МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУРГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра «Безопасность информационных и автоматизированных систем»

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические рекомендации
к выполнению практических работ
по дисциплине «Основы информационной безопасности»
для студентов очной формы обучения
10.05.03 «Информационная безопасность автоматизированных систем»,
09.03.03 «Прикладная информатика»,
09.03.04 «Программная инженерия»

Курган 2026

Кафедра: «Безопасность информационных и автоматизированных систем»

Дисциплины: «Основы информационной безопасности» 10.05.03 «Информационная безопасность автоматизированных систем»; «Основы информационной безопасности» 09.03.03 «Прикладная информатика»; «Основы информационной безопасности» 09.03.04 «Программная инженерия»

Составил: канд. биол. наук, доцент А. В. Человечкова

Печатается в соответствии с планом издания, утвержденным методическим советом университета 13 декабря 2024 г.

Утверждены на заседании кафедры 16 декабря 2025 г.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1

Тема. Изучение основных понятий и определений информационной безопасности.

Цель работы. Ознакомиться с основными понятиями и определениями информационной безопасности.

Теоретическое введение

Под ***информационной безопасностью*** понимают состояние защищенности обрабатываемых, хранимых и передаваемых данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности (Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ (ст. 2, п. 13)).

Природа этих воздействий может быть самой разнообразной. Это и попытки проникновения злоумышленников, и ошибки персонала, и выход из строя аппаратных и программных средств, стихийные бедствия (землетрясение, ураган, пожар и т. п.). Существуют и угрозы безопасности в корпоративных компьютерных сетях.

Информационная безопасность компьютерных систем и сетей достигается принятием комплекса мер по обеспечению конфиденциальности, целостности, достоверности, юридической значимости информации, оперативности доступа к ней, а также по обеспечению целостности и доступности информационных ресурсов и компонентов системы или сети.

Конфиденциальность – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право. Под конфиденциальностью понимается более широкий спектр значений, чем правовая защита определенных массивов информации или режим коммерческой тайны. Общей концепцией становится предоставление уровня доступа исходя из принципа минимальной информированности по вопросам, не входящим в сферу их непосредственной компетенции. Никто не должен иметь возможность изучать данные, которые не были ему необходимы в силу служебных обязанностей. Исходя из этого принципа, устанавливаются основные правила аутентификации, определяются уровни доступа, разрабатываются положения о сведениях, имеющих характер защищенных. Это свойство информации проявляется в политиках безопасности программных продуктов, во внутренних документах компаний и в нормативных документах государственных регуляторов. Сведения, принадлежащие организации или государству, имеют ценность и могут использоваться при принятии достоверных и обоснованных решений только при сохранении такого основного свойства информации, как целостность.

Информация должна быть защищена:

а) от намеренного, случайного искажения или удаления;

б) от случайного искажения, которое может произойти во время обработки или передачи данных.

Целостность информации может пострадать от намеренного ручного вмешательства, а также от вирусов и других вредоносных программ, например, логических бомб; ошибок в программном коде, которые приводят к утрате или искажению данных; ошибок, связанных с недостаточной подготовкой персонала или иными причинами; технических сбоев.

Достоверность информации – свойство информации быть правильно воспринятой. В общем случае достоверность информации достигается указанием времени свершения событий, сведения о которых передаются сопоставлением данных, полученных из различных источников своевременным вскрытием дезинформации, исключением искаженной информации и др.

Задания:

1 Ознакомиться с сайтами ГАРАНТ (http://www.garant.ru/) и Консультант Плюс (http://www.consultant.ru/).

2 Составить список основных действующих нормативных актов в сфере информационной безопасности. Например, Закон Российской Федерации от 21 июля 1993 года №5485-1 «О государственной тайне»; Закон РФ «Об информации, информатизации и защите информации» от 20 февраля 1995 года №24-ФЗ. Полученные данные внести в таблицу 1.

Таблица 1 – Результаты выполнения задания

Наименование	Дата принятия	Дата вступления в силу	Последняя редакция

3 Используя данные сайты и действующие нормативные акты Российской Федерации, составить словарь основных определений в сфере информационной безопасности. Словарь должен включать в себя не менее 40 понятий, а также ссылки на использованные нормативные акты.

4 Ответить на контрольные вопросы:

1 Что является источником информации?

2 Назовите принципы правового регулирования в сфере информации.

3 Можно ли ограничить свободный доступ к информации? Как?

4 Что подразумевается под конфиденциальностью?

5 От чего может пострадать целостность информации?

6 Что такое достоверность информации?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2

Тема. Изучение сравнительных характеристик систем баз данных с правовой информацией «Консультант Плюс», «Гарант» и определение лучшей из них.

Цель работы. Получить сравнительные характеристики систем баз данных с правовой информацией «Консультант Плюс», «Гарант» и определить лучшую из них.

Теоретическое введение

Персональные компьютеры, системы управления и сети на их основе быстро входят во все области человеческой деятельности (например, военная, коммерческая, банковская, научные исследования и т. д.). Широко используя компьютеры и сети на их основе для обработки, хранения и передачи информации, необходимо ее надежно защищать от возможности доступа к ней посторонних лиц, ее утраты или искажения. Согласно статистическим данным более 80 % компаний несут финансовые убытки из-за нарушения целостности и конфиденциальности используемых данных.

Кроме информации, составляющей государственную или коммерческую тайну, существует информация, представляющая собой интеллектуальную собственность. К такой информации можно отнести результаты научных исследований, программы, обеспечивающие функционирование компьютера, игровые программы, аудио и видеоклипы. Стоимость такой информации в мире составляет несколько триллионов долларов в год. Ее несанкционированное копирование снижает доходы компаний и авторов, занятых в ее разработке.

Усложнение методов и средств организации машинной обработки, повсеместное использование глобальной сети Интернет приводит к тому, что информация становится все более уязвимой. Этому способствуют такие факторы, как постоянно возрастающие объемы обрабатываемых данных, накопление и хранение данных в ограниченных местах, постоянное расширение круга пользователей, имеющих доступ к ресурсам, программам и данным, недостаточный уровень защиты аппаратных и программных средств компьютеров и коммуникационных систем и т. д.

Учитывая все эти факторы, защита информации в процессе ее сбора, хранения и передачи приобретает исключительно важное значение.

