См. также: Сниффер.

Соавторство —

Граждане, создавшие произведение совместным творческим трудом, признаются соавторами независимо от того, образует ли такое произведение неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение. *[Гражданский кодекс Российской Федерации*

(часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008].

См. также: Автор результата интеллектуальной деятельности.

Собственник информации —

См. Владелец информации.

Собственность —

Право отдельных лиц контролировать или влиять на сбор и хранение относящейся к ним информации и на определение тех, кем и для кого может быть раскрыта эта информация.

Примечание. Поскольку данный термин относится к праву отдельных лиц, он не может быть точно определен и его использования следует избегать, за исключением обоснованных случаев для запрашиваемой защиты. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].*

См. также: Собственник информации.

Событие [event] **—**

1. Возникновение или изменение ряда конкретных обстоятельств.

Примечание 1. Событие может быть одним или несколькими явлениями и может иметь несколько причин.

Примечание 2. Событие может заключаться в том, что какое-то явление не имело места.

Примечание 3. Иногда событие может рассматриваться как «инцидент» или «несчастный случай».

Примечание 4. Событие без последствий можно также рассматривать как «случайное избежание», «инцидент», «почти опасное или опасное», «почти произошедшее». *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

2. Возникновение или наличие определенной совокупности обстоятельств.

Примечание 1. Характер, вероятность и последствия события могут быть не полностью известны.

Примечание 2. Событие может возникать один или несколько раз.

Примечание 3. Вероятность, связанная с событием, может быть оценена.

Примечание 4. Событие может состоять из невозникновения одного или нескольких обстоятельств.

Примечание 5. Непредсказуемое событие иногда называют «инцидентом».

Примечание 6. Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию (инциденту), опасным состоянием, опасным стечением обстоятельств и т. д. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в*

организации. Основные термины и определения. Введен в действие: 01.10.2009].

См. также: Последствие (в области риск-менеджмента).

Событие в системе информационной безопасности [information security event] —

Выявленное состояние системы, услуги или состояние сети, указывающее на возможное нарушение политики обеспечения информационной безопасности, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуация, которая может иметь значение для безопасности. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

Син.: Событие информационной безопасности.

Событие информационной безопасности [information security event] —

1. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

2. Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. *[ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введен в действие: 01.02.2008]*.

Син.: Событие в системе информационной безопасности.

См. также: Управление событиями безопасности.

Совершенная стойкость (шифрсистемы) [perfect secrecy] —

Свойство системы шифрования, заключающееся в том, что шифрованный текст не содержит информации о ключе и открытом тексте, кроме, возможно, его длины. Например, таким свойством обладает шифрсистема гаммирования, если применяемая гамма является реализацией идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Совершенный шифр.

Совершенная схема разделения секрета [perfect secret sharing scheme] —

Схема разделения секрета, в которой доли секрета любой неправломочной коалиции не позволяет получить никакой информации о значении секрета. Такие схемы называют совершенными, чтобы отличить их от

тех схем разделения секрета, в которых неправомочные коалиции могут получить частичную информацию о секрете. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема разделения секрета.

Совершенно секретные сведения —

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей. *[Постановление Правительства РФ от 04.09.1995 N 870 "Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" (ред. от 22.05.2008)]*.

См. также: Гриф секретности, Сведения особой важности, Секретные сведения, Степень секретности сведений, составляющих государственную тайну.

Совершенное доказательство с нулевым разглашением [perfect zero-knowledge proof] —

Предельный случай доказательства с нулевым разглашением, в котором количество дополнительной информации, которую может получить проверяющий в результате выполнения протокола, равно нулю. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Доказательство с нулевым разглашением.

Совершенный шифр [perfect cipher] —

Шифр, при использовании которого шифрованный текст не дает противнику, не знающему секретного ключа, никакой информации о открытом тексте, т. е. условное распределение на множестве открытых текстов при заданном шифрованном тексте совпадает с безусловным распределением на множестве открытых текстов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Совершенная стойкость (шифрсистемы).

Совет безопасности Российской Федерации —

Совет Безопасности является конституционным совещательным органом, осуществляющим подготовку решений Президента Российской Федерации по вопросам обеспечения безопасности, организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества Российской Федерации с иностранными государствами, по иным вопросам, связанным с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также по вопросам международного сотрудничества в области обеспечения безопасности. Совет Безопасности формируется и возглавляется Президентом Российской Федерации. *[Федеральный закон от 28.12.2010 N 390-ФЗ “О безопасности”. Введен в действие: 29.12.2010]*.

Содержание деятельности по обеспечению безопасности —

Деятельность по обеспечению безопасности включает в себя:

1) прогнозирование, выявление, анализ и оценку угроз безопасности;

2) определение основных направлений государственной политики и стратегическое планирование в области обеспечения безопасности;

3) правовое регулирование в области обеспечения безопасности;

4) разработку и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности, локализации и нейтрализации последствий их проявления;

5) применение специальных экономических мер в целях обеспечения безопасности;

6) разработку, производство и внедрение современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения безопасности;

7) организацию научной деятельности в области обеспечения безопасности;

8) координацию деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области обеспечения безопасности;

9) финансирование расходов на обеспечение безопасности, контроль за целевым расходованием выделенных средств;

10) международное сотрудничество в целях обеспечения безопасности;

11) осуществление других мероприятий в области обеспечения безопасности в соответствии с законодательством Российской Федераци. *[Федеральный закон от 28.12.2010 N 390-ФЗ “О безопасности”. Введен в действие: 29.12.2010]*.

Соискатель лицензии —

Юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии. *[Федеральный закон от 04.05.2011 N 99-ФЗ "О лицензировании отдельных видов деятельности" (с изменениями на 2 июля 2013 года). Введен в действие: 03.11.2011]*.

См. также: Лицензирование.

Сокрытие информации [information hiding] —

Использование способов хранения и передачи информации, основанных на использовании изначально неизвестных для противника каналов передачи и носителей информации. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Сообщение (пакет, кадр) [message] —

Блок данных, передаваемый средствами передачи и имеющий в составе заголовок и содержательную (информационную) часть. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Подписанное сообщение.

Сообщение системы [system message] —

Сообщение любой из системных программ, входящих в операционную систему. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Системная программа.

Сопровождающий [guide] —

Лицо, назначаемое проверяемой организацией для оказания помощи и содействия группе по аудиту. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Аудитор, Группа по аудиту, Наблюдатель, Технический эксперт.

СОРМ —

Система технических средств по обеспечению оперативно-розыскных мероприятий. Разработана ФСБ и внедряется на основании Закона РФ «Об оперативно-розыскной деятельности в Российской Федерации» от 12.08.95 № 144-ФЗ. В соответствии с приказом Минсвязи РФ№ 135 от 08.11.95№ 135 «О внедрении системы технических средств по обеспечению оперативно-розыскных мероприятий на электронных АТС на территории Российской Федерации» СОРМ «... должна устанавливаться на отечественных и импортных электронных телефонных станциях всех телефонных сетей: общего пользования, ведомственных и выделенных сетей, независимо от формы собственности». *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Составной ключ [composite key] —

См. Ключ (криптосистемы).

Сохранение риска [risk retention] —

Принятие потерь или выгод от достигнутого уровня риска.

Примечание 1. Сохранение риска предполагает принятие остаточного риска.

Примечание 2. Сохраняемый уровень риска (3.6.1.8) зависит от критериев риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Удержание риска.

Социальная инженерия [social engineering] —

1. Метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. Зачастую социальную инженерию рассматривают как незаконный метод получения информации, однако это не совсем так. Социальную инженерию можно также использовать и в законных целях — не только для получения информации, но и для совершения действий конкретным человеком. Сегодня социальную инженерию зачастую используют в интернете, для получения закрытой

информации, или информации, которая представляет большую ценность. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

2. Обход системы безопасности информационной системы с помощью нетехнических мер (обмана и т.д.). *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

3. Метод несанкционированного доступа к информационным ресурсам основанный на особенностях психологии человека. Основной целью социальных инженеров, как и других хакеров и взломщиков, является получение доступа к защищенным системам с целью кражи информации, паролей, данных о кредитных картах и т.п. Основным отличием от стандартной кибер-атаки является то, что в данном случае в роли объекта атаки выбирается не машина, а ее оператор. Именно поэтому все методы и техники социальных инженеров основываются на использовании слабостей человеческого фактора, что считается крайне разрушительным, так как злоумышленник получает информацию, например, с помощью обычного телефонного разговора или путем проникновения в организацию под видом ее служащего. Для защиты от атак данного вида следует знать о наиболее распространенных видах мошенничества, понимать, что на самом деле хотят взломщики и своевременно организовывать подходящую политику безопасности. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Ниже: Претекстинг, Фишинг, Вишинг, Троянская программа, Троянский конь, Дорожное яблоко, Кви про кво, Сбор сведений из открытых источников.

См. также: Обратная социальная инженерия.

Спам [spam] —

1. Телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определелить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя *[Постановление Правительства РФ от 10.09.2007 N 575 "Об утверждении Правил оказания телематических услуг связи" (ред. от 16.02.2008). Вступило в силу 01.08.2008]*.

2. Незапрашиваемые сообщения электронной почты, содержание которых может быть вредоносным и (или) мошенническим. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

3. Массовая широковещательная рассылка с помощью специальных программ рекламных сообщений или сообщений иного содержания без предварительного согласия абонента или адресата их получать. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Абузоустойчивый хостинг, Антиспам-бот.

Специализированная ЭВМ [specialized computer] —

ЭВМ, имеющая функциональные возможности и конструктивные особенности, позволяющие использовать ее для эффективного решения ограниченного класса задач в определенных условиях окружающей среды. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Выше: Семейство ЭВМ.

Специальная проверка —

1. Проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Проверка компонентов автоматизированной системы, осуществляемая с целью поиска и изъятия закладочного устройства. *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

См. также: Программная закладка, Аппаратная закладка, Закладочное устройство, Средство поиска закладочных устройств.

Специальная проверка объекта обработки информации —

Проверка технических средств и систем объекта защиты с целью выявления специально установленного закладного устройства. *[ОСТ В1 00464-82 Защита информации об авиационной технике и вооружении от иностранных технических разведок. Термины и определения. Введен в действие: 01.01.1998]*.

См. также: Закладочное устройство.

Специальное закладное электронное устройство —

См. Аппаратная закладка.

Специальное исследование (объекта защиты информации) —

1. Исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Выявление с использованием контрольно-измерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации *[ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введен в действие: 06.04.2000]*.

См. также: Канал утечки информации.

Специальное исследование (объекта технической защиты информации) —

Исследования с целью выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на

объекте технической защиты информации) требованиям нормативных правовых документов в области безопасности информации. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Технический канал утечки информации.

Специальные информационные операции —

Информационные операции, которые в силу своего секретного характера, их возможного потенциального эффекта или воздействия, соображений безопасности или угрозы национальной безопасности требуют особого процесса рассмотрения и одобрения. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

Специальный защитный знак (СЗЗ) —

Сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности СЗЗ путем сравнения самого знака или композиции «СЗЗ - подложка» по критериям соответствия характерным признакам визуальными, инструментальными и другими методами. *[Руководящий документ Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Идентификация специального защитного знака, Несанкционированный доступ к информации, Стойкость защитных свойств специального защитного знака.

Список доступа [access control list] —

Перечень пользователей сети, которым разрешен доступ к информационному ресурсу, с указанием предоставленных прав доступа. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Син.: Список управления доступом.

См. также: Доступ, Управление доступом, Права доступа.

Список конфигурации [configuration list] —

Документ с выходными данными системы управления конфигурацией, в котором перечисляются все элементы конфигурации для конкретного продукта с указанием точной версии каждого элемента конфигурации, актуальной для конкретной версии продукта в целом.

Примечание. Данный список позволяет отличать элементы, относящиеся к оцененной версии продукта, от других версий этих элементов, относящихся к другим версиям данного продукта. Окончательный список управления конфигурацией является конкретным документом для конкретной версии конкретного продукта. (Данный список может быть документом в электронном виде в рамках инструментальных средств управления конфигурацией. В этом случае он может рассматриваться в качестве определенного представления системы управления конфигурацией или части системы, а не в качестве выходных данных системы. Вместе с тем, для практического использования

при оценке список конфигурации будут предположительно поставляться как часть документации для оценки.) Список конфигурации определяет элементы, на которые распространяются требования по управлению конфигурацией. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Система управления конфигурацией.

Список полномочий [privilege matrix)] —

Строка, элементы которой определяют права (полномочия, привилегии) определенного субъекта относительно защищаемых данных. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Нарушение полномочий, Полномочие.

Список управления доступом —

Список логических объектов, имеющих разрешение на доступ к ресурсу, вместе с перечнем их прав на доступ. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Син.: Список доступа.

См. также: Доступ, Управление доступом, Права доступа.

Способ защиты информации —

Порядок и правила применения определенных принципов и средств защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Способы действий по защите информации.

Способ шифрования [encryption method (cipher type)] —

Способ преобразования множества открытых сообщений в множество шифрованных сообщений и обратно. Основные известные способы шифрования реализуются шифром гаммирования, шифром простой замены и шифром перестановки, а также их комбинациями. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Шифрование, Шифр гаммирования, Шифр перестановки.

Способы действий по защите информации —

Выявление возможных каналов утечки информации, поиск и обнаружение реальных каналов утечки информации, оценка степени опасности каждого реального канала, локализации (подавление) опасных каналов и контроль надежности защитных мероприятий. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Способ защиты информации.

Способы несанкционированного доступа —

1. Приемы и порядок действий с целью получения (добывания) охраняемых сведений незаконным путем. *[Ярочкин В.И., Шевцова В.А. Словарь*

терминов и определений по безопасности и защите информации. М.: Ось-89, 1996].

2. К способам несанкционированного доступа относятся: инициативное сотрудничество (предательство, измена), склонение (принуждение, побуждение) к сотрудничеству (подкуп, шантаж), подслушивание переговоров, незаконное ознакомление, хищение, подделка (модификация), уничтожение (порча, разрушение), незаконное подключение к системам и линиям связи и передачи информации; перехват акустических и электромагнитных сигналов, визуальное наблюдение, фотографирование, сбор и анализ документов, публикаций и промышленных отходов. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Син.: Основные способы несанкционированного доступа.

См. также: Несанкционированный доступ.

Справедливая схема цифровой подписи вслепую [fair blind signature scheme] —

Схема цифровой подписи вслепую, в которой неотслеживаемость получателей подписей может быть, при определенных условиях, отозвана. В системах электронных платежей такие схемы используются для предотвращения так называемых «идеальных» преступлений (безусловная неотслеживаемость электронных платежных средств обеспечивает преступникам возможность безопасного получения выкупа или отмывания денег). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи вслепую.

См. также: Система (протокол) электронных платежей.

Спуфинг [spoofing] —

1. Маскировка под легального пользователя или сетевой ресурс. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Общее название для сетевых атак, когда один участник маскируется под другого. В большинстве своём spoofing-атаки направлены на то, чтобы заставить жертву отправлять трафик не легитимному получателю напрямую, а атакующему, который затем уже ретранслирует трафик дальше. При этом атакующий получает возможность модификации трафика или, как минимум, его просмотра. В случае IP-spoofing'a преследуется другая цель — заставить жертву поверить, что трафик приходит от легитимного отправителя и поверить ему (или как минимум, пропустить его). *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Сетевая атака.

См. также: Сетевой трафик.

Сравнительная оценка риска [risk evaluation] —

Процесс сравнения результатов анализа риска с критериями риска для определения приемлемости риска.

Примечание. Сравнительная оценка риска может быть использована при принятии решения об обработке риска. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Оценивание риска.

См. также: Исключение риска.

Среда передачи —

Физическая реализация процесса передачи информации. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Син.: Канал передачи данных.

Средства вычислительной техники [hardware] **—**

См. Аппаратное обеспечение.

Средства защиты от несанкционированного доступа [protection facility] **—**

Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Син.: Средство защиты информации от несанкционированного доступа.

См. также: Защита от несанкционированного доступа (Защита от НСД).

Средства информатизации —

Программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин, средства вычислительной техники, словари, тезаурусы классификаторы, инструкции и методики, положения, уставы, должностные инструкции, эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Информационная система, Информатизация.

Средства информационного воздействия —

Совокупность специальных лингвистических, программных, технических и иных средств, обеспечивающих внедрение, извлечение, искажение или разрушение информации, информационных потоков или информационных ресурсов. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Информационно-техническое воздействие, Разрушение информации, Угроза системе передачи данных.

Средства ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре —

Технологии, а также технические, программные, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, предназначенные для восстановления штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

См. также: Силы ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре, Инцидент (компьютерный).

Средства обработки информации [information processing facilities] —

Любая система обработки информации, услуга или инфраструктура, или их фактическое месторасположение. *[ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Введен в действие: 01.01.2014]*.

Син.: Средство(а) обработки информации.

См. также: Обработка информации, Система обработки информации.

Средства обеспечения национальной безопасности —

Технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению. *[Указ Президента РФ от 12.05.2009 N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"]*.

Выше: Система обеспечения национальной безопасности.

См. также: Силы обеспечения национальной безопасности.

Средства обнаружения и предупреждения компьютерных атак —

Технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры), предназначенные для обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру, мониторинга уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов. *[Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Документ Совета безопасности РФ. Принят в июле 2012]*.

Выше: Единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов, Силы обнаружения и предупреждения компьютерных атак.

Средства связи [communication facilities] —

Технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи, включая технические системы и устройства с измерительными функциями. *[Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.]*.

Выше: Сеть связи.

См. также Услуга связи, Средства телекоммуникации.

Средства телекоммуникации [telecommunication facilities] —

Совокупность средств связи, обеспечивающих передачу данных между ЭВМ и информационными системами, удаленными друг от друга на значительные расстояния. *[И. Ю. Алексеева и др. Под общ. ред. А. В. Федорова, В. Н. Цыгичко Информационные вызовы национальной и международной безопасности. – М.:ПИР-Центр, 2001]*.

См. также: Средства связи.

Средства технической защиты информации [information technical protection facilities] —

Технические средства, предназначенные для предотвращения утечки информации по одному или нескольким техническим каналам. [*Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Син.: Средство обеспечения технической защиты информации.

См. также: Утечка информации по техническому каналу, Техническая защита информации, Средство защиты информации от утечки по техническим каналам.

Средства удостоверяющего центра —

Программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

См. также: Удостоверяющий центр, Федеральный орган исполнительной власти в области обеспечения безопасности.

Средства электронной подписи [secure electronic signature devices] —

Шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций — создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа проверки электронной подписи.

При создании электронной подписи средства электронной подписи должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;

3) однозначно показывать, что электронная подпись создана.

При проверке электронной подписи средства электронной подписи должны:

1) показывать содержание электронного документа, подписанного электронной подписью;

2) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

См. также: Ключ проверки электронной подписи, Ключ электронной подписи, Федеральный орган исполнительной власти в области обеспечения безопасности, Электронный документ, Сертификат средств электронной подписи.

Средство(а) обработки информации [information processing facility(ies)] —

Любая система обработки информации, сервис или инфраструктура, или их физические места размещения. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

Ниже: Техническое средство обработки информации.

Син.: Средства обработки информации.

Средство защиты информации [protection facility] —

1. Техническое, криптографическое, программное и другое средство, предназначенное для защиты сведений, составляющих государственную тайну, средство, в которых они реализованы, а также средство контроля эффективности защиты информации. *[Федеральный закон от 21.07.1993 N 5485-1-ФЗ "О государственной тайне" (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

2. Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты

информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Ниже: Программное средство защиты информации, Средство физической защиты информации, Криптографическое средство защиты информации, Средство обеспечения технической защиты информации, Технические средства защиты (информационной безопасности), Шифровальные (криптографические) средства (средства криптографической защиты информации).

Средство защиты информации от несанкционированного воздействия —

Техническое, программное или программно-техническое средство, предназначенное для предотвращения несанкционированного воздействия на информацию или ресурсы информационной системы. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Защита информации от несанкционированного воздействия (ЗИ от НСВ), Несанкционированное воздействие на информацию.

Средство защиты информации от несанкционированного доступа —

1. Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Син.: Средства защиты от несанкционированного доступа.

Средство защиты информации от утечки по техническим каналам —

Техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Утечка информации по техническому каналу, Средства технической защиты информации.

Средство контроля эффективности защиты информации —

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Контроль эффективности защиты информации.

Средство контроля эффективности технической защиты информации —

Средство измерений, программное средство, вещество и (или) материал, предназначенные и (или) используемые для контроля эффективности

технической защиты информации. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Техническая защита информации.

Средство обеспечения технической защиты информации —

Техническое, программное, программно-техническое средство, используемое и (или) создаваемое для обеспечения технической защиты информации на всех стадиях жизненного цикла защищаемого объекта. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

Выше: Средство защиты информации.

Син.: Средства технической защиты информации, Технические средства защиты (информационной безопасности).

См. также: Техническая защита информации.

Средство обнаружения вторжений —

Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в системе или компьютерной сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности. *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Система обнаружения вторжения.

Средство поиска закладочных устройств —

Техническое средство, предназначенное для поиска закладочных устройств, установленных на объекте информатизации. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Закладочное устройство, Специальная проверка .

Средство физической защиты информации —

Средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Средство защиты информации.

См. также: Физическая защита.

Стандарт [standard] —

Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к

терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

Ниже: Закрытый стандарт, Открытый стандарт, Официальный стандарт.

См. также: Рекомендации в области стандартизации, Требование.

Стандарт функции хеширования SHS [Secure Hash Standard (SHS)] —

Стандарт США, определяющий алгоритмы вычисления значения хеш-функции: алгоритм SHA-1 (введен в действие в 1995 г.) и алгоритмы SHA-256, SHA-384, SHA-512 (введены в действие в 2002 г.). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Стандарт функции хеширования ГОСТ Р 34.11-2012, Стандарт функции хеширования ГОСТ Р 34.11-94.

Стандарт функции хеширования ГОСТ Р 34.11-2012 [GOST hash function P 34.11-2012] —

Российский стандарт хеш-функции, действующий с 01.01.2013 г. Определяет алгоритм и процедуру вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе для реализации процедур обеспечения целостности, аутентичности, электронной цифровой подписи (ЭЦП) при передаче, обработке и хранении информации в автоматизированных системах. *[ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. Введен в действие: 01.01.2013]*.

См. также: Стандарт функции хеширования SHS, Стандарт функции хеширования ГОСТ Р 34.11-94.

Стандарт функции хеширования ГОСТ Р 34.11-94 [GOST hash function P 34.11-94] —

Российский стандарт хеш-функции, действовавший с 1994 г. по 31. 12.2012 г. Определяет алгоритм вычисления значения хеш-функции. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: См. также: Стандарт функции хеширования SHS, Стандарт функции хеширования ГОСТ Р 34.11-2012.

Стандарт цифровой подписи DSS [Digital Signature Standard (DSS)] —

Стандарт цифровой подписи (США), принятый с 2000 г. Рекомендует для использования три схемы цифровой подписи: DSA — основана на вычислениях в мультипликативной группе конечного простого поля из семейства схем цифровой подписи Эль Гамаля (действует с 1994 г.); RSA — основана на вычислениях в кольце вычетов по составному модулю, ECDSA — основана на вычислениях в группе точек эллиптической кривой. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Стандарт электронной цифровой подписи ГОСТ Р 34.10-2001, Стандарт электронной цифровой подписи ГОСТ Р 34.10-2012, Стандарт электронной цифровой подписи ГОСТ Р 34.10-94.

Стандарт шифрования AES [Advanced Encryption Standard (AES)] —

Стандарт шифрования данных США, предназначенный для использования в симметричных шифрсистемах. Построен на основе базового блочного алгоритма зашифрования с размером блока 128 бит и длиной ключа 128, 192 или 256 бит. Введен в действие в 2002 г. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Алгоритм блочного шифрования, Стандарт шифрования DES, Стандарт шифрования ГОСТ 28147-89, Стандарт шифрования с депонированием ключей EES.

Стандарт шифрования DES [Data Encryption Standard (DES)] —

Стандарт шифрования данных США, предназначенный для использования в симметричных шифрсистемах. Был первым в мире открытым официальным стандартом шифрования, действовавшим с 1977 по 1997 г. Построен на основе базового блочного алгоритма зашифрования с размером блока 64 бит и длиной ключа 56 бит. Имеет 4 режима шифрования и 2 режима выработки кода аутентичности сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Алгоритм блочного шифрования, Код аутентичности сообщения, Стандарт шифрования ГОСТ 28147-89, Стандарт шифрования с депонированием ключей EES, Стандарт шифрования AES.

Стандарт шифрования ГОСТ 28147-89 [GOST 28147-89] —

Российский стандарт шифрования, предназначенный для использования в симметричных шифрсистемах. Построен на основе базового блочного алгоритма зашифрования с размером блока 64 бит. Длина ключа — 256 бит заполнения ключевого запоминающего устройства (КЗУ) и 512 бит заполнения узлов замены (УЗ). Имеет 4 режима шифрования и режим выработки имитовставки. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Алгоритм блочного шифрования, Режим выработки имитовставки, Стандарт шифрования DES, Стандарт шифрования с депонированием ключей EES, Стандарт шифрования AES.

Стандарт шифрования с депонированием ключей EES [Escrowed Encryption Standard (EES)] —

Стандарт шифрования с депонированием ключей, принятый в США в 1994 г. Основан на использовании блочного алгоритма зашифрования Skipjack с добавлением в начале шифртекста специального блока информации, называемого LEAF (law enforcement access field), позволяющего в случае необходимости по ключевой информации, хранящейся у двух официально назначенных для этой цели сторон, восстановить ключ. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Депонирование ключей, Стандарт шифрования DES, Стандарт шифрования ГОСТ 28147-89, Стандарт шифрования AES.

Стандарт электронной цифровой подписи ГОСТ Р 34.10-2001 [GOST digital signature algorithm P 34.10-2001] —

Российский стандарт подписи цифровой, действовавший с июля 2002 по 2012 г. Определяет алгоритм формирования цифровой подписи и алгоритм проверки цифровой подписи. Основан на вычислениях в группе точек эллиптической кривой над конечным простым полем и принадлежит семейству схем цифровой подписи Эль Гамаля. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи Эль Гамаля.

См. также: Стандарт цифровой подписи DSS, Стандарт электронной цифровой подписи ГОСТ Р 34.10-2012, Стандарт электронной цифровой подписи ГОСТ Р 34.10-94.

Стандарт электронной цифровой подписи ГОСТ Р 34.10-2012 [GOST digital signature algorithm P 34.10-2012] —

Российский стандарт цифровой подписи, действующий с 01.01.2013 г. Необходимость разработки настоящего стандарта вызвана потребностью в реализации электронной цифровой подписи разной степени стойкости в связи повышением уровня развития вычислительной техники. Стойкость электронной цифровой подписи основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости используемой хеш-функции по ГОСТ Р 34.11-2012. *[ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введен в действие: 01.01.2013]*.

См. также: Стандарт цифровой подписи DSS, Стандарт электронной цифровой подписи ГОСТ Р 34.10-2001, Стандарт электронной цифровой подписи ГОСТ Р 34.10-94.

Стандарт электронной цифровой подписи ГОСТ Р 34.10-94 [GOST digital signature algorithm P 34.10-94] —

Первый российский стандарт цифровой подписи, действовавший с 1994 по 2002 г. Основан на вычислениях в мультипликативной группе конечного простого поля и принадлежит семейству схем подписи цифровой Эль Гамаля. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи Эль Гамаля.

См. также: Стандарт цифровой подписи DSS, Стандарт электронной цифровой подписи ГОСТ Р 34.10-2001, Стандарт электронной цифровой подписи ГОСТ Р 34.10-2012, Стандарт электронной цифровой подписи ГОСТ Р 34.10-94.

Стандартизация [standardization] —

Деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение

упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг. *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

См. также: Стандарт.

Статистический метод [statistical cryptanalysis] **—**

Метод криптографического анализа, основанный на использовании методов математической статистики. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Статический анализ исходных текстов программ —

Совокупность методов контроля (не) соответствия реализованных и декларированных в документации функциональных возможностей обеспечения программного, основанных на анализе структурном и декомпозиции исходных текстов программ. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)]*.

См. также: Динамический анализ исходных текстов программ.

Степень секретности сведений, составляющих государственную тайну —

Должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений. Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно». *[Закон РФ от 21.07.1993 N 5485-1 “О государственной тайне” (с изменениями на 21 декабря 2013 года). Введен в действие: 21.09.1993]*.

См. также: Гриф ограничения доступа к документу, Носитель сведений, составляющих государственную тайну, Сведения особой важности, Секретные сведения, Совершенно секретные сведения.

Стойкость защитных свойств специального защитного знака —

Способность к образованию комплекса устойчивых признаков, сигнализирующих о фактах воздействия на СЗЗ или попытке доступа к объекту защиты, а также способность сохранять весь комплекс характерных признаков подлинности и целостности СЗЗ при его регламентированном использовании. *[Руководящий документ Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Специальный защитный знак (СЗЗ).

Стойкость криптографического примитива [security of a cryptographic primitive] **—**

Соответствие свойств криптографического примитива его предназначению. Например, стойкость односторонней функции предполагает отсутствие эффективных (полиномиальных) алгоритмов ее инвертирования, стойкость криптографической хеш-функции — отсутствие эффективных методов построения коллизий и т.п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптографический примитив.

Страница сайта в сети “Интернет” (интернет-страница) —

Часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет". *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

См. также: Владелец сайта в сети "Интернет", Доменное имя.

Стратегические национальные приоритеты —

Важнейшие направления обеспечения национальной безопасности, по которым реализуются конституционные права и свободы граждан Российской Федерации, осуществляются устойчивое социально-экономическое развитие и охрана суверенитета страны, ее независимости и территориальной целостности. *[Указ Президента РФ от 12.05.2009 N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"]*.

См. также: Национальная безопасность.

Стратегия защиты —

Набор критериев для обеспечения услуг защиты.

Примечание. Полная стратегия защиты неизбежно будет связана с решением многих вопросов, не входящих в сферу взаимосвязи открытых систем. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Ниже: Стратегия защиты, основанная на идентификации, Стратегия защиты, основанная на правилах.

См. также: Доверенная функциональность.

Стратегия защиты, основанная на идентификации —

Стратегия защиты информации, основанная на идентификаторах и/или атрибутах пользователей, группы пользователей или логических объектов, действующих от имени пользователей и доступных им ресурсов/логических объектов. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Стратегия защиты.

См. также: Стратегия защиты, основанная на правилах.

Стратегия защиты, основанная на правилах —

Стратегия защиты, основанная на общих правилах, предъявляемых ко всем пользователям. Эти правила обычно основываются на сравнении чувствительности доступных ресурсов и обладании отдельными пользователями, группами пользователей или логическими объектами, действующими от имени пользователей, соответствующими атрибутами. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Стратегия защиты.

См. также: Стратегия защиты, основанная на идентификации.

Стратегия национальной безопасности Российской Федерации до 2020 года —

Официально признанная система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу. Концептуальные положения в области обеспечения национальной безопасности базируются на фундаментальной взаимосвязи и взаимозависимости Стратегии национальной безопасности Российской Федерации до 2020 года и Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года. *[Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537]*.

Структура доступа [access structure] **—**

В схеме разделения секрета — разбиение семейства всех подмножеств конечного множества участников S на два подсемейства. Множества из первого семейства называются правомочными коалициями, а множества из второго — неправомочными коалициями. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Схема разделения секрета.

Структура менеджмента риска [risk management framework] **—**

Взаимосвязанные элементы, которые обеспечивают реализацию принципов и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге, анализе и постоянном улучшении менеджмента риска организации.

Примечание 1. Принципы отражают политику, цели, полномочия и обязательства в области менеджмента риска.

Примечание 2. Организационные меры включают в себя планы, взаимоотношения, подотчетность, ресурсы, процессы и действия.

Примечание 3. Структура менеджмента риска должна быть интегрирована в общую стратегию, политику и практическую деятельность организации. *[ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

См. также: Менеджмент риска.

Субъект [subject**]** **—**

Активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, которые могут явиться причинами потока информации от объекта к объекту или изменения состояния системы. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

Син.: Субъект (доступа к информации).

См. также: Объект.

Субъект доступа (в автоматизированной информационной системе) [subject] —

Лицо или единица ресурса автоматизированной информационной системы, действия которой по доступу к ресурсам автоматизированной информационной системы регламентируются правилами разграничения доступа. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Аутентификация субъекта доступа, Правила разграничения доступа.

Субъект доступа (в информационной системе) [subject] —

Лицо или единица ресурса информационной системы, действия которого по доступу к ресурсам системы информационной регламентируются правилами разграничения доступа. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Правила разграничения доступа.

Субъект (доступа к информации) [subject] —

1. Активная сущность в объекте оценки, выполняющая операции над обьектами. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие*: 01.12.2013].

2. Сущность в пределах области действия функции безопасности объекта оценки, которая инициирует выполнение операций. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

3. Лицо или процесс, действия которого регламентируются правилами разграничения доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

Син.: Субъект.

См. также: Объект, Правила разграничения доступа, Участник.

Супервизор [supervisor] —

Часть управляющей программы, координирующая распределение ресурсов системы обработки информации. *[ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992]*.

Супер-ЭВМ [supercomputer] —

ЭВМ, относящаяся к классу вычислительных машин, имеющих самую высокую производительность, которая может быть достигнута на данном этапе развития технологии и в основном предназначенных для решения сложных научно-технических задач. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]* .

Выше: Семейство ЭВМ.

Схема групповой цифровой подписи [group signature scheme] —

Схема цифровой подписи, в которой правом вычисления значения подписи обладают только члены определенной группы участников, каждый из которых обладает своим секретным ключом. Проверка цифровой подписи осуществляется с помощью единственного открытого ключа. Подписавший сообщение член группы остается анонимным. Его анонимность может быть нарушена только в случае необходимости разрешения спорной ситуации. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи.

См. также: Групповая цифровая подпись.

Схема идентификации [identification scheme] —

См. Протокол идентификации.

Схема конфиденциальной цифровой подписи [undeniable signature scheme] —

Схема цифровой подписи, в которой процедура проверки подписи предусматривает участие подписавшего. Поэтому факт подписания того или иного сообщения остается конфиденциальным и может быть установлен только в том случае, если подписывающий дает на это согласие. В схеме конфиденциальной цифровой подписи алгоритм проверки цифровой подписи замещается парой протоколов, с помощью которых подписавший доказывает с нулевым разглашением, что подпись корректна, либо, напротив, некорректна. Как и в других схемах цифровой подписи, споры о подлинности подписей решаются с помощью процедуры арбитража. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]* .

Выше: Схема цифровой подписи.

Схема предварительного распределения ключей [preliminary key distribution scheme] —

Схема разделения секрета, применяемая в сети связи для уменьшения объема хранимой информации о ключах. Суть схемы предварительного распределения ключей состоит в том, что предварительно распределяются не ключи, а сгенерированные в центре распределения ключей секретные данные меньшего объема, по которым каждый пользователь самостоятельно вычисляет

по оговоренному алгоритму необходимый для связи ключ. Схема предварительного распределения ключей должна быть устойчивой относительно компрометации части ключей, в том числе, вследствие обмана или сговора некоторых пользователей, и гибкой, т. е. быстро восстанавливаться как после частичной компрометации, так и после подключения новых пользователей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема разделения секрета.

Схема разделения секрета [secret sharing scheme] —

Состоит их трех объектов: структуры доступа и двух протоколов, называемых протоколом разделения секрета и протоколом восстановления секрета. Исходной информацией протокола разделения секрета служит секрет s, а выходом — набор долей секрета s1, ..., sn. Доля si передается i-му участнику. Всякая правомочная коалиция может однозначно восстановить секрет s с помощью долей своих частников, используя алгоритм восстановления секрета, а совокупность долей секрета, полученных любой неправомочной коалицией, не позволяет получить секрет s. В некоторых схемах разделения секрета вместо алгоритма необходим протокол разделения секрета. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Идеальная схема разделения секрета, Пороговая схема разделения секрета, Совершенная схема разделения секрета, Схема предварительного распределения ключей.

См. также: Протокол разделения секрета, Структура доступа.

Схема Фейстеля (Файштеля) [Feistel scheme] —

Способ построения цикла (раунда) шифрования в итеративных (блочных)алгоритмах шифрования на основе регистра нелинейного сдвига длины 2 с функцией обратной связи, зависящей от циклового (раундового) ключа. Схема названа по имени одного из разработчиков и запатентована в США в 1974 г. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Цикл (раунда) шифрования.

Схема цифровой подписи [digital signature scheme] —

Состоит из двух алгоритмов, алгоритма формирования цифровой подписи и алгоритма проверки цифровой подписи. Надежность схемы цифровой подписи определяется сложностью решения следующих трех задач для лица, не являющегося владельцем секретного ключа: подделки цифровой подписи, то есть вычисления значения подписи под заданным документом; создания подписанного сообщения, то есть нахождения хотя бы одного сообщения с правильным значением подписи (экзистенциальная подделка цифровой подписи); подмены сообщения, то есть подбора двух различных сообщений с одинаковыми значениями подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Прикладной криптографический протокол, Система цифровой подписи.

Ниже: Алгоритм формирования цифровой подписи, Алгоритм проверки цифровой подписи, Схема групповой цифровой подписи, Схема конфиденциальной цифровой подписи, Схема цифровой подписи вслепую, Схема цифровой подписи с доказуемостью подделки, Схема цифровой подписи Эль Гамаля.