Правовые базы данных систем «Консультант Плюс» и «ГАРАНТ» – это базы данных полных текстов различных правовых документов законодательства Российской Федерации в электронных форматах. Системы реализуют права граждан на доступ к социально значимой информации. Базы данных документов включают кодексы, законы, указы, постановления Правительства

РФ, нормативные акты, комментарии, правоприменительные акты, правовые акты распорядительного и локального действия, утратившие силу документы, международные правовые акты. Документы представлены в виде полных текстов в последней редакции, а также как специализированные правовые блоки по всем разделам федерального законодательства. Имеются удобные средства поиска информации. Производится еженедельное обновление.

Одной из важных характеристик, с которой сталкивается пользователь при работе с сайтами, базами данных, различными таблицами — это релевантность запроса.

Релевантность запроса – степень удовлетворения пользователя показанными в ответ на его запрос поисковыми результатами. В идеале страница выдачи должна полностью удовлетворять информационную потребность пользователя в независимости от ее полноты и точности.

Задания:

1 Повторить принципы работы с сайтами ГАРАНТ (http://www.garant.ru/) и Консультант Плюс (http://www.consultant.ru/). Выбрать функцию «Расширенный поиск» в системе «Гарант» (http://ivo.garant.ru/#/startpage:0) и карточку поиска в системе «Консультант Плюс»(http://www.consultant.ru/cons/cgi/online.cgi?req=card&rnd=qWky3g&ts=iSxcDdTA6cCfGGQ2#div).

2 Выполнить запрос на информацию из правовых баз данных. Запрос должен включать в себя одно или несколько ключевых слов и относиться к теме, отражающей информационную безопасность. Примеры запросов: «информационная безопасность», «тайна», «доступность» и т. п. Для вариантов запросов можно использовать глоссарий, составленный на практическом занятии № 1.

3 С помощью полученных списков результатов заполнить таблицу 2.

Таблица 2 – Результаты выполнения задания

Показатель	**«Консультант Плюс»**	**«ГАРАНТ»**
Общее количество найденных документов		
Место (общее количество – т. е. у какой системы общее количество документов больше)		
Количество найденных документов, изданных за последние 5 лет		
Место (количество за последние 5 лет)		
Количество найденных документов, действующих на текущую дату		
Место (действующие документы)		
Коэффициент точности поиска (P)		
Место (P)		
Сумма мест (R)		

Коэффициент точности поиска вычисляется по следующей формуле:

$$P = \frac{a}{a+b},$$

где a – число релевантных документов, выданных поисковой системой в ответ на запрос из числа первых 10 документов,

b – число нерелевантных документов, выданных поисковой системой в ответ на запрос из числа первых 10 документов.

Итоговая сумма мест считается по среднему арифметическому из всех полученных мест.

4 Определить лучшую систему правовых баз данных и сделать выводы.

5 Ответить на контрольные вопросы:

1 Что такое релевантность запроса.

2 Почему для пользователя важна релевантность запроса.

3 Почему правовые базы на одинаковый запрос выдают разные результаты.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3

Тема. Знакомство с правовой базой «Кодекс» в области защиты информации.

Цель работы. Ознакомиться с правовой базой в области защиты информации. Изучить основные ГОСТы в области информационной безопасности.

Теоретическое введение

Информация определяется как сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Объектом правового регулирования могут быть конкретные формы существования информации:

– документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

– информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

– информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

– правовая защита информации – законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Интерес к вопросам защиты информации повышается, что связано с возрастанием роли информационных ресурсов в конкурентной борьбе, расширением использования сетей, а следовательно, и несанкционированного доступа к хранимой и передаваемой информации. Правовая защита информации как ресурса признана на международном, государственном уровне и регулируется соответствующими законодательными и правовыми нормами государств и внутренними регламентами организаций разработчиков/пользователей. Структура правовой защиты показана на рисунке 1.

Рисунок 1 – Структура правовой защиты

Множество информационных объектов информационного права подразделяется на две категории – общедоступные и с ограниченным доступом. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не может быть ограничен в соответствии с действующим законодательством (например, информация о состоянии окружающей среды, деятельности государственных органов и т. п.). В свою оче-

редь, информация с ограниченным доступом считается конфиденциальной, включая государственную, служебную, профессиональную (банковская, нотариальная и т. п.), коммерческую тайны, персональные данные и другие виды тайн.

Информация из любой области знаний и деятельности в принципе является открытой и общедоступной, если законодательством не предусмотрено ограничение доступа к ней в установленном порядке. Законами РФ определены режимы доступа к информационным ресурсам и порядок их использования (рисунок 2).

Рисунок 2 – Правовые режимы доступа к информации

Правовое обеспечение функционирования информационных систем – совокупность правовых норм, определяющих создание, юридический статус и функционирование информационных систем, регламентирующих порядок получения, преобразования и использования информации. Главной целью правового обеспечения функционирования информационных систем, в том числе и корпоративных, является укрепление законности использования информационных ресурсов, обеспечение информационной безопасности отдельных граждан, предприятий, организаций и в целом национальной безопасности страны. Регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Правовое обеспечение функционирования информационных систем в Российской Федерации осуществляется путем законодательной поддержки на государственном уровне (законодательный уровень) и на уровне договорных отношений разработчика и заказчика в рамках заключаемых договоров на разработку и создание информационных систем (локальный уровень). Исходя из чего, в правовом обеспечении функционирования информационных систем в РФ можно выделить:

1) общую часть, регулирующую функционирование любой информационной системы (законодательный уровень);

2) локальную часть, регулирующую функционирование конкретной системы при разработке информационных систем (локальный уровень) – договорной уровень;

3) внутренние нормативные акты организации (стандарты и регламенты разработчика/пользователя ИС).

В состав правового обеспечения законодательного уровня входят: Конституция РФ, законы, указы, постановления государственных органов власти, приказы, инструкции и другие нормативные документы министерств, ведомств, организаций, местных органов власти.

Правовое обеспечение этапов разработки информационной системы (локальный уровень) включает нормативные акты, связанные с договорными отношениями разработчика и заказчика ИС и правовым регулированием отклонений от договора; внутренние стандарты, а также регламенты информационной безопасности организации. Регулирование вопросов правового обеспечения этапов разработки и функционирования информационной системы (локальный уровень) включает в том числе:

- статус информационной системы;
- права, обязанности и ответственность персонала;
- правовые положения отдельных видов процесса управления;
- порядок создания и использования информации и другие.

На отношения в информационной сфере локального уровня распространяются нормы административного, гражданского, уголовного, трудового законодательства РФ.

Необходимой составляющей государственной системы обеспечения информационной безопасности являются: национальные стандарты Российской Федерации (утверждаются приказами Росстандарта), руководящие,

нормативно-технические и методические документы по безопасности информации. Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации – ГОСТ Р 1.0-2012 «Стандартизация в Российской Федерации. Основные положения» (взамен ГОСТ Р 1.0-2004).

Задания:

1 Ознакомиться с сайтом «Кодекс» (http://docs.cntd.ru/).

2 Используя правовую базу «Кодекс», заполнить таблицу 3.

Таблица 3 – Нормы, связанные с информацией

Номер статьи Конституции РФ	Содержание статьи Конституции РФ

3 Используя правовую базу «Кодекс», заполнить таблицу 4.

Таблица 4 – Законодательство РФ в информационной сфере

Область правового регулирования	Основные законодательные акты
Основы информационной безопасности	
Обеспечение электронного документооборота	
Правовые режимы доступа к информации, различные виды тайн	
Производство и использование систем защиты информации	
Защита авторских и имущественных прав разработчиков информационных систем	

4 Используя правовую базу «Кодекс», заполнить таблицу 5.

Таблица 5 – ФЗ «Об информации, информационных технологиях и защите информации» № 149-ФЗ

Объекты регулирования	Принципы правового регулирования	Ответственность за правонарушения

5 Используя правовую базу «Кодекс», заполнить таблицу 6.

Таблица 6 – Перечень сведений конфиденциального характера Указ Президента РФ от 06.03.1997 № 188

Вид конфиденциальной информации	Определение (содержание)

6 Ответить на контрольные вопросы:

1 Для чего нужны стандарты в сфере информационной безопасности?

2 Почему обновление стандартов происходит на постоянной основе?

3 Что может повлечь несвоевременное ознакомление со стандартами?

4 Какие основные принципы обеспечения безопасности определены в Федеральном законе «О безопасности»?

5 Какие основные информационные угрозы выделены в Доктрине информационной безопасности Российской Федерации?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4

Тема. Изучение классифицирования угроз и атак на информационную систему.

Цель работы. Научиться классифицировать угрозы и атаки на информационную систему. Ознакомиться с методикой расчета угроз.

Теоретическое введение

Под угрозой будем понимать потенциально возможные воздействия на систему, которые прямо или косвенно могут нанести урон пользователю. Непосредственную реализацию угрозы называют атакой. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Имеет смысл различать неумышленные и умышленные угрозы.

Неумышленные угрозы связаны с:

– ошибками оборудования или программного обеспечения: сбои процессора, питания, нечитаемые дискеты, ошибки в коммуникациях, ошибки в программах;

– ошибками человека: некорректный ввод, неправильная монтировка дисков, запуск неправильных программ, потеря дисков, пересылка данных по неверному адресу;

– форс-мажорными обстоятельствами.

Умышленные угрозы, в отличие от случайных, преследуют цель нанесения ущерба пользователям информационных систем и, в свою очередь, подразделяются на активные и пассивные. Пассивная угроза – несанкционированный доступ к информации без изменения состояния системы, активная – связана с попытками перехвата и изменения информации.

Не существует общепринятой классификации угроз безопасности. Один из вариантов классификации может быть выполнен по следующим признакам:

– по цели реализации;

– по принципу воздействия на систему;

– по характеру воздействия на систему;

– по причине появления используемой ошибки защиты;

– по способу воздействия атаки на объект;

– по объекту атаки;

– по используемым средствам атаки;

– по состоянию объекта атаки.

Рассмотрим некоторые из угроз безопасности.

Несанкционированный доступ (НСД) – наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к ресурсу, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности. **Отказ в обслуживании** представляет собой преднамеренную блокировку легального доступа к информации и другим ресурсам. **Незаконное использование привилегий** применяется злоумышленниками, использующими штатное программное обеспечение, функционирующее в нештатном режиме. Незаконный захват привилегий возможен либо при наличии ошибок в самой системе, либо в случае халатности при управлении системой. Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволяет избежать таких нарушений. **«Скрытые каналы»** представляют собой пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. «Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»). Под **«Маскарадом»** понимается выполнение каких-либо действий одним пользователем от имени другого пользователя. Такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий. Процесс **«Сборки мусора»** также может привести к утечке важной информации. После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти ПК. Данные хранятся на носителе до перезаписи или уничтожения. После выполнении указанных действий на освободившемся пространстве диска находятся остаточные данные, которые возможно прочитать с помощью специальных программ и оборудования. **«Люки»** представляют собой скрытую, недокументированную точку входа в программный модуль. «Люки» относятся к категории угроз, возникающих вследствие ошибок реализации какого-либо проекта (системы в целом, комплекса программ и т. д.). Поэтому в большинстве случаев обнаружение «люков» – результат случайного

поиска. **Вредоносные программы** – специально созданные программы воздействия на вычислительные системы. Эти программы прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

Перечисленные атаки зачастую используются совместно для реализации комплексных атак. Так, например, вредоносная программа может использоваться для сбора информации о пользователях на удаленном компьютере и пересылки ее злоумышленнику, после чего последний может осуществить атаку методом «маскарада».

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности информации информационной системы и ее проектирования. В модели угроз дается обобщенное описание информационных систем как объектов защиты, возможных источников угрозы безопасности персональных данных, основных классов уязвимостей информационной системы, возможных видов деструктивных воздействий на ПД, а также основных способов их реализации.

Задания:

1 Определение объекта для разработки модели угроз.

Придумать предприятие, которое будет состоять из нескольких филиалов, расположенных в разных частях города. Оценить необходимое количество компьютеров для данного предприятия и филиалов. Придумать охранную систему. Проработать способы обмена информационными ресурсами между филиалами и головным предприятием.

2 Определение вероятности реализации угрозы для созданного предприятия из задания 1.

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности данных в складывающихся условиях обстановки. Для оценки вероятности возникновения угрозы используется числовой коэффициент – Y_2, который имеет четыре вербальных градации.