См. также: Параметр схемы ЭЦП, Подделка цифровой подписи, Экзистенциальная подделка цифровой подписи, Пространство подписей, Арбитраж.

Схема цифровой подписи вслепую [blind signature scheme] —

Схема цифровой подписи, в которой алгоритм формирования цифровой подписи выполняется вслепую в том смысле, что этот алгоритм применяется к специально сформированному сообщению, из которого без знания секретного ключа нельзя получить никакой информации о том сообщении, которое будет извлечено из него вместе с корректной подписью получателем. Используется в системах электронных платежей как средство обеспечения неотслеживаемости. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи.

Ниже: Справедливая схема цифровой подписи вслепую.

См. также: Слепая цифровая подпись.

Схема цифровой подписи с доказуемостью подделки [fail-stop signature scheme] —

Схема цифровой подписи, позволяющая в случае обнаружения подделки подписи с вероятностью близкой к единице доказать этот факт третьим лицам. Первоначально появилась как одноразовая, то есть ее использование прекращалось после проведения доказательства подделки, но в дальнейшем была модифицирована для случая многоразового использования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи.

Схема цифровой подписи Эль Гамаля [El Gamal digital signature scheme] —

Схема цифровой подписи, основанная на задаче дискретного логарифмирования. В более широком смысле говорят о семействе схем цифровой подписи Эль Гамаля, к которому относят саму схему Эль Гамаля, схему Шнорра, схему стандарта DSA (США), ГОСТ Р.34.10 и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Схема цифровой подписи.

Ниже: Стандарт электронной цифровой подписи ГОСТ Р 34.10-2001, Стандарт электронной цифровой подписи ГОСТ Р 34.10-94.

Тайна связи —

На территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи. Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям

электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами. Операторы связи обязаны обеспечить соблюдение тайны связи. *[Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004].*

Выше: Профессиональная тайна.

Тайна страхования —

Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными статьей 139 или статьей 150 настоящего Кодекса. *[Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 N 14-ФЗ (с изменениями на 28 декабря 2013 года). Введен в действие 01.03.1996].*

Выше: Коммерческая тайна.

Телекоммуникационная система [telecommunication system] —

Система, обеспечивающая телекоммуникации и состоящая из передатчика, который получает информацию и преобразует ее в передаваемые сигналы, среды передачи, несущей сигналы, и приемника, который получает сигналы и осуществляет их обратное преобразование в удобную для использования информацию. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009].*

См. также: Телекоммуникация, Среда передачи, Канал передачи данных, Сигнал.

Телекоммуникация [telecommunication] —

Передача информации на расстояние для целей коммуникации. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009].*

См. также: Телекоммуникационная система.

Теоретико-информационная (шенноновская) стойкость [information-theoretic (Shannon) security] —

Вид теоретической стойкости, определяемый с точки зрения математической теории информации. Теоретико-информационная стойкость криптосистемы обычно характеризуется количеством информации (всмысле К. Шеннона) относительно неизвестного противнику и/или нарушителю элемента криптосистемы, содержащимся в перехваченном шифрованном тексте или других доступных данных и вычисленным в рамках той или иной вероятностной модели. Говорят также, что теоретико-информационная стойкость криптосистемы характеризует ее способность противостоять атакам со стороны противника и/или нарушителя, располагающего неограниченными вычислительными ресурсами. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Теоретическая стойкость (криптосистемы).

См. также: Теоретико-сложностная стойкость.

Теоретико-сложностная стойкость [complexity-based security] —

Вид теоретической стойкости, определяемый с точки зрения математической теории сложности алгоритмов. Теоретико-сложностная стойкость криптосистемы означает ее способность противостоять атакам со стороны противника и/или нарушителя, располагающего ограниченными вычислительными ресурсами. Ограниченность ресурсов при этом обычно понимается в том смысле, что противник может использовать только алгоритмы, для которых временная (емкостная, коммуникационная) сложность алгоритма удовлетворяет заданным ограничениям (например, полиномиальные алгоритмы). Как правило, теоретико-сложностная стойкость основывается на каком-либо криптографическом предположении. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Теоретическая стойкость (криптосистемы).

См. также: Временная сложность алгоритма, Емкостная сложность алгоритма, Коммуникационная сложность (протокола), Теоретико-информационная (шенноновская) стойкость, Криптографическое (криптологическое) предположение.

Теоретическая стойкость (криптосистемы) [theoretical security] —

Криптографическая стойкость, определяемая в рамках некоторой математической модели. Основные подходы к определению теоретической стойкости в настоящее время — теоретико-информационная стойкость и теоретико-сложностная стойкость. Рассмотрение теоретической стойкости в рамках абстрактных математических моделей позволяет говорить о доказуемой стойкости. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая стойкость.

Ниже: Теоретико-информационная (шенноновская) стойкость, Теоретико-сложностная стойкость.

Теория аутентификации Симмонса [Simmons authentication theory] —

Теория безусловно стойких протоколов аутентификации сообщений для систем имитозащиты, разработанная Г. Симмонсом, аналог теории К. Шеннона (безусловно стойких) систем секретной связи. Основу теории аутентификации составляют модель кода аутентификации, определение атак — имитация и подмена, и нижние границы длин ключей в безусловно стойких протоколах аутентификации сообщений. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Система имитозащиты, Протокол аутентификации сообщений.

Терроризм в информационном пространстве —

Использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел*

РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011].

Син.: Кибертерроризм.

См. также: Международный информационный терроризм.

Тест автокорреляции [autocorrelation test] —

Критерий проверки качества псевдослучайной последовательности, основанный на сравнении выборочной автокорреляционной функции последовательности с распределением этой функции для идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Набор статистических тестов.

Тест профиля линейной сложности [linear complexity profile test] —

Критерий проверки качества псевдослучайной последовательности, основанный на вычислении линейной сложности ее отрезков с помощью алгоритма Берлекемпа-Мэсси и на сравнении выборочного распределения полученных значений с их распределением для идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Набор статистических тестов.

Тест серий [run test] —

Критерий проверки качества псевдослучайной последовательности, основанный на сравнении суммарного числа серий из нулей и серий из единиц (в случае двоичной последовательности) с распределением этого числа для идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Набор статистических тестов.

Тест следующего бита (предсказатель) [next bit test (predictor)] —

Критерий проверки качества двоичной псевдослучайной последовательности, основанный на оценке качества наилучшего прогноза бита по значениям всех предыдущих битов. Для идеальной случайной последовательности вероятность совпадения бита с любым его прогнозом равна. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Набор статистических тестов.

Тест частот цепочек [serial test] —

Критерий проверки качества псевдослучайной последовательности, основанный на разбиении ее на цепочки заданной длины и сравнении эмпирических частот появления разных цепочек с их распределением для идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Набор статистических тестов.

Техника защиты информации —

Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства

контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Средство защиты информации, средство контроля эффективности защиты информации.

Техническая защита информации —

1. Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

2. Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

3. Обеспечение защиты некриптографическими методами информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию и носители информации в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации.

Примечание. Техническая защита информации при применении информационных технологий осуществляется в процессах сбора, обработки, передачи, хранения, распространения информации с целью обеспечения ее безопасности на объектах информатизации. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Защита информации.

См. также: Правовая защита информации, Физическая (непосредственная) защита информации, Организационная защита информации, Комплексная защита информации, Средства технической защиты информации, Средство контроля эффективности технической защиты информации, Средство обеспечения технической защиты информации

Технические средства защиты авторских прав —

Любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения. *[Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от*

23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013). Введен в действие 01.01.2008].

См. также: Авторские права, Программное пиратство.

Технические средства защиты (информационной безопасности) —

1. Оборудование, используемое для защиты информационной безопасности организации.

Примечание. Такое оборудование может быть представлено техническими и программно-техническими средствами. *[ГОСТ Р 53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009].*

2. Аппаратные (встроенные в аппаратуру) и функционирующие автономно (независимо от аппаратуры) технические средства, обеспечивающие техническую защиту конфиденциальной информации. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996].*

Син.: Средство обеспечения технической защиты информации, Техническое средство обеспечения информационной безопасности.

См. также: Техническая защита информации.

Технические средства преднамеренного силового электромагнитного воздействия —

Осуществляют искажение, уничтожение или блокирование информации путем преднамеренного силового электромагнитного воздействия:

• по сети электропитания на порты электропитания постоянного и переменного тока;

• по проводным линиям связи на порты ввода-вывода сигналов и порты связи;

• по металлоконструкциям на порты заземления и порты корпуса;

• посредством электромагнитного быстроизменяющегося поля на порты корпуса, порты ввода — вывода сигналов и порты связи. *[ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. Введен в действие: 01.07.2008].*

См. также: Устойчивость автоматизированной системы в защищенном исполнении к преднамеренному силовому электромагнитному воздействию.

Технические средства системы обработки информации —

Все оборудование, включая носители данных, предназначенное для автоматизированной обработки информации. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

См. также: Система обработки информации.

Технический канал утечки информации —

Совокупность объекта технической разведки, физической среды и средства технической разведки, которыми добываются разведывательные

данные. *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

Выше: Канал утечки информации.

См. также: Специальное исследование (объекта технической защиты информации).

Технический регламент [technical regulation] —

Документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации). *[Федеральный закон от 27.12.2002 N 184-ФЗ "О техническом регулировании" (с изменениями на 28 декабря 2013 года). Введен в действие: 01.07.2003]*.

См. также: Декларирование соответствия, Оценка соответствия, Требование.

Технический эксперт [technical expert] —

Лицо, обладающее специальными знаниями или опытом, необходимыми группе по аудиту.

Примечания:

1. Специальные знания или опыт включают в себя знания или опыт, относящиеся к организации, процессу или деятельности, подвергаемым аудиту, а также знание языка и культуры страны, в которой проводится аудит.

2. Технический эксперт не имеет полномочий аудитора в группе по аудиту. *[ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента. Введен в действие 01.02.3013]*.

См. также: Аудитор, Группа по аудиту, Наблюдатель, Сопровождающий

Техническое обеспечение автоматизированной системы [AS hardware] —

Совокупность всех технических средств, используемых при функционировании АС. *[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Автоматизированная система, Информационное обеспечение автоматизированной системы, Методическое обеспечение автоматизированной системы, Организационное обеспечение автоматизированной системы, Правовое обеспечение автоматизированной системы, Программное обеспечение автоматизированной системы.

Техническое средство обеспечения информационной безопасности —

Оборудование, используемое для обеспечения информационной безопасности организации некриптографическими методами. Примечание. Такое оборудование может быть представлено техническими и

программно-техническими средствами, встроенными в объект защиты и/или функционирующими автономно (независимо от объекта защиты). *[ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Син.: Технические средства защиты (информационной безопасности)

См. также: Техническая защита информации.

Техническое средство обработки информации —

Техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и/или передачи информации по каналам связи. К техническим средствам обработки информации относятся средства вычислительной техники, средства и системы связи, средства записи, усиления и воспроизведения звука, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекционная аппаратура и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и/или передачей информации по каналам связи. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

Выше: Средство(а) обработки информации.

См. также: Обработка информации, Средства вычислительной техники.

Технология —

1. Система взаимосвязанных методов, способов, приемов предметной деятельности. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

2. Система взаимосвязанных методов, способов, приемов предметной деятельности. *[ГОСТ Р52069.0-2013 Защита информации. Система стандартов. Основные положения. Введен в действие: 01.09.2013]*.

Технология глубокого анализа пакетов [DPL (Deep Packet Inspection (DPL), Complete Packet Inspection, Information eXtraction (IX)] —

Технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэров, Deep Packet Inspection анализирует не только заголовки пакетов, но и полное содержимое трафика на уровнях модели OSI со второго и выше. Deep Packet Inspection способно обнаруживать и блокировать вирусы, фильтровать информацию, не удовлетворяющую заданным критериям.

Deep Packet Inspection может принимать решение не только по содержимому пакетов, но и по косвенным признакам, присущим каким-то определённым сетевым программам и протоколам. Для этого может использоваться статистический анализ (например статистический анализ частоты встречи определённых символов, длины пакета и т. д.).

Deep Packet Inspection часто используются провайдерами для контроля трафика, а иногда и для блокировки некоторых приложений, таких как BitTorrent. С помощью Deep Packet Inspection можно определить, какое приложение сгенерировало или получает данные, и на основании этого предпринять какое-либо действие. Помимо блокирования, Deep Packet Inspection может собирать подробную статистику соединения каждого пользователя по отдельности. Также, при помощи quality of service Deep Packet Inspection может управлять скоростью передачи отдельных пакетов, подняв её или, напротив, уменьшив. По мнению некоторых Интернет-провайдеров, Deep Packet Inspection позволяет сдерживать приложения, забивающие Интернет-канал, изменять приоритеты передачи различных типов данных, например, ускоряя открытие Интернет страниц за счёт уменьшения скорости загрузки больших файлов. Кроме того, Deep Packet Inspection способно обнаруживать среди общего потока трафика кусочки, соответствующие компьютерным вирусам и блокировать их, повышая, таким образом, безопасность сети. Иногда Deep Packet Inspection используется в больших корпорациях для предотвращения случайных утечек данных, а также для защиты от отправки по e-mail внутренних защищённых файлов. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Фильтрация.

Тип доступа [access type] —

Сущность права доступа к определенному устройству, программе, файлу и так далее (обычно read, write, execute, append, modify, delete). *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Права доступа.

Типовые испытания [type test] —

Контрольные испытания выпускаемой продукции, проводимые с целью оценки эффективности и целесообразности вносимых изменений в конструкцию, рецептуру или технологический процесс. *[ГОСТ 16504-81 Система государственных испытаний продукции. Испытания и контроль качества продукции. Основные термины и определения. Введен в действие: 01.05.2011]*.

Выше: Испытания.

См. также: Аттестационные испытания, Контрольные испытания, Сертификационные испытания.

Толерантность к риску [risk tolerance] —

Готовность организации или заинтересованных сторон согласиться с новым уровнем риска, достигнутым после воздействия на него, для достижения установленных целей.

Примечание. На толерантность к риску могут влиять законодательные и нормативные требования. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE*

Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].

См. также: Принятие риска.

Транзакция (протокол) депозита [deposit transaction (protocol)] —

Криптографический протокол, компонент автономной системы электронных платежей. В транзакции депозита два участника — продавец и банк. Продавец посылает банку электронные монеты для депозита. Банк проверяет подлинность электронных денег и, после решения проблемы повторной траты электронных денег методом идентификации нарушителя, post factum выполняет надлежащую процедуру. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Автономная система электронных платежей.

См. также: Электронные деньги, Электронные монеты, Проблема повторной траты электронных денег.

Транзакция (протокол) платежа [payment transaction (protocol)] —

Криптографический протокол, компонент системы электронных платежей. В случае централизованной системы электронных платежей в транзакции платежа три участника — покупатель, продавец и банк. Покупатель передает электронные деньги продавцу, который, в свою очередь, пересылает их в банк. Последний проверяет подлинность электронных денег, а также выясняет, не были ли они уже потрачены ранее. Если все корректно, банк кладет электронные деньги на счет продавца и уведомляет его об этом. В автономных системах электронных платежей в транзакции платежа два участника — покупатель и продавец. Продавец может проверить только подлинность полученных электронных денег, которые он в дальнейшем в любой момент времени может положить на свой счет помощью транзакции депозита. Поскольку банк не участвует в транзакции платежа, существует угроза повторной траты электронных денег. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система (протокол) электронных платежей.

См. также: Электронные деньги, Проблема повторной траты электронных денег.

Транзакция (протокол) снятия со счета [withdrawal transaction protocol] —

Криптографический протокол, компонент системы электронных платежей. В транзакции снятия со счета два участника — банк и покупатель, являющийся клиентом этого банка. Покупатель передает банку запрос на снятие со счета определенной суммы, и банк выдает эту сумму электронными деньгами. Для защиты электронных денег от подделки банк, как правило, использует схему цифровой подписи. Неотслеживаемость платежей, осуществляемых электронными деньгами, обычно осуществляется за счет применения схемы цифровой подписи вслепую. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система (протокол) электронных платежей.

См. также: Электронные деньги, Неотслеживаемость, Схема цифровой подписи вслепую.

Трансграничная передача персональных данных [personal data transborder transmission] —

Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Выше: Обработка персональных данных.

Трансляция адреса —

Функция межсетевых экранов, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

Трафик [traffic] —

Нагрузка, создаваемая потоком вызовов, сообщений и сигналов, поступающих на средства связи. *[Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004]*.

Ниже: Сетевой трафик.

См. также: Средства связи.

Требование —

Положение нормативного документа, содержащее критерии, которые должны быть соблюдены. *[ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения. Введен в действие: 01.07.2003]*.

Требование безопасности (объекта оценки) [security requirement] —

Требование, изложенное на стандартизованном языке и направленное на достижение целей безопасности для объекта оценки. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Интерфейс функциональных требований безопасности объекта оценки, Объект оценки, Функциональные возможности безопасности объекта оценки, Элемент.

Требование по защите информации —

Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации. *[ГОСТ Р50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Син.: Требования по защите информации.

См. также: Концепция защиты информации.

Требования по защите информации —

Обязательные для применения и исполнения требования в области защиты информации некриптографическими методами, установленные нормативными правовыми актами Российской Федерации, нормативными правовыми актами федерального органа исполнительной власти, уполномоченного в области внешней разведки, принятыми в пределах его компетенции, и документами в области стандартизации. *[Постановление Правительства РФ от 21.04.2010 N 266 " Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения". Вступило в силу 12.05.2010]*.

Выше: Обязательные требования.

Син.: Требование по защите информации.

Третья сторона [third party] —

Лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме. *[ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. Введен в действие: 01.01.2014]*.

См. также: Заинтересованная сторона, Причастная сторона.

Троян [trojan] —

См. Троянская программа, Троянский конь.

Троянская программа [trojan horse] —

1. Вредоносная программа, используемая злоумышленником для сбора, разрушения или модификации информации, нарушения работоспособности компьютера или использования ресурсов пользователя в своих целях. Данная техника зачастую эксплуатирует любопытство, либо другие эмоции цели. Чаще всего злоумышленник отправляет жертве электронное сообщение, содержащее «интересный» контент, обновление антивируса, или другую информацию, способную ее заинтересовать. Открывая прикрепленный к письму файл, пользователь устанавливает себе на машину вредоносное программное обеспечение, позволяющее мошеннику получить доступ к конфиденциальной информации. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

2. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию,

нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для распределенных DoS-атак на удаленные ресурсы сети). *[Сайт Лаборатории Касперского http://www.securelist.com/ru/]*.

3. Троянской программой (троянцем, или троянским конем) называется:

- программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;

- программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

Таким образом, троянская программа — это особая разновидность программной закладки. Она дополнительно наделена функциями, о существовании которых пользователь даже не подозревает. Когда троянская программа выполняет эти функции, компьютерной системе наносится определенный ущерб. Однако то, что при одних обстоятельствах причиняет непоправимый вред, при других— может оказаться вполне полезным. К примеру, программу, которая форматирует жесткий диск, нельзя назвать троянской, если она как раз и предназначена для его форматирования (как это делает команда format операционной системы DOS). Но если пользователь, выполняя некоторую программу, совершенно не ждет, что она отформатирует его винчестер, — это и есть самый настоящий троянец. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

Выше: Вредоносное программное обеспечение, Социальная инженери

Ниже: Зевс (троянская банковская программа), Карберп (троянская банковская программа

См. также: Программная закладка, Троянский конь

Троянский конь [trojan horse] —

Специальная подпрограмма, которая разрешает действия, отличные от определенных в спецификации программы. *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm*

Выше: Виды вторжений, Социальная инженерия, Компьютерный вирус См. также: Троянская программа.

Туннелирование [tunnelling] —

Процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов. Туннелирование, как и экранирование, можно рассматривать как самостоятельную функцию-сервис безопасности. Его суть состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». Данный сервис может применяться для обеспечения

конфиденциальности и целостности всей передаваемой порции, включая служебные поля. Туннелирование может применяться как на сетевом, так и на прикладном уровнях. Комбинация туннелирования и шифрования позволяет реализовать закрытые виртуальные частные сети. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006*

См. также: Виртуальная частная сеть, Криптомаршрутизатор, Экранирование.

Угроза [threat] —

1. Потенциальная причина инцидента, который может нанести ущерб системе или организации. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

2. Потенциальная возможность нарушения защиты. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

3. Опасность, предполагающая возможность потерь (ущерба). *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

4. Потенциальная опасность нарушения одного или нескольких свойств криптографической системы (криптографического протокола), например, конфиденциальности, целостности, аутентификации, невозможности отказа, неотслеживаемости. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Активная угроза, Пассивная угроза.

Син. Угроза (безопасности информации), Угроза информационной безопасности.

См. также: Виды угроз, Управление угрозами.

Угроза (безопасности информации) [threat] —

1. Совокупность условий и факторов, создающих потенциальную или реальную опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее. *[ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

2. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

3. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации. *[Р50.1.053-2005*

Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006].

Син.: Угроза, Угроза информационной безопасности.

См. также: Инцидент информационной безопасности, Источник угрозы безопасности информации, Модель угроз (безопасности информации).

Угроза безопасности сети электросвязи —

Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба сети электросвязи или ее компонентам. *[ГОСТ Р52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Безопасность сети электросвязи, Меры обеспечения безопасности, Механизм обеспечения безопасности сети электросвязи, Риск нарушения безопасности сети электросвязи.

Угроза в информационном пространстве —

Факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве. *[Конвенция об обеспечении международной информационной безопасности (концепция). Разработана Советом безопасности РФ, Министерством иностранных дел РФ, Институтом проблем информационной безопасности (ИПИБ МГУ). Представлена 22.09. 2011]*.

Син.: Угроза информационной безопасности.

Угроза информационной безопасности [information security threat] —

Угроза нарушения свойств информационной безопасности — доступности, целостности или конфиденциальности информационных активов организации банковской системы Российской Федерации. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Син.: Угроза (безопасности информации).

См. также: Инцидент информационной безопасности.

Угроза информационной безопасности Взаимоувязанной сети связи Российской Федерации —

Возможное последствие воздействия нарушителя информационной безопасности ВСС РФ на информационную сферу ВСС РФ, непредотвращение, либо необнаружение и неликвидация которого средствами ВСС РФ может привести к ухудшению заданного уровня качества службы или к ухудшению заданных качественных характеристик функционирования ВСС РФ и, как следствие, к нанесению ущерба пользователю или оператору связи ВСС РФ.

Примечание. К потенциальным последствиям воздействия нарушителя на ВСС РФ, например, могут быть отнесены: несанкционированный доступ к услугам электросвязи ВСС РФ, несанкционированный доступ к информационной сфере ВСС РФ, несанкционированное изменение информации, несанкционированное изменение сообщения, несанкционированное изменение последовательности сообщения,

несанкционированный повтор сообщения, несанкционированное изменение маршрута сообщения, блокировка передачи информации (сообщения) пользователя. [*ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Ниже: Несанкционированный доступ к услугам электросвязи Взаимоувязанной сети связи Российской Федерации (сети связи общего пользования), Несанкционированный доступ к информационной сфере Взаимоувязанной сети связи Российской Федерации, Несанкционированное изменение информации, Несанкционированное изменение сообщения, Несанкционированное изменение последовательности сообщения, Несанкционированный повтор сообщения, Несанкционированное изменение маршрута сообщения.

См. также: Информационная сфера взаимоувязанной сети связи Российской Федерации, Нарушитель информационной безопасности Взаимоувязанной сети связи Российской Федерации.

Угроза информационной безопасности организации —

Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации. Примечание 1. Формой реализации (проявления) угрозы информационной безопасности является наступление одного или нескольких взаимосвязанных событий информационной безопасности и инцидентов информационной безопасности, приводящего(их) к нарушению свойств информационной безопасности объекта(ов) защиты организации. Примечание 2. Угроза характеризуется наличием объекта угрозы, источника угрозы и проявления угрозы. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Угроза, Обеспечение информационной безопасности организации, Нарушение информационной безопасности организации.

Угроза национальной безопасности —

Прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства. *[Указ Президента РФ от 12.05.2009 N 537 "О Стратегии национальной безопасности Российской Федерации до 2020 года"]*.

См. также: Национальная безопасность, Обеспечение национальной безопасности.

Угроза системе передачи данных —

Опасность системы передачи данных, состоящая в разрушении информации или других ресурсов; искажении или модификации информации; хищении, удалении или потере информации и/или других ресурсов; раскрытии

информации; прерывании обслуживания. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Син.: Угрозы системе передачи данных.

См. также: Средства информационного воздействия, Разрушение информации, Модификация информации.

Угрозы безопасности информационных и телекоммуникационных средств и систем —

Угрозами безопасности как уже развернутых, так и создаваемых на территории Российской Федерации информационных и телекоммуникационных средств и систем могут являться:

• противоправные сбор и использование информации;

• нарушения технологии обработки информации;

• внедрения в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

• разработка и распространения программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

• уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

• воздействие на парольно-ключевые системы защиты систем автоматизированных обработки и передачи информации;

• компрометация ключей и средств криптографической защиты информации;

• утечка информации по техническим каналам; внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

• уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

• перехват информации в сетях передачи данных и на линиях связи, дешифрирование этой информации и навязывание ложной информации;

• использование не сертифицированных отечественных и зарубежных технологий информационных, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской инфраструктуры информационной;

• несанкционированный доступ к информации, находящейся в банках и базах данных;

• нарушение законных ограничений на распространение информации. *[Доктрина информационной безопасности Российской Федерации*

(утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Компрометация криптографических ключей.

Угрозы безопасности, реализованные с помощью скрытых каналов —

Включают в себя:

• внедрение вредоносных программ и данных;

• подачу злоумышленником команд агенту для выполнения;

• утечку криптографических ключей или паролей;

• утечку отдельных информационных объектов. *[ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. Введен в действие: 01.12.2009].*

См. также: Скрытый канал.

Угрозы информационной безопасности в области науки и техники —

К числу основных внешних угроз информационной безопасности Российской Федерации в области науки и техники следует отнести:

• стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

• создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);

• политику западных стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств — участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

• активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в области науки и техники.

Угрозы информационной безопасности в общегосударственных информационных и телекоммуникационных системах —

Основными угрозами информационной безопасности Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

• деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

• вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

• нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

• использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

• привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах.

Угрозы информационной безопасности в правоохранительной и судебной сферах —

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

• разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;

• деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

• нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

• недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

• отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического и статистического характера;

• отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

• преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в правоохранительной и судебной сферах.

Угрозы информационной безопасности в сфере внешней политики —

Из внешних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

• информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Российской Федерации;

• распространение за рубежом дезинформации о внешней политике Российской Федерации;

• нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

• попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

Из внутренних угроз информационной безопасности Российской Федерации в сфере внешней политики наибольшую опасность представляют:

• нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти,

реализующих внешнюю политику Российской Федерации, и на подведомственных им предприятиях, в учреждениях и организациях;

• информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Российской Федерации;

• недостаточная информированность населения о внешнеполитической деятельности Российской Федерации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в сфере внешней политики.

Угрозы информационной безопасности в сфере внутренней политики —

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:

• нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

• недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

• распространение дезинформации о политике Российской Федерации, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

• деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в сфере внутренней политики.

Угрозы информационной безопасности в сфере духовной жизни —

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Российской Федерации:

• деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

• ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

• возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

• использование зарубежными специальными службами средств массовой информации, действующих на территории Российской Федерации, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

• неспособность современного гражданского общества России обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в сфере духовной жизни.

Угрозы информационной безопасности в сфере обороны —

Могут быть внешними и внутренними. Внешними угрозами являются:

• все виды разведывательной деятельности зарубежных государств; информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

• диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

• деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

Внутренними угрозами являются:

• нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах учреждениях Министерства обороны Российской Федерации, на предприятиях оборонного комплекса;

• преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

• ненадежное функционирование информационных и телекоммуникационных систем специального назначения;

• возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;

• нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;

• нерешенность вопросов социальной защиты военнослужащих и членов их семей. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в сфере обороны.

Угрозы информационной безопасности в сфере экономики —

Угрозы создают:

• бесконтрольная деятельность отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

• бесконтрольное привлечение иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб;

• критическое состояние предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств.

Угрозы составляют:

• возникновение технологической зависимости России от иностранных государств;

• компьютерные преступления, связанные с проникновением криминальных элементов в системы и компьютерные сети банков и иных кредитных организаций;

• недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном;

• разглашение информации, содержащей коммерческую тайну;

• в системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны

противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в сфере экономики.

Угрозы информационной безопасности в условиях чрезвычайных ситуаций —

Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях:

• к приведению в движение больших масс людей, испытывающих психический стресс;

• к быстрому возникновению и распространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)].*

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

См. также: Объекты обеспечения информационной безопасности в условиях чрезвычайных ситуаций, Чрезвычайная ситуация.

Угрозы информационной безопасности Российской Федерации —

Подразделяют на случайные и преднамеренные, активные и пассивные. К основным видам угроз информационной безопасности Российской Федерации относятся следующие:

• угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению Российской Федерации;

• угрозы информационному обеспечению государственной политики Российской Федерации;

• угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на

мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных ресурсов информационных;

• угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории Российской Федерации. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Ниже: Угрозы информационной безопасности в области науки и техники, Угрозы информационной безопасности в общегосударственных информационных и телекоммуникационных системах, Угрозы информационной безопасности в правоохранительной и судебной сферах, Угрозы информационной безопасности в сфере внешней политики, Угрозы информационной безопасности в сфере внутренней политики, Угрозы информационной безопасности в сфере духовной жизни, Угрозы информационной безопасности в сфере обороны, Угрозы информационной безопасности в сфере экономики, Угрозы информационной безопасности в условиях чрезвычайных ситуаций, Угрозы безопасности информационных и телекоммуникационных средств и систем, Угрозы информационному обеспечению государственной политики Российской Федерации, Угрозы развитию отечественной индустрии информатизации.

См. также: Виды угроз информационной безопасности Российской Федерации, Внешние источники угроз информационной безопасности Российской Федерации, Внутренние источники угроз информационной безопасности Российской Федерации.

Угрозы информационному обеспечению государственной политики Российской Федерации —

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

• монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

• блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

• низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

Угрозы международной информационной безопасности —

Условия и факторы, которые могут стать причиной нарушения мировой стабильности и безопасности государства и мирового сообщества в информационном пространстве. Такими факторами являются:

• разработка, создание и использование средств воздействия и нанесения ущерба информационным ресурсам и телекоммуникационным системам другого государства;

• целенаправленное информационное воздействие на критически важные структуры другого государства;

• информационное воздействие с целью подрыва политической, экономической и социальной системы других государств, психологической обработки населения с целью дестабилизации общества;

• несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерное использование;

• действия, ведущие к доминированию и контролю в информационном пространстве;

• противодействие доступу к новейшим информационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам;

• поощрение действий международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющих угрозу информационным ресурсам и критически важным» структурам государства;

• разработка и принятие планов, доктрин, предусматривающих возможность ведения информационных войн и способных спровоцировать гонку вооружений, а также вызвать напряженность в отношениях между государствами и собственно возникновение информационных войн;

• использование информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в сфере информационной;

• трансграничное распространение информации, противоречащей принципам и нормам международного права, а также внутреннему законодательству конкретных стран;

• манипулирование информационными потоками, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозии традиционных культурных, нравственных, этических и эстетических ценностей. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Угрозы развитию отечественной индустрии информатизации —

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных ресурсов информационных могут являться:

• противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии

информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

• закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

• вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

• увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Угрозы информационной безопасности Российской Федерации, Виды угроз информационной безопасности Российской Федерации.

Угрозы системе передачи данных —

Угрозы системе передачи данных означают следующее:

• разрушение информации или других ресурсов;

• искажение или модификацию информации;

• хищение, удаление или потерю информации и/или других ресурсов;

• раскрытие информации;

• прерывание обслуживания. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Син.: Угроза системе передачи данных.

См. также: Разрушение информации, Модификация информации.

Удаленный доступ [remote access] —

Процесс получения доступа к сетевым ресурсам из другой сети или с терминала, не являющегося постоянно соединенным физически или логически с сетью, к которой он получает доступ. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Удержание риска [risk retention] —

Принятие ответственности за возможные потери или приобретения от конкретного риска.

Примечание 1. Удержание риска включает принятие остаточного риска.

Примечание 2. Удерживаемый уровень риска может зависеть от критериев риска. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Остаточный риск.

Удостоверение личности —

Данные, передаваемые для установления заявленной подлинности логического объекта. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Удостоверяющий центр [sertification authority] —

Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом “Об электронной подписи”.

Удостоверяющий центр:

1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);

2) устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5) ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

10) осуществляет иную связанную с использованием электронной подписи деятельность. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Ниже: Аккредитованный удостоверяющий центр.

См. также: Ключ проверки электронной подписи, Ключ электронной подписи, Сертификат ключа проверки электронной подписи, Средства электронной подписи.

Узел [node] —

В Сети узел — это сущность, которая соединена с одной или более другими сущностями.

Примечание 1. В топологии сети или в ее абстрактной структуре узлы обозначаются точками на схеме. В компьютерной сети узлами являются компьютеры или оборудование коммуникации

данных.

Примечание 2. Сеть может содержать конечные узлы и промежуточные узлы. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Сеть.

Уклонение от риска [risk avoidance] —

Обоснованное решение не вовлекаться или уклоняться от действий, чтобы не подвергаться конкретному риску.

Примечание. Уклонение от риска может основываться на результатах оценивания риска и/или законодательных и нормативных обязательств. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Универсальная подделка цифровой подписи [universal forgery] —

Подделка цифровой подписи, при которой противник и/или нарушитель, не владеющий секретным ключом, создает алгоритм, функционально эквивалентный алгоритму генерации цифровой подписи. Тем самым он может подделывать цифровые подписи для любых сообщений. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Подделка цифровой подписи.

См. также: Выборочная подделка цифровой подписи, Экзистенциальная подделка цифровой подписи.

Универсальный тест Маурера [Maurer universal test] —

Критерий проверки качества псевдослучайной последовательности, основанный на вычислении сумм логарифмов от длин промежутков между повторными появлениями мультиграмм заданной длины и сравнении этой суммы с ее распределением для идеальной случайной последовательности. Универсальность теста состоит в том, что при неограниченном увеличении длин мультиграмм последовательности он обнаруживает отличие любой неидеальной стационарной случайной последовательности от идеальной. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]* .

Выше: Набор статистических тестов.

Унифицированное управление угрозами [Unified Threat Management (UTM)] —

Единое решение по обеспечению сетевой безопасности, получившее широкое распространение для защиты сетевых ресурсов организации, основанное на использовании единого защищающего шлюза. Основная идея, развивающая традиционный подход на основе файервола, заключается в совмещении в одном устройстве нескольких функций безопасности: предотвращение сетевых вторжений, антивирусный шлюз, защита от спама, виртуальная частная сеть, фильтрация содержания, балансировка нагрузки, предотвращение утечки данных, оповещение об угрозах. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*

Выше: Управление угрозами.

Уничтожение информации —

Случайное или умышленное стирание информации на ее носителях при обработке техническими средствами, в том числе хищение носителей и технических средств. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

См. также: Модификация информации, Разрушение информации.

Уничтожение персональных данных —

Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных. *[Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (ред. от 23.07.2013). Введен в действие: 26.01.2007]*.

Выше: Обработка персональных данных.

Уполномоченный пользователь (объекта оценки) [authorised user] —

1. Пользователь объекта оценки, которому в соответствии с фкнкциональным требованием безопасности разрешено выполнять некоторую операцию. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

2. Пользователь, которому в соответствии с политикой безопасности разрешено выполнять какую-либо операцию. *[ГОСТ Р53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Пользователь.

Уполномоченный федеральный орган —

В сфере использования электронной подписи определяется Правительством Российской Федерации. Уполномоченный федеральный орган:

1) осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены настоящим Федеральным законом и на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае выявления их несоблюдения выдает предписания об устранении выявленных нарушений;

2) осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров.

Уполномоченный федеральный орган обязан обеспечить хранение следующей указанной в настоящей части информации и круглосуточный беспрепятственный доступ к ней с использованием информационно-телекоммуникационных сетей:

1) наименования, адреса аккредитованных удостоверяющих центров;

2) реестр выданных и аннулированных уполномоченным федеральным органом квалифицированных сертификатов;

3) перечень удостоверяющих центров, аккредитация которых аннулирована;

4) перечень аккредитованных удостоверяющих центров, аккредитация которых приостановлена;

5) перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;

6) реестры квалифицированных сертификатов, переданные в уполномоченный федеральный орган. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Федеральные органы исполнительной власти в сфере использования электронной подписи.

См. также: Аккредитация удостоверяющего центра, Аккредитованный удостоверяющий центр, Удостоверяющий центр, Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

Управление безопасностью —

Система регулярных защитных мероприятий, направленных на обеспечение безопасности в соответствии с изменяющимися условиями внутренней и внешней среды. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

См. также: Меры защиты.

Управление доступом [access control] —

1. Предотвращение несанкционированного использования какого-либо ресурса, включая предотвращение использования ресурса неполномочным способом. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных). Управление доступом включает следующие функции защиты: идентификацию пользователей, персонала и ресурсов; проверку полномочий, разрешение и создание условий работы в пределах установленного регламента; регистрацию (протоколирование) обращения к защищаемой информации; реагирование при попытках несанкционированного действия. *[Ярочкин В.И., Шевцова В.А. Словарь терминов и определений по безопасности и защите информации. М.: Ось-89, 1996]*.