1) $Y_2 = 0$ характеризует отсутствие объективных предпосылок для осуществления угрозы. Реализация угрозы считается маловероятной.

2) $Y_2 = 2$ характеризует низкую вероятность реализации угрозы. Считается, что объективные предпосылки для реализации угрозы существуют, но принятые меры существенно ее затрудняют.

3) $Y_2 = 5$ – средняя вероятность реализации угрозы. Объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны.

4) $Y_2 = 10$ характеризует высокую вероятность реализации угрозы. Считается, что объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

Определение вероятности реализации угроз безопасности данных проводится для всех выявленных угроз. Угрозы берутся в типовом перечне методики расчета вероятности реализации угроз и дополняются угрозами, которые возможны только в данной организации. Значение коэффициента Y_2 определяется пользователем.

Выделим наиболее часто встречающиеся и общие угрозы.

1 Угрозы утечки акустической (речевой) информации.

Данный вид связан в возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя, при обработке данных, возможно при наличии функций голосового ввода данных или функций воспроизведения данных акустическими средствами.

2 Угрозы утечки видовой информации.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптико-электронных средств с экранов дисплеев и других средств отображения и обработки графической, видео- и буквенно-цифровой информации.

3 Кража компьютеров.

Угроза осуществляется путем несанкционированного доступа внешними и внутренними нарушителями в помещения, где расположены элементы информационной системы.

4 Кража носителей информации.

Угроза осуществляется путем несанкционированного доступа внешними и внутренними нарушителями к носителям информации и их последующей кражи.

5 Действия вредоносных программ (вирусов).

Преднамеренная и непреднамеренная установка вредоносного ПО, которое способствуют утечке или искажению информации.

6 Установка ПО, не связанного с исполнением служебных обязанностей.

Угроза осуществляется путем несанкционированной установки ПО внутренним нарушителям, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПД или ее элементов.

7 Непреднамеренная модификация (уничтожение) информации сотрудниками.

Угроза осуществляется за счет влияния человеческого фактора пользователей системы, которые нарушают положения принятых правил работы с системой или не осведомлены о них.

8 Сбой системы электроснабжения.

Угроза вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

9 Стихийное бедствие.

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

10 Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке.

Угроза осуществляется путем несанкционированного доступа внешних нарушителей в помещения, где расположены элементы системы и средства защиты, а также происходит работа пользователей.

11 Разглашение информации, модификация, уничтожение лицами, допущенными к ее обработке.

Угроза осуществляется за счет влияния человеческого фактора пользователей системы, которые нарушают положения о неразглашении информации или не осведомлены о них.

3 Оценить реальную возможность реализуемости данных угроз.

По итогам оценки уровня исходной защищённости (Y_1), который для данного предприятия примем средним ($Y_1=5$), и вероятности реализации угрозы (Y_2), который определяется вербальным значением: 0, 2, 5 или 10, рассчитывается коэффициент реализуемости угрозы (Y). Коэффициент реализуемости угрозы Y будет определяться соотношением $Y=(Y_1+Y_2) / 20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

если $0 \leq Y \leq 0,3$, то возможность реализации угрозы признаётся низкой;

если $0,3 < Y \leq 0,6$, то возможность реализации угрозы признаётся средней;

если $0,6 < Y \leq 0,8$, то возможность реализации угрозы признаётся высокой;

если $Y > 0,8$ то возможность реализации угрозы признаётся очень высокой.

По результатам оценки заполняется таблица 7, которую необходимо дополнить своими примерами угроз. Дополнительных примеров должно быть не менее пяти.

Таблица 7 – Оценка угроз организации

Тип угроз безопасности	Вербальная градация	Y	Вербальная интерпретация
Угрозы утечки информации по каналам ПЭМИН	*Y_2=0*	*Y = (5 + 0)/20 = 0,25*	*Низкая*
Угрозы утечки акустической (речевой) информации			
Угрозы утечки видовой информации			
Кража компьютеров			
Кража носителей информации			
Действия вредоносных программ (вирусов)			
Установка ПО, не связанного с исполнением служебных обязанностей			
Непреднамеренная модификация (уничтожение) информации сотрудниками			
Сбой системы электроснабжения			
Стихийное бедствие			
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке			
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке			

4 Проанализировать таблицу. Сделать выводы о возможности реализации рассмотренных угроз для предприятия. Предложить мероприятия по уменьшению воздействия угроз на информационные ресурсы.

5 Ответить на контрольные вопросы:

1 Для чего необходимо рассчитывать вероятность угроз атаки на информационную систему?

2 Возможно ли подготовиться ко всем угрозам?

3 Какие основные каналы утечки информации?

4 В чем разница между вирусом и червем?

5 Назовите основные компьютерные вирусы.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5

Тема. Настройка параметров безопасности ОС Windows.

Цель работы. Ознакомление с механизмами аутентификации и идентификации, локальными политиками безопасности.

Теоретическое введение

При подключении пользователей к системам безопасности операционных систем должен реализовываться механизм аутентификации или идентификации. Идентификация и аутентификация применяются для ограничения доступа случайных или незаконных субъектов к информационной системе, объектам – ресурсам (аппаратным, программным, информационным).

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации в ОС Windows XP выполняется в рамках политики безопасности.

Вкладка «Локальная политика безопасности» используется для изменения политики учетных записей и локальных политик безопасности на компьютере. При помощи данной вкладки можно определить:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на компьютере;
- включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задания:

1 Настроить параметры локальной политики безопасности на примере операционной системы Windows XP (итоговый отчет должен содержать скриншоты выполнения этапов заданий).

а) выберите кнопку «Пуск» на панели задач.

б) откройте меню «Настроить – Панель управления».

в) в открывшемся окне выберите ярлык «Администрирование – Локальная политика безопасности» (рисунок 3).