3. Наделение каждого пользователя (субъекта доступа) индивидуальными правами по доступу к ресурсу информационному и проведению операций по ознакомлению с информацией, ее документированию, модификации и уничтожению. Разграничение доступа может осуществляться по различным моделям, построенным по тематическому признаку или по грифу секретности разрешенной к пользованию информации. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

4. Совокупность методов, средств и мероприятий, обеспечивающих защиту данных от несанкционированного доступа пользователей. *[Приходько А.Я. Словарь-справочник по информационной безопасности. М.:СИНТЕГ,2001]*.

Выше: Виды механизмов защиты.

Ниже: Дискреционное управление доступом, Мандатное управление доступом.

Син.: Разграничение доступа, Контроль доступа.

См. также: Система разграничения доступа, Несанкционированный доступ, Права доступа, Список доступа, Список управления доступом, Управление идентификацией.

Управление идентификацией [Identity Management (IdM)] —

Управление процессами идентификации, аутентификации, авторизации и получения привилегий внутри или извне системы и границ организации с целью усиления защищенности, повышения производительности, а также уменьшения стоимости и времени обслуживания. Управление идентификацией отвечает за присвоение индивидуальных идентификаторов и организацию служебных данных о сторонах, в качестве которых могут выступать пользователи, компьютерное оборудование и приложения. Так как каждая из сторон может быть зарегистрирована в системе под несколькими именами, которым соответствуют различные виды доступа, то для организации контроля важно, чтобы способ идентификации позволял эффективно отслеживать действия каждой из строн. Это особенно актуально для организаций с распределенными ресурсами и большим числом пользователей, например, предприятий, занимающихся электронной коммерцией. Управление идентификацией охватывает вопросы безопасности идентификационной информации и технологии обеспечения безопасности такой информации.

Компоненты управления идентификацией могут быть классифицированы на 4 категории:

• модуль аутентификации — отвечает за управление начальной аутентификацией и управление сеансами, на которые ссылаются до тех пор, пока пользователь не выйдет из системы, либо сеанс не будет прерван по какой-либо иной причине;

• модуль авторизации — обеспечивает комплексное управление процессом предоставления полномочий на доступ по запросам, основанное на данных или информации или политиках, включающих атрибуты пользователей, ролей/групп пользователей, выбранные действия, каналы доступа, время, требуемые ресурсы, внешние данные и бизнес правила;

• модуль управления пользователями — осуществляет управление жизненным циклом пользователя, роли/группы пользователей, позволяющее организовывать и обеспечивать весь период жизни конкретного аккаунта, а также делегирование некоторых функций конечным пользователям с целью распределения нагрузки между пользовательскими устройствами организации;

• центральное хранилище идентификационных данных пользователей — осуществляет хранение объединенной идентификационной информации из различных баз данных, содержащих информацию о множествах пользователей, и предоставление идентификационной информации другим службам, обеспечивая сервис проверки данных, предоставленных клиентами. **[***Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]***.**

См. также: Управление доступом.

Управление идентификацией и доступом [Identity and Access Management (IAM)] **—**

Обеспечение доступа легитимным пользователям к запрашиваемым ресурсам в нужное время в точном соответствии с их правами. Наиболее критичное значение проблема обеспечения гарантий соответствующего доступа приобретает в связи с широким применением технологически неоднородного оборудования и необходимостью точного соответствия требованиям усиленных политик безопасности. Данная проблема имеет ключевое значение для любой организации. Правильная организация у. и. д. предоставляет возможность оптимизации затрат и, что более важно, создает условия для подключения новых приложений. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

Управление информацией о безопасности [Security Information Management (SIM)] **—**

Сферой управления информацией о безопасности является сбор, долговременное хранение и анализ сообщений, поступающих от различных источников, записей журналов протоколирования данных о безопасности систем обнаружения вторжений, межсетевых экранов, операционных систем, различных приложений, баз данных, антивирусных систем и т. д.; формирование отчетов и оповещение. При анализе данных используются

современные методы анализа данных, корреляция, фильтрация, нормализация, агрегирование и др. Предоставляет возможность централизованным образом анализировать разнородную информацию, генерируемую различными устройствами в различных форматах, сохраняемую на различных носителях и направляемую в различные места. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Проверка безопасности, Сбор и корреляция событий безопасности.

Управление информационным потоком [information flow control] —

Процедуры управления информационным потоком, удостоверяющие, что информация не может передаваться с верхних уровней безопасности на нижние (в соответствии с положениями модели Белла-Лападула). Более общее определение контроля информационных потоков подразумевает процедуры управления, удостоверяющие, что информация не может передаваться по скрытым каналам (то есть в обход политики безопасности). *[Словарь терминов по информационной безопасности http://domarev.com.ua/book-02/gloss.htm]*.

См. также: Информационный поток, Скрытый канал.

Управление конфигурацией [configuration management] —

Вид деятельности, предусматривающий техническое и административное руководство и контроль, направленные на идентификацию и документирование функциональных и физических характеристик элементов конфигурации, контроль изменений этих характеристик, регистрацию и представление информации о состоянии обработки и реализации изменений, а также - верификацию соответствия установленным требованиям. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013]*.

См. также: Система управления конфигурацией.

Управление маршрутизацией —

Применение правил в процессе маршрутизации по выбору или исключению конкретных сетей, звеньев данных или ретрансляторов. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды механизмов защиты.

Управление мобильными устройствами [Mobile Device Management (MDM)] —

Технология управления, мониторинга и поддержки мобильных устройств, развернутых мобильными операторами, провайдерами и производителями. Обычно MDM включает over-the-air распределение приложений и данных, установку конфигураций для всех типов мобильных устройств, с целью обеспечения единой функциональности, повышения безопасности коммуникаций и уменьшения временных и ресурсных затрат на поддержку.

[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013].

См. также: Доступ с собственного устройства.

Управление правами доступа к данным [Information Rights Management (IRM)] —

Технология, обеспечивающая управление доступом к контенту не зависимо от размещения, что позволяет управлять доступом к файлам, даже после того как они выходят из под контроля. Функциональность IRM обычно включает в себя:

• шифрование информации;

• защиту от копирования и печати;

• удобную политику классификации информации;

• управление правами пользователей на доступ к документам;

• аудит доступа к документам. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Управление доступом.

Управление приложениями [application control] —

Технология обеспечения безопасности корпоративной сети. Использует базу доверенных приложений (Whitelisting), содержащую полную и актуальную информацию о большинстве существующих легитимных приложений. Осуществляет детектирование, идентификацию и контроль доступа к приложениям и социальным сетям на основе установленной политики безопасности, независимо от используемого порта или протокола, включая трафик, зашифрованный по протоколу SSL. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Контроль приложений с запретом по умолчанию, Осведомленность об идентификационных данных.

Управление рисками [risk management] —

1. Скоординированные действия по управлению организацией с учетом рисков. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Координированные действия по направлению и контролю над деятельностью организации в связи с рисками. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

Син.: Риск-менеджмент, Менеджмент риска.

См. также: Отчетность о риске, План управления рисками, Политика управления рисками.

Управление событиями безопасности [Security Event Management (SEM)] —

Управление информацией о событиях безопасности, основанное на мониторинге событий в реальном времени; ранжировании информации о

событиях ИБ, что позволяет рассматривать в первую очередь наиболее критичные для функционирования информационной инфраструктуры инциденты; корреляционном анализе полученных данных на предмет определения комплексных атак сетевых, а также атак, распределенных по времени; автоматическом выявлении, определении причин и реагировании на проблемы, связанные с нарушением безопасности; визуализации полученных данных в реальном времени и оповещении операторов системы об инцидентах и об элементах сети, вовлеченных в атаку. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Событие информационной безопасности, Инцидент (компьютерный).

Управление угрозами [threat management] —

Технология обеспечения безопасности сетевых ресурсов организации, основанная на комплексном использовании различных программных и аппаратных средств, реализующих функции сетевой безопасности: предотвращение сетевых вторжений, антивирусный шлюз, защита от спама, виртуальная частная сеть, фильтрация содержания, балансировка нагрузки, предотвращение утечки данных, оповещение об угрозах и т. п. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

Ниже: Унифицированное управление угрозами.

См. также: Угроза.

Управление уязвимостями [vulnerability management] —

Деятельность, направленная на идентификацию, классификацию, устранение и ослабление уязвимостей. Основана на использовании технологий сканирования известных уязвимостей, фиксации состояний и следов работы подозрительных программ для более эффективного восстановления, а также своевременном устранении и ослаблении выявленных уязвимостей. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Уязвимость.

Управляющая последовательность [control sequence] —

Псевдослучайная последовательность или истинно случайная последовательность, используемая при реализации криптографического алгоритма. Частными случаями являются гамма шифра и ключевая последовательность. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Гамма (шифра), Ключевая последовательность.

Управляющая программа [control program] —

Системная программа, реализующая набор функций управления, в который включают управление ресурсами и взаимодействие с внешней средой системы обработки информации, восстановление работы системы после проявления неисправностей в технических средствах. *[ГОСТ 19781-90*

Обеспечение систем обработки информации программное. Термины и определения. Введен в действие: 01.01.1992].

Управляющий модуль поточной шифрсистемы [stream cipher control module] —

Часть поточной шифрсистемы, генерирующая в зависимости от ключа криптосистемы ключевую (управляющую) последовательность, определяющую в каждом такте выбор отображения для шифрования очередного блока текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].*

Выше: Поточная шифрсистема.

См. также: Шифрующий модуль поточной шифрсистемы.

Уравнение зашифрования —

Соотношение, выражающее процесс образования зашифрованных данных из открытых данных в результате преобразований, заданных алгоритмом криптографического преобразования. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990].*

См. также: Функция зашифрования, Алгоритм зашифрования, Уравнение расшифрования.

Уравнение расшифрования —

Соотношение, выражающее процесс образования открытых данных из зашифрованных данных в результате преобразований, заданных алгоритмом криптографического преобразования. *[ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990].*

См. также: Функция расшифрования, Алгоритм расшифрования, Уравнение зашифрования.

Уровень полномочий субъекта доступа [subject privilege] —

Совокупность прав доступа субъекта доступа. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)].*

См. также: Список полномочий, Права доступа.

Уровень риска [level of risk] —

Величина риска или комбинации рисков, выраженная как комбинация последствий и их возможности. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)].*

См. также: Возможность (в области риск-менеджмента), Последствие (в области риск-менеджмента).

Услуга [service] —

Результат деятельности исполнителя по удовлетворению потребности потребителя.

Примечание. В качестве исполнителя (потребителя) услуги может выступать организация, физическое лицо или процесс. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Качество услуги.

Услуга защиты [security service] —

Услуга, предоставляемая каким-либо уровнем взаимосвязанных открытых систем, которая обеспечивает адекватную защиту систем или процедур передачи данных. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Аутентификация отправителя данных, Аутентификация равноправного логического объекта, Конфиденциальность потока трафика, Избирательная защита поля.

Услуга информационной безопасности Взаимоувязанной сети связи Российской Федерации (сети связи общего пользования, службы электросвязи) —

Результат деятельности системы обеспечения информационной безопасности ВСС РФ (ССОП, службы электросвязи), предоставляемый пользователю по его запросу к соответствующей службе информационной безопасности ВСС РФ (ССОП, службы электросвязи). *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

См. также: Система обеспечения информационной безопасности сети связи Российской Федерации.

Услуга связи —

Деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи или почтовых отправлений. *[Федеральный закон от 07.07.2003 N 126-ФЗ “О связи” (с изменениями на 2 апреля 2014 года). Введен в действие: 01.01.2004]*.

См. также: Пользователь услугами связи, Оператор связи.

Услуги информационных технологий [information technologies services] —

Совокупность функциональных возможностей информационных и, возможно, неинформационных технологий, предоставляемая конечным пользователям в качестве услуги.

Примечание. Примерами услуг ИТ могут служить передача сообщений, бизнес-приложения, сервисы файлов и печати, сетевые сервисы и т.д. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Информационные технологии.

Услуги сети —

Комплекс функциональных возможностей, предоставляемых абонентам сети с помощью прикладных протоколов (протоколы электронной почты, FTP -

File Transfer Protocol - прием/передача файлов, HTTP - Hiper Text Transfer Protocol - доступ к Web-серверам, IRC - Internet Relay Chat -диалог в реальном времени, Telnet - терминальный доступ в сети, WAIS - Wide Area Information Servers - система хранения и поиска документов в сети и т.д.). *[Приказ Гостехкомиссии России от 30.08.02 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации»]*.

См. также: Провайдер сети, Абонент сети.

Установление области применения (в области риск-менеджмента) [establishing the context] —

Определение внешних и внутренних факторов, которые следует учитывать при управлении риском и установлении сферы применения критериев риска и менеджмента риска, необходимых для определения политики в области менеджмента риска. *[ГОСТ Р51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Установление ситуации (контекста).

См. также: Внешнняя область применения (в области риск-менеджмента), Внутренняя область применения (в области риск-менеджмента).

Установление ситуации (контекста) (в области риск-менеджмента) [establishing the context] —

Определение внешних и внутренних параметров, принимаемых во внимание при управлении риском, и установление области применения и критериев риска для политики управления рисками. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Син.: Установление области применения (в области риск-менеджмента).

См. также: Внешнняя ситуация (контекст) (в области риск-менеджмента), Внутренняя ситуация (контекст) (в области риск-менеджмента), Менеджмент риска информационной безопасности организации.

Установление целостности [manipulation detection] —

Процедура, позволяющая выявить, подвергалось ли сообщение или блок данных случайным или преднамеренным воздействиям. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Целостность.

Устойчивость [resilience] —

Способность организации противостоять нарушению, будучи затронутой им. *[ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. Введен в действие: 01.01.2014]*.

См. также: Нарушение.

Устойчивость автоматизированной системы в защищенном исполнении к преднамеренному силовому электромагнитному воздействию —

Свойство автоматизированной системы в защищенном исполнении выполнять свои функции и сохранять параметры в пределах установленных норм во время и после воздействия на нее воздействующего фактора в течение всего срока службы в заданных условиях эксплуатации. *[ГОСТ Р52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. Введен в действие: 01.07.2008]*.

См. также: Технические средства преднамеренного силового электромагнитного воздействия, Показатели устойчивости автоматизированной системы в защищенном исполнении.

Устойчивость организации (в области риск-менеджмента) [resilience] —

Способность организации к адаптации в сложной и изменчивой окружающей среде. *[ГОСТ Р51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Гибкость организации.

Устойчивость функционирования сети электросвязи —

Способность сети электросвязи выполнять свои функции при выходе из строя части элементов сети в результате дестабилизирующих воздействий. *[ГОСТ Р52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007]*.

См. также: Механизм обеспечения безопасности сети электросвязи, Риск нарушения безопасности сети электросвязи, Угроза безопасности сети электросвязи.

Устройство управления системы обработки информации [control unit] —

Устройство, предназначенное для выполнения функции управления в системе обработки информации в целом или ее отдельными частями. *[ГОСТ15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Система обработки информации, Функциональное устройство системы обработки информации.

Устройство хранения [storage device] —

Функциональный блок, в котором данные могут помещаться и оставаться, и из которого они могут быть получены. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Утечка информации [information loss] —

Неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками. *[ГОСТ Р53114-2008 Защита*

информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009].

Ниже: Утечка информации по техническому каналу.

См. также: Защита информации от утечки, Защищаемая информация, Несанкционированный доступ к информации, Носитель защищаемой информации, Разглашение информации.

Утечка информации по техническому каналу —

Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

Выше: Утечка информации.

См. также: Защищаемая информация, Носитель защищаемой информации, Средства технической защиты информации, Средство защиты информации от утечки по техническим каналам.

Участник [entity] **—**

Одна из сторон взаимодействия, в качестве которой может выступать пользователь, группа пользователей или устройство, способная выступать в системе в роли субъекта доступа, инициирующего выполнение операций. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013]*.

См. также: Субъект (доступа к информации).

Участник (протокола) [party] **—**

Субъект, участвующий в той или иной форме в выполнении протокола. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Центр доверия, Честный участник.

Участники электронного взаимодействия —

Осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

См. также: Информационная система общего пользования, Корпоративная информационная система.

Учетная запись [account] **—**

Запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе. Учётная запись, как правило, содержит сведения, необходимые для идентификации пользователя при подключении к системе, информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации — например, биометрические характеристики). Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде (в целях его безопасности). Учётная

запись может содержать также дополнительные анкетные данные о пользователе — имя, фамилию, отчество, псевдоним (ник), пол, национальность, расовую принадлежность, вероисповедание, группу крови, резус-фактор, возраст, дату рождения, адрес [|электронной почты, домашний адрес, рабочий адрес, нетмейловый адрес, номер домашнего телефона, номер рабочего телефона, номер сотового телефона, номер ICQ, идентификатор Skype, ник в IRC, другие контактные данные систем обмена мгновенными сообщениями, адрес домашней страницы и/или блога в Паутине или интранете, сведения о хобби, о круге интересов, о семье, о перенесённых болезнях, о политических предпочтениях, о партийной принадлежности, о культурных предпочтениях, об умении общаться на иностранных языках, о принесённых обетах, и так далее. Конкретные категории данных, которые могут быть внесены в такую анкету, определяются создателями и (или) администраторами системы. Учётная запись может также содержать одну или несколько фотографий или аватар пользователя. Учётная запись пользователя также может учитывать различные статистические характеристики поведения пользователя в системе: давность последнего входа в систему, продолжительность последнего пребывания в системе, адрес использованного при подключении компьютера, интенсивность использования системы, суммарное и (или) удельное количество определённых операций, произведённых в системе, и так далее. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Син.: Аккаунт.

Учетность —

Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Подотчетность.

Ущерб [damage] **—**

1. Отрицательные последствия, возникающие вследствие причинения вреда активам. *[ГОСТ Р53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

2. Нанесение физического повреждения или другого вреда здоровью людей, или вреда имуществу или окружающей среде. *[ГОСТ Р51898-2002 Аспекты безопасности. Правила включения в стандарты. Введен в действие: 01.01.2003]*.

3. Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации банковской системы Российской Федерации, наступивший в результате реализации угроз безопасности информационной через уязвимости

безопасности информационной. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

Уязвимость [vulnerability] —

1. Слабое место актива или меры и средства контроля и управления, которое может быть использовано угрозой. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Свойство системы, которое можно использовать для нарушения информационной безопасности системы информационных технологий и автоматизированных систем. *[ГОСТ Р53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Управление уязвимостями, Уязвимость (информационной системы), Эксплойт.

Уязвимость (автоматизированной информационной системы) —

Недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

См. также: Уязвимость, Уязвимость (информационной системы).

Уязвимость информационной безопасности [information security vulnerability] —

Слабое место в инфраструктуре организации банковской системы Российской Федерации, включая систему обеспечения информационной безопасности, которое может быть использовано для реализации или способствовать реализации угрозы информационной безопасности. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Уязвимость.

Уязвимость (информационной системы) [vulnerability] —

1. Внутренние свойства объекта, проявляющиеся в чувствительности к источнику риска, которая может привести к событию с последствием. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

2. Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Примечание 1. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе.

Примечание 2. Если уязвимость соответствует угрозе, то существует риск. *[ГОСТ Р50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*

3. Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

4. Некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

5. Свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации.

Примечание 1. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе.

Примечание 2. Если уязвимость соответствует угрозе, то существует риск. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

6. Ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты. *[Родионов С. , Комов С. , Ракитин В. , Рябцунов П. и др. Термины и определения в области информационной безопасности. М.: Издательство АС-ТРАСТ, 2009]*.

Син.: Брешь безопасности.

См. также: Уязвимость, Уязвимость (автоматизированной информационной системы), Нарушение безопасности (информационной системы), Угроза.

Уязвимость нулевого дня [zero day exploit] —

Термин, обозначающий вредоносные программы, против которых еще не разработаны защитные механизмы или уязвимости, которые не устранены. Происхождение термина связано с тем обстоятельством, что уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от неё). *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

См. также: Атака нулевого дня.

Уязвимость (объекта оценки) [residual vulnerability] —

Слабое место объекта оценки, которое может быть использовано для нарушения функциональных требований безопасности в некоторой среде. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].*

См. также: Объект оценки, Мониторинговые атаки (объекта оценки), Обнаруженные потенциальные уязвимости (объекта оценки), Остаточная уязвимость (объекта оценки), Пригодная для использования уязвимость (объекта оценки).

Уязвимость сети электросвязи —

Недостаток или слабое место в средстве связи, технологическом процессе (протоколе) обработки/передачи информации, мероприятиях и механизмах обеспечения безопасности сети электросвязи, позволяющие нарушителю совершать действия, приводящие к успешной реализации угрозы безопасности. *[ГОСТ Р 52448-2005 Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения. Введен в действие: 01.01.2007].*

См. также: Безопасность сети электросвязи, Меры обеспечения безопасности, Механизм обеспечения безопасности сети электросвязи, Риск нарушения безопасности сети электросвязи, Угроза безопасности сети электросвязи.

Файловые атрибуты —

См. Атрибуты файла.

Фактический маршрут выполнения функциональных объектов —

Последовательность фактически выполняемых функциональных объектов при определѐнных условиях (входных данных). *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)].*

Выше: Маршрут выполнения функциональных объектов.

Фактор, воздействующий на защищаемую информацию —

Явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008].*

См. также: Воздействие.

Фарминг [pharming] —

Сравнительно новый вид интернет - мошенничества. Фарминг - технологии позволяют изменять DNS (Domain Name System) записи либо записи в файле HOSTS. При посещении пользователем легитимной, с его точки зрения, страницы производится перенаправление на поддельную страницу,

созданную для сбора конфиденциальной информации. Чаще всего такие страницы подменяют страницы банков – как оффлайновых, так и онлайновых. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

Выше: Интернет – мошенничество.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) —

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере (ключевые системы информационной инфраструктуры), в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействия иностранным техническим разведкам на территории Российской Федерации;

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней на территории Российской Федерации (техническая защита информации);

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля. *[Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (с изменениями от 21 декабря 2013 г.)]*.

Федеральные органы исполнительной власти в сфере использования электронной подписи —

В соответствии со ст. 8 Федерального закона «Об электронной подписи» такими органами являются:

1) Уполномоченный федеральный орган;

2) Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий; 3) Федеральный орган исполнительной власти в области обеспечения безопасности. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной*

подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011].

Ниже: Уполномоченный федеральный орган, Федеральный орган исполнительной власти в области обеспечения безопасности, Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

Федеральные органы по сертификации —

Органы, уполномоченные проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности Российской Федерации, Министерство обороны Российской Федерации). Федеральный орган по сертификации в пределах своей компетенции:

- создает системы сертификации;
- осуществляет выбор способа подтверждения соответствия средств защиты информации требованиям нормативных документов;
- устанавливает правила аккредитации центральных органов систем сертификации, органов по сертификации средств защиты информации и испытательных лабораторий;
- определяет центральный орган для каждой системы сертификации;
- выдает сертификаты и лицензии на применение знака соответствия;
- ведет государственный реестр участников сертификации и сертифицированных средств защиты информации;
- осуществляет государственные контроль и надзор за соблюдением участниками сертификации правил сертификации и за сертифицированными средствами защиты информации, а также устанавливает порядок инспекционного контроля;
- рассматривает апелляции по вопросам сертификации;
- представляет на государственную регистрацию в Комитет Российской Федерации по стандартизации, метрологии и сертификации системы сертификации и знак соответствия;
- устанавливает порядок признания зарубежных сертификатов;
- приостанавливает или отменяет действие выданных сертификатов. *[Постановление Правительства РФ от 26.06.1995 N 608 "О сертификации средств защиты информации" (ред. от 21.04.2010)].*

См. также: Орган по сертификации, Сертификация.

Федеральный орган исполнительной власти в области обеспечения безопасности —

В сфере использования электронной подписи:

1) устанавливает требования к форме квалифицированного сертификата;

2) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра;

3) осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», и публикует перечень таких средств. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Федеральные органы исполнительной власти в сфере использования электронной подписи.

См. также: Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат), Средства электронной подписи, Средства удостоверяющего центра, Уполномоченный федеральный орган.

Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий —

В сфере использования электронной подписи устанавливает:

1) порядок передачи реестров квалифицированных сертификатов и иной информации в уполномоченный федеральный орган в случае прекращения деятельности аккредитованного удостоверяющего центра;

2) порядок формирования и ведения реестров квалифицированных сертификатов, а также предоставления информации из таких реестров;

3) правила аккредитации удостоверяющих центров, порядок проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом «Об электронной подписи» и на соответствие которым эти центры удостоверяющие были аккредитованы. *[Федеральный закон от 06.04.2011 N 63-ФЗ "Об электронной подписи" (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

Выше: Федеральные органы исполнительной власти в сфере использования электронной подписи.

См. также: Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат), Аккредитация удостоверяющего центра, Уполномоченный федеральный орган.

Физическая защита —

Средства, используемые для обеспечения физической защиты ресурсов от преднамеренной или случайной угрозы. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды механизмов защиты.

См. также: Средство физической защиты информации.

Физическая (непосредственная) защита информации [physical security] —

Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. *[ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

Выше: Защита информации.

См. также: Техническая защита информации, Правовая защита информации, Организационная защита информации, Комплексная защита информации.

Физическая охрана средств вычислительной техники —

Система мер, предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время. *[Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением председателя Гостехкомиссии при Президенте Российской Федерации от 30 марта 1992 г.)]*.

См. также: Система контроля и управления доступом (СКУД), Контролируемая зона.

Фильтрация [filtering] —

Процесс приема или отклонения потоков данных в сети в соответствии с определенными критериями. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Ниже: Пакетная фильтрация.

См. также: Критерии фильтрации, Правила фильтрации, Межсетевой экран (сетевой экран), Технология глубокого анализа пакетов.

Фильтрация URL [URL filtering (URLF)] —

Программное обеспечение для маршрутизаторов, использующее облачную классификацию URL, обеспечивающее возможность проверки протокола SSL и интеграцию с функциональным модулем контроля приложений, реализующее централизованное управление всеми аспектами web-безопасности. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*.

Фильтрующая функция [filtering function] —

Функция, используемая для усложнения псевдослучайной последовательности, вырабатываемой линейным регистром сдвига, при построении управляющей последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Финансирование риска [risk financing] —

Форма воздействия на риск, предусматривающая меры резервирования фондов на непредвиденные расходы для погашения или изменения финансовых

последствий в случае их возникновения. *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

Выше: Воздействие на риск.

Фишинг [phishing] **—**

1. Технология интернет - мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д. При помощи спамерских рассылок или почтовых червей потенциальным жертвам рассылаются подложные письма, якобы от имени легальных организаций, в которых их просят зайти на подделанный преступниками "сайт" такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, используемую в последствии злоумышленниками для кражи денег со счета жертвы и в других преступлениях. *[Сайт Компьютерная помощь. Лучшие антивирусы-бесплатные и лицензионные. http://help-antivirus.ru/]*.

2. Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков (Ситибанк, Альфа-банк), сервисов (Rambler, Mail.ru) или внутри социальных сетей (Facebook, Вконтакте, Одноклассники.ru). В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг». *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

Выше: Социальная инженерия, Интернет-мошенничество.

См. также: Вишинг, Кардинг.

Формальный (formal) —

Выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях. *[ГОСТ*

Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].

См. также: Неформальный, Полуформальный.

Фрод (fraud) —

Вид мошенничества в области информационных технологий, в частности, несанкционированные действия и неправомочное пользование ресурсами и услугами в сетях связи. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

Выше: Интернет-мошенничество.

См. также: Антифрод системы.

Фрод-мониторинг —

См. Антифрод системы.

Функциональная возможность —

Маркер, используемый в качестве идентификатора какого-либо ресурса, овладение которым дает право на доступ к данному ресурсу. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000].*

См. также: Доступ к информации (ресурсам информационной системы).

Функциональное устройство системы обработки информации —

Функционально законченная часть технических средств системы обработки информации. *[ГОСТ15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992].*

См. также: Система обработки информации, Устройство управления системы обработки информации.

Функциональные возможности безопасности объекта оценки [TOE security functionality] —

Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения объекта оценки, которые необходимо использовать для корректной реализации функциональных требований безопасности. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].*

См. также: Требование безопасности (объекта оценки).

Функциональный объект [functional object] —

Элемент программы, осуществляющий выполнение действий по реализации законченного фрагмента алгоритма программы. В качестве функциональных объектов могут выступать процедуры, функции, ветви, операторы. *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля*

отсутствия недекларированных возможностей» (утв. приказом председателя Гостехкомиссии России от 4 июня 1999 г. N 114)].

См. также: Маршрут выполнения функциональных объектов.

Функция без запретов [interdiction free function] —

Дискретная функция, не имеющая запретов функции. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Дискретный, Функция с запретами.

Функция зашифрования [encryption function] —

Функция зашифрования описывает процесс зашифрования и осуществляет зависящее от ключа отображение последовательностей блоков открытого текста (сообщения) в последовательности блоков шифрованного текста (сообщения). Доопределяется на множество всех открытых текстов (сообщений) и реализуется алгоритмом зашифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция шифрования.

См. также: Свойство перемешивания, Свойство рассеивания, Свойство усложнения, Уравнение зашифрования, Алгоритм зашифрования, Функция расшифрования.

Функция расшифрования [decryption function] —

Функция, описывающая процесс расшифрования и осуществляющая отображение, обратное к функции зашифрования. Доопределяется на множество всех шифрованных текстов (сообщений) и реализуется алгоритмом расшифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция шифрования.

См. также: Уравнение расшифрования, Алгоритм расшифрования, Функция зашифрования.

Функция с запретами [function with interdictions] —

Дискретная функция, для которой существует запрет функции. Выходная последовательность фильтрующего генератора, построенного с помощью функции с запретами, является псевдослучайной последовательностью, в которой отсутствуют некоторые мультиграммы символов, поэтому она может быть отбракована набором статистических тестов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Дискретный, Функция без запретов.

Функция с секретом [trapdoor function] —

Дискретная функция, зависящая от параметра (секрета, описания секрета). Знание параметра позволяет эффективно (с полиномиальной сложностью) вычислять и инвертировать данную функцию. Если параметр неизвестен, то не существует эффективного алгоритма инвертирования функции. Семейство функций с секретом обладает свойствами односторонней функции. Применение функций с секретом предполагает построение соответствующего генератора функций с секретом, т. е. эффективного

алгоритма, порождающего пары (функция, секрет). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Дискретный, Семейство подстановок с секретом.

Функция-сервис аутентификации источника данных [data origin authentication service] —

Функция-сервис безопасности, обеспечивающая возможность проверки того, что полученные данные действительно созданы конкретным источником. Данная функция не обеспечивает защиты от повторного навязывания или модификации данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

См. также: Функция-сервис аутентификации сторон.

Функция-сервис аутентификации сторон [peer entity authentication service] —

Функция-сервис безопасности, обеспечивающая возможность проверки того, что одна из сторон информационного взаимодействия действительно является той, за которую она себя выдает. Применяется с целью защиты от атаки типа имитация и от атаки на протокол с повторной передачей. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

См. также: Функция-сервис аутентификации источника данных, Атака на протокол с повторной передачей.

Функция-сервис безопасности [security services] —

Защитная функция, выполняемая подсистемой безопасности и определяемая ее целевым назначением. В соответствии со стандартом ISO 7498.2 выделено пять классов функций-сервисов безопасности для архитектуры безопасности эталонной модели взаимодействия: аутентификация сторон и аутентификация источника данных, разграничение доступа, конфиденциальность, целостность и невозможность отказа от факта отправления или получения сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Прикладной криптографический протокол.

Ниже: Функция-сервис аутентификации источника данных, Функция-сервис аутентификации сторон, Функция-сервис конфиденциальности данных, Функция-сервис обеспечения невозможности отказа, Функция-сервис обеспечения целостности соединения без восстановления, Функция-сервис обеспечения целостности соединения с восстановлением, Функция-сервис разграничения доступа, Функция-сервис целостности данных.

Функция-сервис конфиденциальности данных [data confidentiality service] —

Функция-сервис безопасности, обеспечивающая невозможность несанкционированного получения доступа к данным или раскрытия данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

Функция-сервис обеспечения невозможности отказа [non-repudiation service] —

Функция-сервис безопасности, обеспечивающая невозможность отказа одной из сторон от факта участия в информационном обмене (полностью или в какой либо его части). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

Ниже: Функция-сервис обеспечения невозможности отказа с доказательством источника, Функция-сервис обеспечения невозможности отказа с доказательством получения.

См. также: Невозможность отказа.

Функция-сервис обеспечения невозможности отказа с доказательством источника [non-repudiation service with proof of origin] —

Функция-сервис безопасности, обеспечивающая невозможность отказа отправителя от факта отправления сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис обеспечения невозможности отказа.

См. также: Невозможность отказа, Функция-сервис обеспечения невозможности отказа с доказательством получения.

Функция-сервис обеспечения невозможности отказа с доказательством получения [non-repudiation service with proof of delivery] —

Функция-сервис безопасности, обеспечивающая невозможность отказа получателя от факта получения сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис обеспечения невозможности отказа.

См. также: Невозможность отказа, Функция-сервис обеспечения невозможности отказа с доказательством источника.

Функция-сервис обеспечения целостности соединения без восстановления [connection integrity service without recovery] —

Функция-сервис безопасности, обеспечивающая возможность проверки того, что все данные, передаваемые при установленном соединении, не подверглись модификации, без восстановления этих данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

См. также: Функция-сервис обеспечения целостности соединения с восстановлением.

Функция-сервис обеспечения целостности соединения с восстановлением [connection integrity service with recovery] —

Функция-сервис безопасности, обеспечивающая возможность проверки того, что все данные, передаваемые при установленном соединении, не подверглись модификации, с восстановлением этих данных. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

См. также: Функция-сервис обеспечения целостности соединения без восстановления.

Функция-сервис разграничения доступа [access control service] —

Функция-сервис безопасности, обеспечивающая невозможность несанкционированного использования ресурсов системы. Данный термин понимается в самом широком смысле. На практике решение о предоставлении доступа основывается на аутентификации сторон. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

Функция-сервис целостности данных [data integrity service] —

Функция-сервис безопасности, обеспечивающая возможность проверки того, что защищаемая информация не подверглась несанкционированной модификации или разрушению. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Функция-сервис безопасности.

Функция сжатия [compression function] —

Функция, отображающая входные данные, состоящие из текущего хеш-значения и очередного блока хешируемого сообщения, в новое хеш-значение. Используется в интерактивных конструкциях хеш-функций, позволяющих хешировать сообщения произвольной длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Функция усложнения [combining function] —

Функция, используемая для увеличения аналитической сложности промежуточных последовательностей, например, в генераторах фильтрующих и генераторах комбинирующих шифрсистем поточных или реализуемая s-блоками в шифрсистемах блочных. Должна обладать, в частности, свойством рассеивания и/или свойством усложнения и/или свойством перемешивания. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Свойство перемешивания, Свойство рассеивания, Свойство усложнения.

Функция шифрования [encryption function] —

Термин, объединяющий понятия функции зашифрования и функции расшифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографическая функция.

Ниже: Функция зашифрования, Функция расшифрования.

Хакер [hacker] —

1. Персона, которая «взламывает» систему информационно-телекоммуникационную путем обхода или отключения мер по обеспечению безопасности. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

2. Квалифицированный взломщик систем, создатель вирусов компьютерных, червей и других программ вредоносных. *[Глоссарий по*

информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009].

3. Высококлассный специалист в области программирования, увлеченный своим делом. [Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]

См. также: Хакер взломщик, Хакер любитель.

Хакер взломщик [hacker] —

Лицо, которое использует свои знания и умения для получения несанкционированного доступа к защищаемым ресурсам. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Хакер, Хакер любитель.

Хакер любитель [hacker] —

Искушенный в технических вопросах компьютерный энтузиаст. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Хакер, Хакер взломщик.

Хеш-значение [hash-code, hash-result, hash-value, hash, imprint, digital fingerprint, message digest] —

Значение хеш-функции для данного аргумента. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Хеш-функция.

Хеш-функция [hash function] —

Функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографический примитив.

Ниже: Односторонняя хеш-функция, Хеш-функция с трудно обнаружимыми вторыми прообразами, Хеш-функция с трудно обнаружимыми коллизиями.

См. также: Криптографическая хеш-функция, Хеш-значение.

Хеш-функция с трудно обнаружимыми вторыми прообразами [second preimage resistant hash function] —

Хеш-функция, для которой задача поиска коллизий второго прообраза является вычислительно трудной. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Хеш-функция.

Хеш-функция с трудно обнаружимыми коллизиями [collision-intractable hash function] —

Хеш-функция, для которой задача поиска коллизий является вычислительно трудной. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Хеш-функция.

См. также: Коллизия.

Целостность [integrity] —

1. Свойство сохранения правильности и полноты активов. *[ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введен в действие: 01.06.2007]*.

2. Состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право. *[Р50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации. Введен в действие: 01.01.2006]*.

3. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения). *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

4. Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью. Необходимым условием соблюдения ц. является защищенность сообщения от преднамеренной или случайной несанкционированной модификации или уничтожения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Безопасность информации (данных), Информационная безопасность, Установление целостности, Конфиденциальность, Доступность, Целостность данных, Целостность информации.

Целостность выделенных полей [selective field integrity] —

Обеспечение возможности проверки того, что выделенные поля передаваемых данных не подверглись несанкционированной модификации или уничтожению. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Избирательная защита поля.