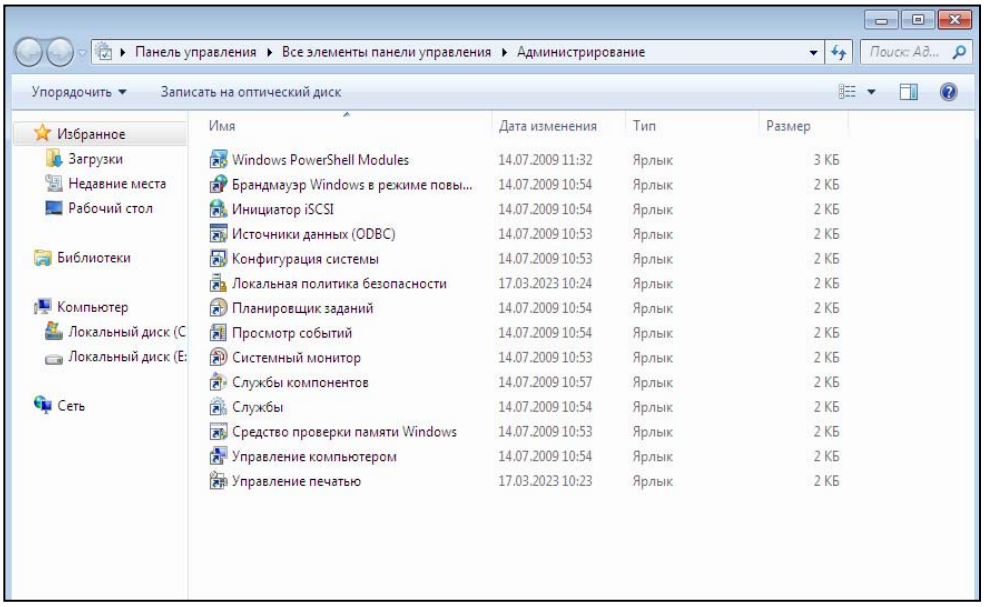


Рисунок 3 – «Администрирование – Локальная политика безопасности»

г) выберите пункт «Политика учетных записей» (включает два подпункта: «Политика паролей» и «Политика блокировки учетной записи») (рисунок 4).

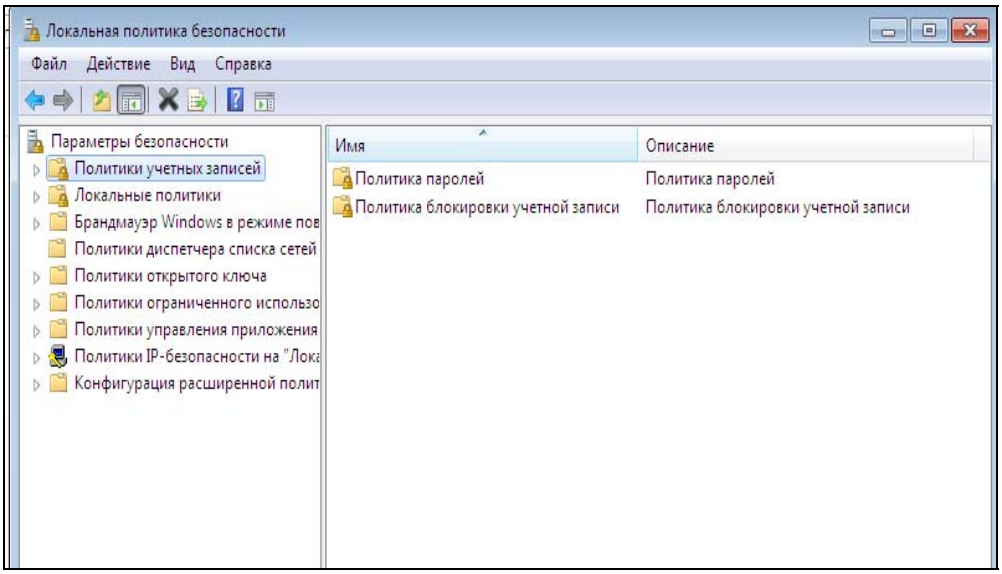


Рисунок 4 – «Политика паролей» и «Политика блокировки учетной записи»

д) откройте подпункт «Политика паролей». В правом окне появится список настраиваемых параметров (рисунок 5).

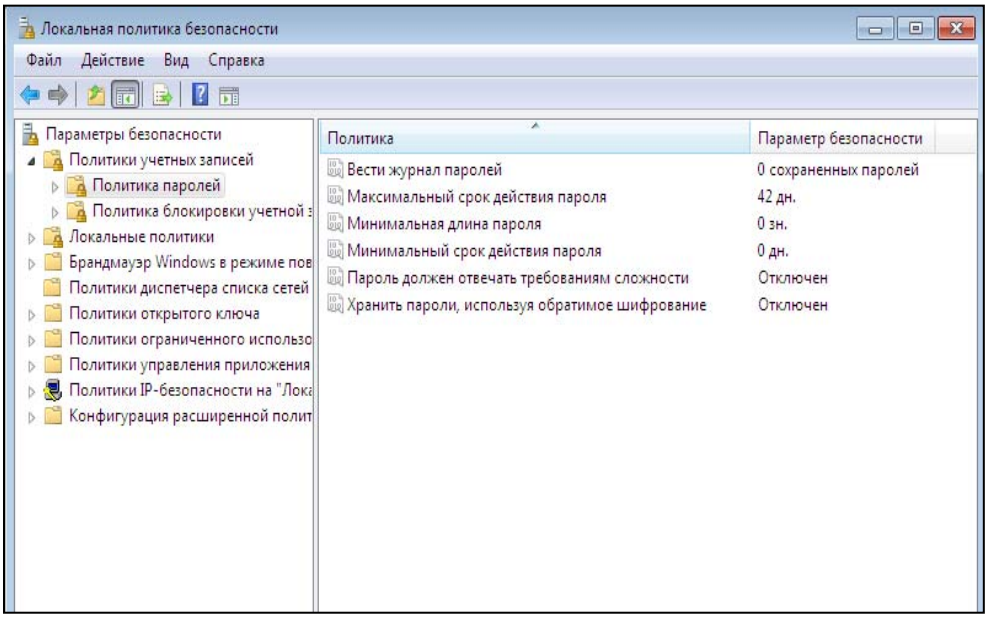


Рисунок 5 – Список настраиваемых параметров

2 Ознакомиться со свойствами параметров подпункта «Политика паролей». Данная вкладка может содержать параметры, представленные в таблице 8. В исходном состоянии системы безопасности после установки операционной системы, ни один из параметров, как правило, не настроен.

Таблица 8 – Параметры вкладки «Политика паролей»

Параметр	Значение
Требовать повторяемости паролей	Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать пароль старый пароль. Это значение должно принадлежать диапазону от 0 до 24.
Максимальный срок действия пароля	Определяет период времени, в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно дать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.
Минимальный срок действия пароля	Определяет период времени, в течении которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0.

Продолжение таблицы 8

Минимальная длина пароля	Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0.
Пароль должен отвечать требованиям сложности	Определяет, должны ли отвечать пароли требованиям сложности. Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям: пароль не может содержать имя учетной записи пользователя или какую-либо его часть; пароль должен состоять не менее чем из 6 символов; в пароле должны присутствовать символы трех категорий из числа других. 1 Прописные буквы английского алфавита от A до Z. 2 Строчные буквы английского алфавита от A до Z. 3 Символы, которые не принадлежат алфавитно-цифровому набору (!, $, #, %). Проверка этих требований выполняется при изменении или создании паролей.
Хранить пароли всех пользователей в домене, используя обратимое шифрование	Определяет, стоит ли в системах Windows 2000, Windows XP хранить пароли, используя обратимое шифрование. Данная политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Политику следует использовать только в исключительных случаях, если потребности приложения важнее, чем защита пароля.

3 Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды на изменяемом параметре). В результате этого действия появится окно (рисунок 6).

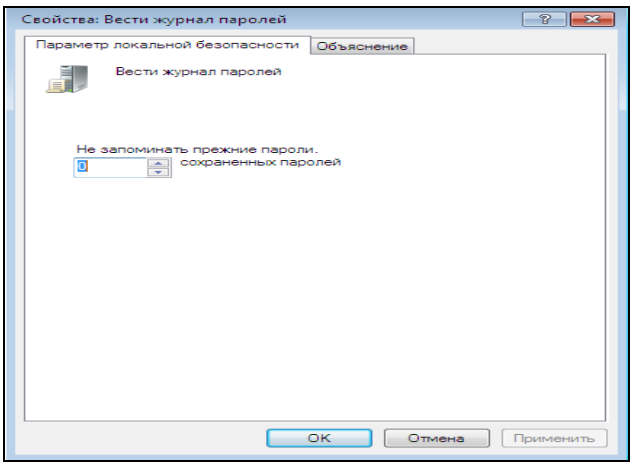


Рисунок 6 – Окно изменения параметров

4 Измените значение параметра и нажмите ОК.

5 Выберите параметр «Требовать неповторяемость паролей» и измените значение на 1.

6 Для настройки «Политики безопасности блокировки учетной записи» выберите этот подпункт и откройте его.

7 Ознакомиться со свойствами всех параметров для данного подпункта. Значения параметров «Политики учетной записи» приведены в таблице 9.

Таблица 9 – Параметры вкладки «Политика учетной записи»

Параметр	Значение
Пороговое значение блокировки	Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется.
Блокировка учетной записи	Определяет число минут, в течении которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована.
Сброс счетчика блокировки через	Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0.

8 Повторить задания 3-5 для настроек «Политики безопасности блокировки учетной записи».

9 Ответить на контрольные вопросы:

1 Что такое аутентификация и идентификация?

2 Для чего применяются эти механизмы?

3 Что можно настроить с помощью вкладки «Локальные политики безопасности»?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6

Тема. Исследование защиты с применением пароля, а также методы противодействия атакам на пароль.

Цель работы. Исследовать защиту с применением пароля, а также методы противодействия атакам на пароль.

Теоретическое введение

Для выполнения работы необходима установленная основная ОС Windows и ПО Elcomsoft ADRP (если отсутствует, то скачать с сайта производителя https://www.elcomsoft.com/arpr.html).

К наиболее распространенным метода взлома пароля относятся.

1 Атака с использованием словарей.

В данном методе используется простой файл, содержащий слова, которые можно найти в словаре. Другими словами, атаки такого типа перебирают именно слова, которые многие люди используют в качестве пароля.

Такая «хитрость», как умело сгруппированные вместе слова, например, «симсимоткройся» или «ясуперадминистратор», не спасут пароль от взлома. Возможно, хакеры всего лишь потратят несколько лишних секунд.

2 Атака методом полного перебора (грубой силы).

Этот метод похож на атаку по словарю, но с дополнительным бонусом, конечно, для хакера, который позволяет обнаружить слова, не содержащиеся в словаре, перебирая все возможные буквенно-цифровые комбинации от aaa1 до zzz10. Это не быстрый способ, особенно, если ваш пароль состоит из нескольких символов, но, в конечном счете, пароль будет раскрыт. Метод полного перебора может быть упрощен с помощью использования дополнительных вычислительных мощностей компьютера, в том числе с использованием возможностей видеокарты GPU, и, например, использования распределенных вычислительных моделей и зомби-ботнетов.

3 Атака с использованием радужной таблицы.

Радужная таблица – это список предварительно вычисленных хэшей (числовых значений зашифрованных паролей), используемых большинством современных систем. Таблица включает в себя хэши всех возможных комбинаций паролей для любого вида алгоритма хэширования. Время, необходимое для взлома пароля с помощью радужной таблицы, сводится к тому времени, которое требуется, чтобы найти захэшированный пароль в списке. Тем не менее, сама таблица огромна и для просмотра требует серьезных вычислительных мощностей. Также она будет бесполезна, если хэш, который она пытается найти был усложнен добавлением случайных символов к паролю до применения алгоритма хеширования. Стоит сказать о возможности существования усложненных радужных таблиц, но они были бы настолько вели-

ки, что их было бы трудно использовать на практике. Они, скорее всего, работали бы только с набором заранее заданных «случайных величин», при этом пароль должен состоять менее чем из 12 символов, иначе размер таблицы будет непомерно велик, даже для хакеров государственного уровня.

4 Фишинг.

Самый простой способ взлома – спросить у пользователя его/ее пароль. Фишинговое сообщение приводит ничего не подозревающего читателя на поддельные сайты онлайн-банкинга, платежных систем или иные сайты, на которых нужно обязательно ввести личные данные, чтобы «исправить какую-то страшную проблему с безопасностью».

5 Социальная инженерия.