Целостность данных [data integrity] —

Способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Выше: Виды механизмов защиты.

См. также: Целостность, Целостность информации.

Целостность информации —

1. Состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения. *[ГОСТ Р52863-2007 Защита информации.*

Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. Введен в действие: 01.07.2008].

2. Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

3. Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения). *[Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Доступность информации, Конфиденциальность информации, Целостность, Целостность данных.

Целостность информационных активов [information assets integrity] **—**

Свойство информационной безопасности организации банковской системы Российской Федерации сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах. *[Стандарт Банка России СТО БР ИББС-1.0-2010 (Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года № Р-705)]*.

См. также: Доступность информационных активов, Конфиденциальность информационных активов, Информационный актив

Целостность ресурсов информационной системы —

Состояние ресурсов информационной системы, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия. *[Р50.1.056-2005 Техническая защита информации. Основные термины и определения. Введен в действие: 01.06.2006]*.

См. также: Ресурс (информационной системы).

Целостность специального защитного знака —

Неизменность внешнего вида СЗЗ и совокупности характерных признаков, предусмотренных техническими условиями. *[Руководящий документ Гостехкомиссии России «Защита информации. Специальные защитные знаки. Классификация и общие требования» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

Выше: Идентификация специального защитного знака.

См. также: Специальный защитный знак (СЗЗ).

Цель безопасности [security objective] **—**

Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям. *[ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки*

безопасности информационных технологий. Часть 1. Введение и общая модель. Введен в действие: 01.12.2013].

См. также: Доверие, Цель информационной безопасности (организации), Цель защиты информации.

Цель защиты информации [security goal] —

Заранее намеченный результат защиты информации. Примечание. Результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию. *[ГОСТ Р50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008].*

См. также: Замысел защиты информации, Эффективность защиты информации, Цель безопасности.

Цель информационной безопасности (организации) [security objective] —

Заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).

Примечание. Результатом обеспечения ИБ может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009].*

См. также: Цель безопасности, Информационная безопасность организации

Цель применения мер и средств контроля и управления [control objective] —

Формулировка, характеризующая, чего следует достичь в результате реализации мер и средств контроля и управления. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013].*

См. также: Ведомость применимости.

Ценная информация —

Информация, ущерб от нарушения защиты которой (связанный, например, с утечкой промышленных и коммерческих секретов) может превысить 100 тыс. рублей в государственном секторе экономики (но не более 1 млн. рублей); Особо ценная информация - это информация, ущерб от нарушения защиты которой может превысить 1 млн. рублей в государственном секторе экономики. *[Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.).*

См. также: Информация, составляющая коммерческую тайну (секрет производства).

Центр доверия [trusted entity, trusted authority, authority, trusted third party] —

Особый участник криптографического протокола, которому доверяют все остальные его участники, введенный в протокол для усиления его безопасности. Различают следующие виды центра доверия: центр регистрации, центр распределения ключей, центр сертификации, центр установки временных меток, центр нотаризации и т.д. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Центр распределения ключей, Центр регистрации, Центр сертификации (открытых ключей), Центр установки меток (временных)

См. также: Участник (протокола)

Центр обработки данных [data processing center] —

Ресурс, который состоит из персонала, хардвера и софтвера, организованный таким образом, чтобы обеспечивать услуги в виде обработки данных. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Обработка данных.

Центр распределения ключей [key distribution center] —

Центр доверия, распределяющий среди участников (протокола) секретные ключи в симметричных шифрсистемах или асимметричных шифрсистемах. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Центр доверия.

Центр регистрации [registration center] —

Центр доверия, который работает вместе с центром сертификации, выполняя роль местного автономного центра хранения реестра сертификатов ключей. Основные функции центра регистрации — регистрация пользователей в системе и присвоение им уникальных идентификаторов, оптимизация управления реестром сертификатов при большом числе запросов, позволяющая масштабировать систему управления сертификатами для большого числа пользователей на большой территории, одновременно сдвигая процесс подтверждения ближе к пользователям. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Центр доверия.

См. также: Центр сертификации (открытых ключей).

Центр сертификации (открытых ключей) [certification center, certification authority] —

1. Орган, которому доверяет один или более пользователей в вопросе создания и распределения сертификатов открытого ключа.

Примечания.

1. Факультативно орган сертификации может создавать ключи пользователей.

2. Роль органа сертификации в этом процессе заключается в обеспечении уверенности, что лицо, которому выдан уникальный сертификат, на самом деле является тем, кем оно себя заявляет. Обычно это означает, что орган сертификации имеет соглашение с учреждением, предоставляющим ему информацию для подтверждения предъявленной идентификационной информации в отношении лица. Органы сертификации являются важнейшим компонентом в информационной безопасности и электронной коммерции, потому что они гарантируют, что две стороны, обменивающиеся информацией, действительно являются теми, кем они себя заявляют. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

2. Центр доверия, обеспечивающий аутентичность открытых ключей путем придания им сертификатов ключей, заверенных цифровой подписью. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Центр доверия.

См. также: Центр регистрации.

Центр управления безопасностью [Security Operation Center, SOC] —

Централизованное подразделение в организации, имеющее дело с вопросами безопасности на организационном и техническом уровне. Основное назначение — детектирование и реагирование на инциденты информационной безопасности. Основная проблема построения центра управления безопасностью — интеграция всех частей, как правило, реализованных в виде автономных модулей, сохраняющих информацию об инцидентах в различных форматах. Обычно включает следующие функциональные модули, осуществляющие мониторинг: распространения вредоносного кода, серверов Windows, Active Directory, утечек данных (DLP), соответствия стандартам серии PCI (отчетность и оповещение), систем предотвращения вторжений (IPS), устройств топ-менеджеров (VIP мониторинг), привилегированных пользователей и др. В своей работе центр управления безопасностью использует следующие технологии: аудит событий; сбор, фильтрация, классификация и хранение событий; корреляция событий и выявление инцидентов; типизация и приоритизация инцидентов; расследование инцидентов; отчетность на всех уровнях управления инцидентами. Построение центра управления безопасностью позволяет решить целый ряд задач обеспечения информационной безопасности: сократить время обнаружения инцидентов и реакции на них; контролировать выполнение политик и правил по результатам расследования инцидентов; осуществлять централизованный мониторинг состояния; повысить эффективность управления рисками и выявить необходимые меры защиты; повысить уровень стабильности и управляемости компании; реализовать нормативные и международные требования по мониторингу событий ИБ (PCI DSS, СТО БР, ГОСТ Р ИСО/МЭК 27001-2006, ФЗ «О персональных данных») и т. п. Создание центра управления

безопасностью позволяет снизить ущерб от инцидентов ИБ за счет своевременного и эффективного реагирования и сбора доказательной базы. Постоянный анализ событий и инцидентов ИБ, выяснение причин их возникновения позволяют оценить эффективность мер защиты, выявить их недостатки и выработать предложения по их замене или корректировке. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*.

Син.: Центр управления инцидентами информационной безопасности.

См. также: Менеджмент инцидента информационной безопасности, Инцидент информационной безопасности, Система предотвращения утечек, Система предотвращения вторжений.

Центр управления инцидентами информационной безопасности [Information Security Operation Center, ISOC] —

См. Центр управления безопасностью.

Центр установки меток (временных) [timestamping authority] —

Центр доверия или процесс, который связывает документ со временем его создания или последнего изменения для защиты от атак, в которых противник и/или нарушитель изменяет дату в недействительном сертификате ключа на то время, когда он был действителен. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Центр доверия.

См. также: Временная метка.

Централизованная система электронных платежей [on-line e-cash system] —

Система электронных платежей, в которой транзакция платежа выполняется с участием банка-эмитента электронных денег. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Система (протокол) электронных платежей.

См. также: Автономная система электронных платежей, Транзакция (протокол) платежа.

Централизованное управление компонентами межсетевого экрана —

Выполнение с одного рабочего места (рабочей станции, узла) всех функций по сопровождению МЭ (его компонент), только со стороны санкционированного администратора, включая инициализацию, останов, восстановление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Администратор межсетевого экрана, Локальное (местное) управление компонентами межсетевого экрана, Дистанционное управление компонентами межсетевого экрана.

Центральный процессор [central processing unit] —

Процессор, выполняющий в данной вычислительной машине или системе обработки информации основные функции по обработке информации и управлению работой других частей вычислительной машины или системы. *[ГОСТ15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Цикл (раунд) (криптографического протокола) [round, pass (of cryptographic protocol)] —

В криптографических протоколах с двумя участниками — временной интервал, в котором активен только один из участников. Другое название — проход (pass) протокола. Цикл (раунд) завершается формированием и отсылкой сообщения с последующим переходом активного участника в состояние ожидания и передачей активности другому участнику. В протоколах с тремя и более участниками в синхронном случае цикл — период времени между двумя точками синхронизации. К очередной точке синхронизации каждый участник должен отослать все сообщения, которые ему предписано передать другим участникам в текущем цикле. В протоколах интерактивного доказательства циклом (раундом) часто называют комбинацию из трех шагов: заявка, запрос, ответ. В асинхронном случае понятие цикла (раунда) условно. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Шаг (протокола).

Цикл (раунд) шифрования [round] —

Один шаг (из ряда однородных шагов) в итеративном алгоритме шифрования. Реализуется, как правило, с помощью относительно простых преобразований, обладающих определенными/криптографическими свойствами. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Схема Фейстеля (Файштеля), Итеративный алгоритм шифрования, Цикловой (раундовый) ключ.

Цикловой (раундовый) ключ [round key] —

Набор, вычисляемый по секретному ключу итеративного алгоритма шифрования в процессе развертывания ключа. Используется для преобразования блока информации на одном из циклов (раундов) шифрования. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Цикл (раунд) шифрования.

Цифровая информация [digital information] —

Информация, представленная в виде данных, предназначенных для обработки, хранения и обмена в компьютерных системах. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Документированная информация, Компьютерная информация

Цифровая подпись [digital signature] —

1. Дополнительные данные или криптографическое преобразование какого-либо блока данных, позволяющие получателю блока данных убедиться в подлинности отправителя и целостности блока данных и защитить его от

искажения с помощью, например, средств получателя. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Представляет собой строку в некотором алфавите (например, цифровую), зависящую от сообщения или документа и от некоторого секретного ключа, известного только подписывающему субъекту. Предполагается, что цифровая подпись должна быть легко проверяемой без получения доступа к секретному ключу. При возникновении спорной ситуации, связанной с отказом подписывающего от факта цифровой подписи некоторого сообщения либо с попыткой подделки подписи, третья сторона должна иметь возможность разрешить спор. Реализуется системой цифровой подписи. Цифровая подпись позволяет решить следующие три задачи: осуществить аутентификацию источника данных, установить целостность сообщения или электронного документа, обеспечить невозможность отказа от факта подписи конкретного сообщения или документа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Виды механизмов защиты, Криптографический примитив.

Ниже: Групповая цифровая подпись, Многократная цифровая подпись, Одноразовая цифровая подпись, Цифровая подпись, не допускающая отказа, Цифровая подпись с восстановлением сообщения.

Син.: Электронная подпись.

См. также: Подделка цифровой подписи, Система цифровой подписи, Электронный документ.

Цифровая подпись, не допускающая отказа [undeniable digital signature] —

Цифровая подпись, сформированная с использованием конфиденциальной схемы цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Цифровая подпись.

Цифровая подпись с восстановлением сообщения [digital signature with message recovery] —

Цифровая подпись, сформированная с использованием разновидности схемы цифровой подписи, в которой получателю передается только цифровая подпись, а сообщение извлекается из нее алгоритмом проверки цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Цифровая подпись.

Цифровой —

Определение, относящееся к данным, которые состоят из цифр. *[ГОСТ 5971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Аналоговый.

Цифровые деньги [digital money, digiCash, e-cash, e-coin] —

Платежные средства, представляющие собой зашифрованные записи (в т. н. электронном бумажнике), используемые для взаиморасчетов в компьютерной сети и существующие исключительно в электронной форме (электронная наличность (e-cash), электронная монета (e-coin)). Достоверность цифровых денег проверяется с помощью открытого ключа цифровой подписи банка-эмитента. Целью защиты является невозможность подделки и повторной траты цифровых денег, а также обеспечение анонимности покупателя. Создание системы электронных платежей с использованием цифровых денег требует решения таких задач, как: обеспечение конфиденциальности, целостности, аутентификации, невозможности отказа, анонимности и неотслеживаемости. Одной из характеристик, отличающих цифровые деньги от других электронных средств платежа, является возможность совершения полностью анонимных транзакций, в которых отсутствует связь между платежными средствами и личностью их держателя. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Проблема повторной траты электронных денег, Электронный бумажник, Электронные деньги.

Частный стандарт —

См. Закрытый стандарт.

Частота (в области риск-менеджмента) [frequency] —

Количество событий или исходов за определенный период времени. Примечание. Частота может быть применима к прошлым событиям или потенциальным будущим событиям, тогда частоту можно рассматривать как меру возможности/вероятности события *[Russian translation of Risk management – Vocabulary ISO GUIDE 73:2009 by the Russian Risk Management Society (RusRisk)- HSE Moscow. Перевод Russian Risk Management Society (RusRisk, FERMA member) and the High School of Economics (HSE, Moscow)]*.

См. также: Возможность (в области риск-менеджмента), Вероятность (в области риск-менеджмента).

Частотный метод [frequency cryptanalysis] —

Метод криптографического анализа, основанный на изучении частотных характеристик открытого и шифрованного текстов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Метод криптографического анализа (криптоанализа).

Частотный тест [frequency test] —

Критерий проверки качества псевдослучайной последовательности, основанный на вычислении частот появлений знаков в отрезках последовательности и сравнении этих частот с их распределением для идеальной случайной последовательности. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Набор статистических тестов.

Человек посередине [man-in-the-middle)] —

См. Атака «противник в середине».

Черный ящик [black-box] —

Конечный автомат, у которого известны только входной и выходной алфавиты и доступны для наблюдения выходные последовательности при произвольных входных последовательностях. Если дополнительно известна оценка числа состояний автомата, то говорят о относительном черном ящике. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Семейство псевдослучайных функций, Предположение о черном ящике.

Честный участник [honest party] —

Участник криптографического протокола, владеющий всей необходимой информацией, в т. ч., если требуется, секретными ключами, и выполняющий действия в соответствии с протоколом. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Участник (протокола).

Чрезвычайная ситуация —

Обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Примечание - Различают чрезвычайные ситуации по характеру источника (природные, техногенные, биолого-социальные и военные) и по масштабам (локальные, местные, территориальные, региональные, федеральные и трансграничные). *[ГОСТ Р22.0.02-94 Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий. Введен в действие: 01.01.1996]*.

См. также: Непредвиденная ситуация, Чрезвычайная ситуация (в организации), Чрезвычайное событие, Угрозы информационной безопасности в условиях чрезвычайных ситуаций, Объекты обеспечения информационной безопасности в условиях чрезвычайных ситуаций.

Чрезвычайная ситуация (в организации) —

Внезапное, незапланированное катастрофическое событие, которое не позволяет организации выполнять критичные бизнес-процессы в требуемом для бизнеса объеме. *[ГОСТ Р53131-2008 (ИСО/МЭК ТО 24762:2008) Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения. Введен в действие: 01.10.2009]*.

См. также: Чрезвычайная ситуация.

Чрезвычайное событие —

Событие, приводящее к чрезвычайной ситуации. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Чрезвычайная ситуация.

Чувствительная информация [sensitive information] —

Информация с ограниченным доступом. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. Информация ограниченного доступа.

Чувствительность —

Характеристика ресурса, которая определяет его ценность или важность и может учитывать его уязвимость. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

Шаг (протокола) [step (of a protocol), protocol action] —

Конкретное, законченное действие, выполняемое участником (протокола) во время одного цикла (раунда) протокола, например, вычисление значения некоторой функции, проверка правильности сертификата ключа, генерация случайного числа, отправка сообщения, и т.п. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Цикл (раунд) (криптографического протокола).

Шимминг —

Шимминг представляет собой разновидность скимминга. В этом случае в картридер банкомата помещается не крупная накладка, как при традиционном скимминге, а очень компактное электронное устройство (шиммер, shim, shimmer), позволяющее получить информацию о банковской карте. Толщина шиммера — порядка 0,1-0,2 мм. Устанавливается шиммер с помощью карты-носителя вглубь приемной щели за небольшое время. Внешнее определение наличия шиммера крайне затруднено. Защитой от шиммера является только то, что шиммер не перехватывает PIN-код. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Выше: Скимминг.

Шифр [cipher] —

1. Совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей. *[ГОСТ 8147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

2. Семейство обратимых отображений множества последовательностей блоков открытых текстов (сообщений) в множество последовательностей блоков шифрованных текстов (сообщении) и обратно, задаваемых функцией шифрования. Каждое из отображений определяется некоторым параметром, называемым ключом, и описывается некоторым алгоритмом шифрования, реализующим один из режимов шифрования. Математическая модель шифра включает алгоритм зашифрования, алгоритм расшифрования, определение режима шифрования, а также модель множества открытых текстов. В

зависимости от способа представления открытых текстов (сообщений) различают блочные, поточные и другие шифры. Основными требованиями, определяющими качество шифра, являются: стойкость криптографическая, имитостойкость, помехоустойчивость шифра и др. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Помехоустойчивость шифра, Совершенный шифр, Функция шифрования, Алгоритм зашифрования, Алгоритм расшифрования, Режим шифрования.

Шифр гаммирования [keystream cipher] —

Шифр, в котором функция зашифрования осуществляет гаммирование. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Гаммирование.

Шифр перестановки [permutation cipher] —

Шифр, в котором шифрованный текст (сообщение) получается из открытого текста (сообщения) перестановкой блоков открытого текста (сообщения). *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Шифровальные (криптографические) средства (средства криптографической защиты информации) [cryptographic tools] —

1. К шифровальным (криптографическим) средствам (средствам криптографической защиты информации), включая документацию на эти средства, относятся:

а) средства шифрования - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

б) средства имитозащиты - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

в) средства электронной подписи;

г) средства кодирования - средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

д) средства изготовления ключевых документов - аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов

для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

е) ключевые документы - электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

ж) аппаратные шифровальные (криптографические) средства - устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

з) программные шифровальные (криптографические) средства - программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

и) программно-аппаратные шифровальные (криптографические) средства - устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части. *[Постановление Правительства РФ от 16.04.2012 N 313 "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)"]*.

2. Неализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства,

системы и комплексы, предназначенные для защиты информации (в т.ч. и входящие в системы и комплексы защиты информации от НСД), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи";

- аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации. *[Положение о государственном лицензировании деятельности в области защиты информации. (утв. решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ от 27 апреля 1994 г. №10 (с изменениями и дополнениями от 24 июня 1997 г. №60)]*.

Выше: Средство защиты информации.

См. также: Криптографические средства, Криптографическая защита.