Социальная инженерия придерживается концепции, что и фишинг – «спросить у пользователя пароль», но не с помощью почтового ящика, а в реальном мире. Любимый трюк социальной инженерии – позвонить в офис под видом сотрудника ИТ-безопасности и просто попросить пароль доступа к сети. Вы будете удивлены, как часто это работает. Некоторые преступники даже испытывают потребность надеть костюм и бейдж до того, как прийти в компанию, чтобы задать администратору в приемной тот же вопрос лицом к лицу.

6 Вредоносное программное обеспечение.

Программа перехвата вводимой с клавиатуры или выводимой на экран информации может быть установлена вредоносным ПО, которое фиксирует всю информацию, которую вы вводите, или создает скриншоты во время процесса авторизации, а затем направляет копию этого файла хакерам. Некоторые вредоносные программы ищут существующий файл с паролями веб-браузера клиента, затем копируют этот файл, который (кроме хорошо зашифрованных) будет содержать легкодоступные сохраненные пароли из истории страниц, посещенных пользователем.

7 Офлайн-хакинг.

Есть представление, что пароли находятся в безопасности, когда они защищены системами блокировки (пользователей блокируют после трех-четырех неудачных попыток набора пароля). Также происходит блокировка приложения автоматического подбора паролей. Это было бы верно, если бы не тот факт, что большинство взломов паролей происходит в оффлайне, с использованием набора хэшей в файле паролей, которые были «получены» от скомпрометированной системы. Часто рассматриваемая жертва оказывается скомпрометирована через взлом третьей стороны, которая тем самым обеспечивает доступ хакерам к системе серверов и всем важным файлам пользователя с хэшированными паролями. Взломщик паролей может работать

столько времени, сколько ему нужно, чтобы попытаться взломать код без оповещения целевой системы или отдельных пользователей.

8 Подглядывание через плечо.

Наиболее самоуверенные хакеры под видом курьеров, специалистов по техническому обслуживанию кондиционеров или любых других служащих проникают в офисные здания. Как только они попадают в офисное здание, униформа обслуживающего персонала предоставляет им своего рода бесплатный билет на беспрепятственный доступ во все уголки офисного здания. Это позволяет им записывать пароли, вводимые реальными сотрудниками, а также предоставляет отличную возможность увидеть все те пароли, которые многие так любят писать на стикеры и клеить прямо на мониторы своих компьютеров.

9 Метод «пауков».

Опытные хакеры поняли, что многие корпоративные пароли состоят из слов, которые связаны с бизнесом. Изучение корпоративной литературы, материалов веб-сайтов, сайтов конкурентов и даже список клиентов могут обеспечить хакеров «боеприпасами» для построения пользовательского списка слов, который затем используется для взлома методом грубой силы. Они автоматизировали процесс и запускают «паутинные» приложения, аналогичные тем, которые применяются ведущими поисковыми системами, чтобы определить ключевые слова, собрать и обработать списки для взлома.

10 Догадки.

Лучшим другом взломщиков паролей, конечно, является предсказуемость пользователей. Если действительно случайный пароль был создан с помощью программного обеспечения, предназначенного для этой задачи, то пользовательский «случайный» пароль, вряд ли будет напоминать что-то подобное. Вместо этого, благодаря нашей эмоциональной привязанности к вещам, которые нам нравятся, скорее всего, те «случайные» пароли, которые мы создадим, будут основаны на наших интересах, хобби, именах домашних животных, семье и так далее. На самом деле, пароли, как правило, строятся на основе всех тех вещей, о которых мы так хотели бы поговорить в социальных сетях и даже включить в наш профиль. Взломщики паролей, вполне вероятно, посмотрят на эту информацию и сделают несколько, часто правильных, догадок при попытке взломать пароль потребительского уровня, не прибегая к словарю или методу грубой силы.

Задания:

1 Зашифровать файл формата ZIP. Для этого создаем папку на рабочем столе и добавляем в нее любой текстовый документ (ВАЖНО: имя текстового файла не должно содержать русских букв). Правым кликом мышки по

папке выбираем «Добавить в архив…» (рисунок 7). Итоговый отчет должен содержать скриншоты выполнения этапов заданий.

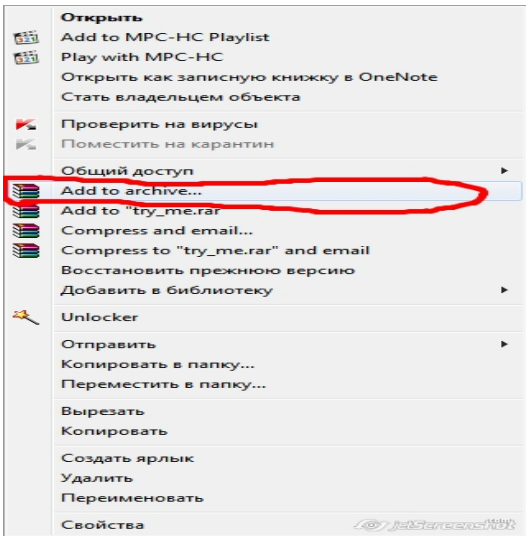


Рисунок 7 – Добавление файлов в архив

2 В появившемся окне выбрать «Установить пароль» (рисунок 8).

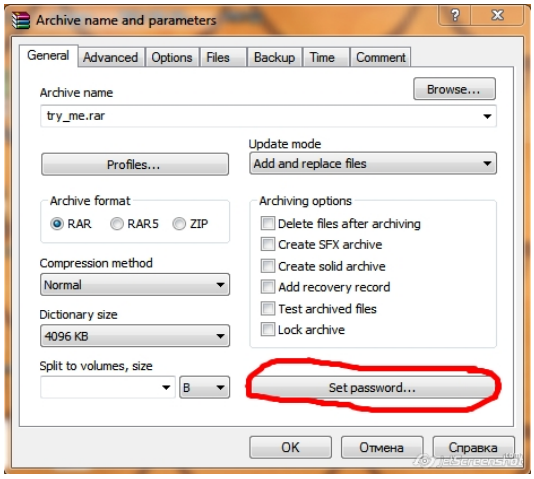


Рисунок 8 – Окно установки пароля

3 Далее в окне Enter password вводим пароль, который состоит из первой буквы фамилии, первой буквы имени и последних двух цифр текущего года (например, для Петрова Ильи, который выполняет данную лабораторную в 2017 году, паролем будет PI17). Нажимаем «ОК» (рисунок 9).