Шифрование [encryption, enciphering] —

1. Криптографическое преобразование данных для получения шифротекста.

Примечание. Шифрование может быть необратимым процессом, в связи с чем соответствующий процесс дешифрования невозможно реализовать. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

2. Процесс зашифрования или расшифрования. *[ГОСТ28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введен в действие: 01.07.1990]*.

3. Термин объединяющий термины зашифрование и расшифрование. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Виды механизмов защиты .

Ниже: Аппаратное шифрование, Межконцевое шифрование, Позвенное шифрование, Программное шифрование.

См. также: Дешифрование, Способ шифрования, Зашифрование данных, Расшифрование.

Шифрование в конечной точке [end-point encryption] —

Тенденция, состоящая в создании средств надежного и помехоустойчивого шифрования передаваемых и сохраняемых данных и контроля за работой стационарных и переносных компьютеров, мобильных устройств и подключаемых CD-, DVD-, USB-устройств, и т.п. Является комплексным решением по обеспечению безопасности конфиденциальной информации организации, использующей широкий спектр устройств и

имеющей распределенные информационные ресурсы. Основная цель – обеспечение возможностей надежного шифрования в оконечных устройствах без потери эффективности обработки информации. Предполагает использование технологий полного шифрования локальных дисков, файлов/каталогов, контроля за работой драйверов устройств с целью предотвращения неавторизованного доступа к конфиденциальной информации. Как правило, предполагает реализацию в виде специального аппаратного модуля или набора драйверов с централизованным управлением процессами программного и аппаратного шифрования для различных оконечных устройств с гибким использованием различных алгоритмов шифрования. *[Энциклопедия информационной безопасности WikiSec http://wikisec.ru/]*.

См. также: Помехоустойчивость шифра.

Шифрование сеанса [session encryption] —

Способ реализации сеанса связи между двумя сторонами, при котором все передаваемые в процессе его выполнения сообщения шифруются на специально сгенерированном для данного сеанса сеансовом ключе. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Сеансовый ключ.

Шифрованное сообщение [ciphertext] —

Сообщение, полученное в результате зашифрования открытого сообщения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Криптограмма, Открытое сообщение.

Шифрованный текст (шифртекст) [ciphertext] —

Текст, полученный в результате зашифрования открытого текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Шифрованное сообщение, Открытый текст.

Шифротекст —

Данные, получаемые в результате использования шифрования. Семантическое содержимое полученных в результате шифрования данных недоступно.

Примечание. Шифротекст может сам по себе служить входом в процесс шифрования, в результате чего вырабатывается суперзашифрованный выход. *[ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. Введен в действие: 01.01.2000]*.

См. также: Шифрованный текст (шифртекст).

Шифрсистема [cryptosystem, cipher] —

См. Система шифрования.

Шифрсистема RSA [RSA cryptosystem] —

Асимметричная шифрсистема, реализующая алгоритм шифрования RSA. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Асимметричная система.

См. также: Алгоритм шифрования RSA.

Шифрсистема с открытым ключом [public-key cryptosystem] —

См. Асимметричная система.

Шифрсистема с секретным ключом [private-key cryptosystem] —

См. Симметричная шифрсистема.

Шифртекст [ciphertext] —

Текст, полученный в результате зашифрования открытого текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Шифрованный текст (шифртекст).

Шифрующий модуль поточной шифрсистемы [stream cipher ciphering module] —

Часть поточной шифрсистемы, реализующая под воздействием ключевой (управляющей) последовательности шифрование очередного блока текста. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Поточная шифрсистема.

См. также: Управляющий модуль поточной шифрсистемы.

Шлюз безопасности [security gateway] —

Точка соединения между сетями, между сегментами сетей или между программными приложениями в различных доменах безопасности, предназначенная для защиты сети в соответствии с существующей политикой безопасности. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

См. также: Домен безопасности, Политика сетевой безопасности.

Шпионская программа —

См. Шпионское программное обеспечение.

Шпионское программное обеспечение [spyware] —

Программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Также могут производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя. Например, разработчик ПО может собирать информацию о конфигурациях, настройках, системных ошибках. Изготовители часто вставляют в текст лицензии упоминание о присутствии функций spyware. Однако большинство пользователей по привычке игнорируют полное прочтение документа и просто нажимают кнопку «Согласен». В связи с этим антивирусные и анти-spyware компании используют для обозначения подобных продуктов такие термины, как программы потенциально нежелательные. Шпионское программное обеспечение может также официально устанавливаться владельцем корпоративной или общедоступной системы с целью контроля за работой

пользователей и мониторинга работы системы. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*.

Син.: Шпионская программа .

См. также: Вредоносное программное обеспечение.

Штатные криптографические средства [cryptographic services] —

Криптографические средства, заложенные в функциональные возможности операционных систем. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Криптографические средства.

Штатные средства, предоставляемые средством вычислительной техники или автоматизированной системой —

Совокупность программного, микропрограммного и технического обеспечения средства вычислительной техники или автоматизированной системы. *[Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 30 марта 1992 г.)]*.

См. также: Программное обеспечение, Техническое обеспечение автоматизированной системы, Программное обеспечение автоматизированной системы.

ЭВМ общего назначения [mainframe computer] —

ЭВМ, относящаяся к классу вычислительных машин, занимающих по шкале производительности широкий диапазон и предназначенных для решения широкого класса задач с примерно одинаковой технико-экономической эффективностью.

Примечание. Как правило, ЭВМ общего назначения устанавливаются на вычислительных центрах. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Выше: Семейство ЭВМ.

Эвристический анализатор —

См. Антивирусные базы данных.

Эквивалентные ключи [equivalent keys] —

Ключи, при которых криптосистема реализует одинаковые отображения. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Атака на основе эквивалентных ключей, Метод эквивалентных ключей.

Экзистенциальная подделка цифровой подписи [existential forgery] —

Подделка цифровой подписи, при которой противник и/или нарушитель, не владеющий секретным ключом, получает открытый ключ и создает пару (сообщение, подпись), которая будет принята алгоритмом проверки цифровой подписи. При этом противник никак не контролирует выбор того сообщения, для которого в итоге будет подделана подпись. Вероятно, это сообщение будет бессмысленным. Криптографическая стойкость против экзистенциальной

подделки цифровой подписи — основная тема теоретических исследований схем цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Выше: Подделка цифровой подписи.

См. также: Выборочная подделка цифровой подписи, Универсальная подделка цифровой подписи.

Экономические методы обеспечения информационной безопасности —

Включают:

• разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;

• совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц. *[Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895)]*.

Выше: Общие методы обеспечения информационной безопасности.

Экранирование —

Функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области. В результате экранирования уменьшается уязвимость внутренних объектов, поскольку первоначально сторонний нарушитель должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Экранирование дает также возможность контролировать информационные потоки, направленные во внешнюю область, что способствует поддержанию во внутренней области режима конфиденциальности. Помимо функций разграничения доступа, экраны осуществляют регистрацию информационных обменов. *[Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Председателем Гостехкомиссии России 25 июля 1997 г.)]*.

См. также: Межсетевой экран (сетевой экран).

Экспертиза документа по защите информации —

Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение. Примечание. Экспертиза документа по защите информации может включать в себя научно-техническую, правовую, метрологическую, патентную и

терминологическую экспертизу. [ГОСТ Р50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008].

Экспертная система [expert system] —

Система обработки данных, которая обеспечивает экспертное решение проблем в заданной области применения, строя выводы на основе базы знаний, в которой формализован человеческий опыт.

Примечания 1. Термин «система, основанная на знаниях» иногда используется как синоним термина «экспертная система», но последний подчеркивает экспертный характер знаний.

Примечание 2. Некоторые экспертные системы могут улучшать свои базы знаний и создавать новые правила выводов за счет уже решенных задач. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

Эксплойт [exploit] —

1. Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования (DoS-атака). В зависимости от метода получения доступа к уязвимому обеспечению программному различают:

• удаленный (remote) эксплойт работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе;

• локальный (local) эксплойт запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней. Обычно используется для получения взломщиком прав суперпользователя. Атака эксплойта может быть нацелена на различные компоненты системы вычислительной — серверные приложения, клиентские приложения или модули системы операционной. Для использования серверной уязвимости эксплойту достаточно сформировать и послать серверу запрос, содержащий вредоносный код. Использовать уязвимость клиента немного сложнее — требуется убедить пользователя в необходимости подключения к поддельному серверу (перехода по ссылке в случае если уязвимый клиент является браузером).

Виды эксплойтов:

• эксплойты для операционных систем;
• эксплойты для обеспечения программного прикладного (музыкальные проигрыватели, офисные пакеты и т.д.);

• эксплойты для браузеров (Internet Explorer, Mozilla Firefox, Opera и другие);

• эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB);

• эксплойты для интернет-сайтов (facebook.com, hi5.com, livejournal.com);

• другие эксплойты. Эксплойт может распространяться в виде исходных текстов, исполняемых модулей, или словесного описания использования

уязвимости. Он может быть написан на любом компилируемом или интерпретируемом языке программирования (наиболее частые: C/C++, Perl, PHP, HTML+JavaScript). Эксплойты могут быть классифицированы также по типу используемой ими уязвимости, такой как: переполнение буфера, SQL-инъекция, межсайтовый скриптинг, подделка межсайтовых запросов и т.д. *[Свободная энциклопедия Википедия www.wikipedia.org, русский язык.]*

2. Программа, в которой содержатся данные или исполняемый код, позволяющие использовать одну или несколько уязвимостей в обеспечении программном на локальном или удаленном компьютере с заведомо вредоносной целью. Обычно эксплойты используются злоумышленниками для проникновения на компьютер-жертву с целью последующего внедрения туда вредоносного кода (например, заражение всех посетителей взломанного веб-сайта программой вредоносной). Также эксплойты интенсивно используются программами типа червь сетевой для проникновения на компьютер-жертву без участия пользователя. Широко известны также так называемые программы-Nuker'ы, которые отправляют на локальный или удаленный компьютер специальным образом сформированные запросы, в результате чего система прекращает свою работу. *[Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2013.]*

См. также: Уязвимость, Атака.

Экспозиция [exposure] —

Степень подверженности организации и/или причастных сторон воздействию события. *[ГОСТ Р51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения. Введен в действие: 01.12.2012]*.

Син.: Подверженность риску.

Экстранет [extranet] —

Расширение сети Интранет организации, особенно через инфраструктуру общедоступной сети, делающее возможным совместное использование ресурсов организацией, другими организациями и лицами, с которыми она имеет дело, с предоставлением ограниченного доступа к своей сети Интранет.

Примечание. Например, клиентам организации может предоставляться доступ к некоторым частям ее сети, Интранет посредством создания Экстранет, но клиентов нельзя считать "доверенными" с точки зрения безопасности. *[ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. Введен в действие: 01.01.2012]*.

Электромагнитные наводки —

Токи и напряжения в токопроводящих элементах, электрические заряды или магнитные потоки, вызванные электромагнитным полем. *[ГОСТ Р51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Введен в действие: 30.06.2000]*.

Син.: Наводка (наведенный в токопроводящих линейных элементах технических средств сигнал).

См. также: Побочные электромагнитные излучения и наводки.

Электронная вычислительная машина (ЭВМ) [electronic computer] —

Вычислительная машина, основные функциональные устройства которой выполнены на электронных компонентах. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

См. также: Вычислительная машина, Поколение ЭВМ, Семейство ЭВМ.

Электронная монета [e-coin] —

Название электронных платежных средств, используемых в автономных системах электронных платежей. Такая трактовка термина не является общепринятой. Многие авторы называют электронной монетой любое электронное платежное средство. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Электронные деньги, Цифровые деньги, Автономная система электронных платежей.

Электронная платежная система [electronic payment system] —

Инфраструктура информационно-коммуникационная, а также совокупность норм, правил и процедур, позволяющие в соответствии с установленным порядком взаимодействия, правами и обязанностями участников осуществлять платежи и расчеты участников друг с другом. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Банкомат.

Электронная подпись [electronic signature] —

1. Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. *[Федеральный закон от 06.04.2011 N 63-ФЗ “Об электронной подписи” (с изменениями на 2 июля 2013 года) (редакция, действующая с 01.09.2013). Введен в действие: 08.04.2011]*.

2. Термин, применяемый в международных правовых актах для электронной идентификационной информации, добавляемой в качестве атрибута к электронному документу. Позволяет идентифицировать физических лиц путем сличения их подписей. Охватывает различные технологии, в том числе использующие биометрические характеристики, временные и физические характеристики процесса собственноручной подписи, цифровые подписи, электронные ключи, пластиковые карты и др. Основное назначение: идентификация пользователя (в информационной системе), подтверждение целостности подписываемого документа, а также обеспечение невозможности отказа от факта подписи. В настоящее время всем трем целям удовлетворяет только технология цифровой подписи. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

Ниже: Квалифицированная электронная подпись (усиленная квалифицированная электронная подпись), Неквалифицированная электронная подпись (усиленная неквалифицированная электронная подпись), Простая электронная подпись.

Син.: Цифровая подпись.

См. также: Директива 1999/93/ЕС, Средства электронной подписи, Участники электронного взаимодействия, Электронный документ.

Электронная почта [e-mail] —

Переписка в виде сообщений, передаваемых между пользовательскими терминалами по компьютерной сети. *[ISO/IEC 2382-1:1993. Информационная технология. Словарь. Часть 1. Основные термины и определения]*.

См. также: Адресная книга, Почтовая бомба, Сервис шифрования почтовых сообщений.

Электронная система обмена данными [Electronic Data Interchange (EDI)] —

Автоматизированная технология осуществления сбора, классификации, хранения, поиска, обработки и передачи информации, основанная на едином представлении и структурировании данных. В настоящее время интегрируется с технологиями автоматизации делопроизводства и документооборота. Для защиты электронной системы обмена данными применяются криптографические системы, обеспечивающие конфиденциальность, целостность, аутентификацию и невозможность отказа. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Электронный обмен данными.

Электронная система перевода денежных средств [Electronic Funds Transfer (EFT)] —

Система автоматизации перевода финансовых средств с использованием электронной системы обмена данными. Собирает данные транзакций, сортирует и группирует их в соответствии с банком назначения и передает в общем формате в систему, занимающуюся проведением финансовых расчетов. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Электронная система обмена данными.

Электронное сообщение [electronic message] —

Информация, переданная или полученная пользователем информационно-телекоммуникационной сети. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Электронные деньги [electronic money, e-money] —

Банковские платежные средства, представляющие собой записи (в так называемом электронном кошельке) о наличии реальных денежных средств, которыми обладает некоторое лицо. Реализованы в системах смарт-карт. Защита хранимого значения основывается на невозможности создания фальшивой карты или осуществления операций с использованием чужой карты. Для защиты платежей применяются криптографические системы, обеспечивающие конфиденциальность, целостность, аутентификацию и невозможность отказа. В широком смысле, электронные деньги — форма организации денежного обращения с использованием компьютерных сетей.

[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006].

Выше: Криптографический примитив.

См. также: Электронная монета, Цифровые деньги.

Электронный бумажник [e-wallet, wallet] —

Специальное электронное устройство, предназначенное для решения проблемы повторной траты денег электронных. Электронный бумажник, выдаваемый клиенту банка, состоит из компьютера, которому доверяет клиент, и защищенного модуля, называемого наблюдателем, которому доверяет банк. Наблюдатель имеет возможность общаться с «внешним миром» только через компьютер клиента. Клиент не может потратить цифровые деньги без санкции наблюдателя; тем самым предотвращается повторная трата электронных денег. Криптографические протоколы автономной системы электронных платежей с электронным бумажником обеспечивают неотслеживаемость действий клиентов, даже если и банк, и наблюдатель нечестные, и информация, накопленная банком, сопоставляется с содержимым наблюдателя. *[Погорелов Б.А., Сачков В.Н. Словарь криптографических терминов. М.:МЦНМО, 2006]*.

См. также: Проблема повторной траты электронных денег, Автономная система электронных платежей, Цифровые деньги.

Электронный документ [electronic message] —

Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. *[Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями на 28 декабря 2013 года) (редакция, действующая с 1 февраля 2014 года). Введен в действие: 09.08.2006]*.

Выше: Документ.

См. также: Временная метка, Электронный обмен данными.

Электронный обмен данными [electronic data interchange] —

Передача данных между компьютерами в стандартном формате. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

См. также: Электронная система обмена данными, Электронный документ.

Электронный паспорт [electronic passport] —

Паспорт, содержащий в дополнение к традиционным паспортным данным чип, на котором записана биометрия владеющего им лица с использованием криптографии для обеспечения защиты данных. *[Глоссарий по информационному обществу / Под общ. ред. Ю.Е. Хохлова. М.: Институт развития информационного общества, 2009]*.

Элемент [element] —

Неделимое требование безопасности. *[Руководящий документ "Безопасность информационных технологий. Критерии оценки безопасности информационных технологий." (Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. № 187)]*.

См. также: Требование безопасности (объекта оценки).

Эмуляция [emulation] —

Имитация функционирования одного устройства посредством другого устройства или устройств вычислительной машины, при которой имитирующее устройство воспринимает те же данные, выполняет ту же программу и достигает того же результата, что и имитируемое. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Эффективность [efficiency] —

1. Связь между достигнутым результатом и тем, насколько целесообразно использованы ресурсы. *[ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Введен в действие: 01.01.2013]*.

2. Свойство объекта удовлетворять требованиям к услуге с заданными количественными характеристиками. *[ОСТ 45.127-99 Система обеспечения информационной безопасности взаимоувязанной сети связи Российской Федерации. Термины и определения. Введен в действие: 01.01.2000]*.

Эффективность защиты информации —

Степень соответствия результатов защиты информации цели защиты информации. *[ГОСТ Р50922-2006 Защита информации. Основные термины и определения. Введен в действие: 01.02.2008]*.

См. также: Защищенность информации, Цель защиты информации, Показатель эффективности защиты информации, Эффективность обеспечения информационной безопасности.

Эффективность обеспечения информационной безопасности —

Связь между достигнутым результатом и использованными ресурсами для обеспечения заданного уровня информационной безопасности. *[ГОСТ Р53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Введен в действие: 01.10.2009]*.

См. также: Эффективность защиты информации.

Ядро защиты [security kernel] —

См. Диспетчер доступа.

Ячейка памяти [storage location] —

Минимальная адресуемая область памяти данных. *[ГОСТ 15971-90 Системы обработки информации. Термины и определения. Введен в действие: 01.01.1992]*.

Учебное издание

Новоструев Андрей Викторович, Солодовников Вячеслав Михайлович,
Терентьева Анна Александровна

ТЕЗАУРУС В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Редактор

Подписано к печати	Формат 60×84 1/16	Бумага тип. №1
Печать трафаретная	Усл. печ.л.	Уч.-изд.л.1
Заказ	Тираж	Цена свободная

РИЦ Курганского государственного университета
640669, г. Курган, ул. Гоголя,25
Курганский государственный университет