Рисунок 9 – Установка пароля на архив

4 Запускаем программу Advanced Archive Password Recovery. В качестве области перебора выступят заглавные буквы и длина от 1 до 4 символов (рисунок 10).

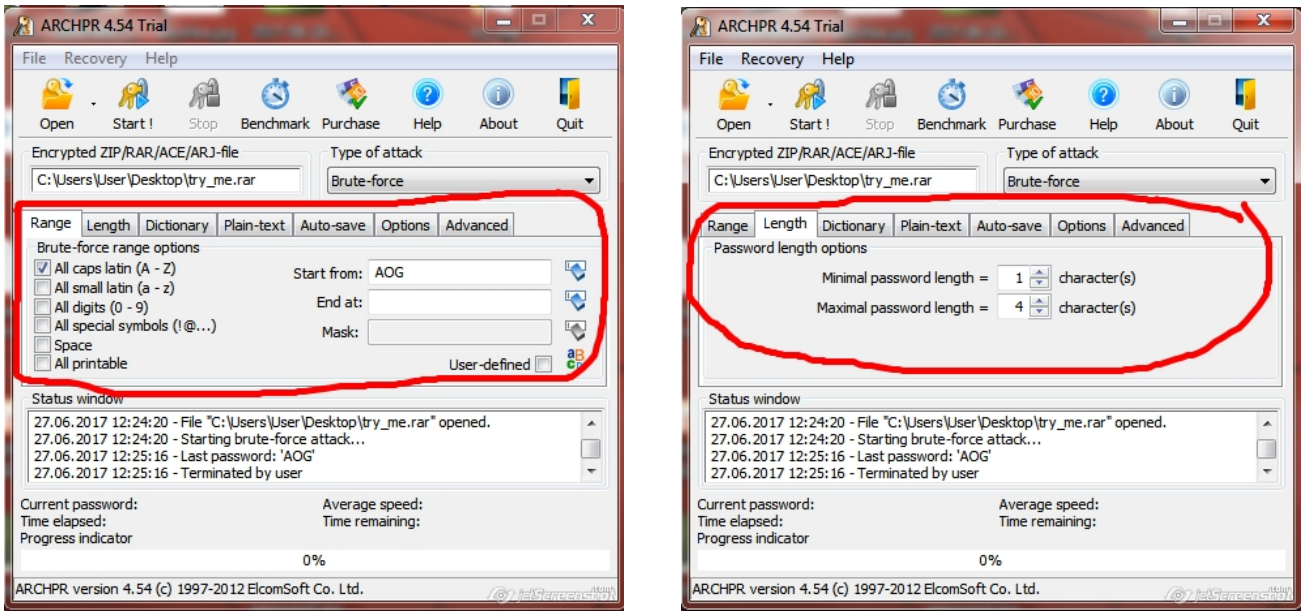


Рисунок 10 – Окно программы Advanced Archive Password Recovery

5 Выбираем зашифрованный файл кнопкой «Open». Процесс брутфорса запустится автоматически.

6 Записать результаты подбора пароля, а также затраченное на это время.

7 Провести атаку по словарю. Для созданного архива зададим пароль из английского словаря, например, «love». В программе меняем тип атаки на «Dictionary» (рисунок 11).

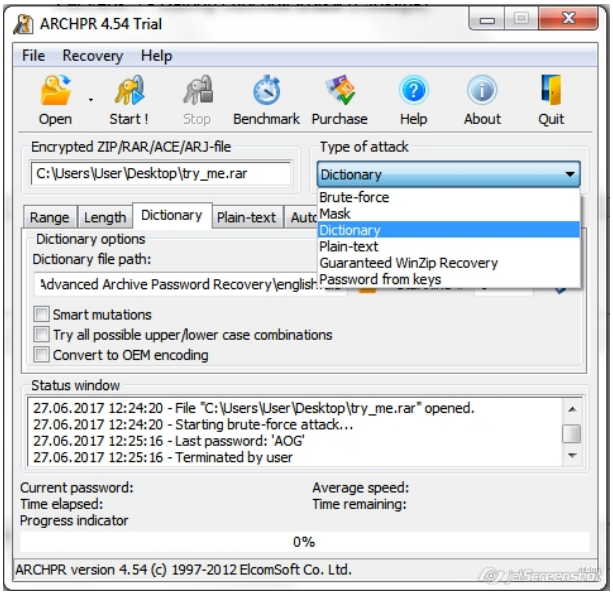


Рисунок 11 – Окно программы Advanced Archive Password Recovery

8 Записать результаты подбора пароля, а также затраченное на это время.

9 Проверить этот же архив методом простого перебора (тип атаки «Brute-force»). В качестве настроек выбираем «All small latin» (рисунок 12).

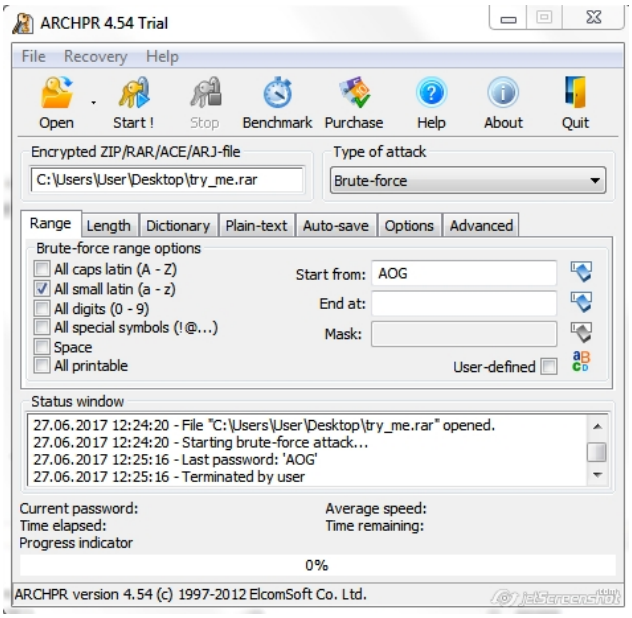


Рисунок 12 – Окно программы Advanced Archive Password Recovery

10 Записать результаты подбора пароля, а также затраченное на это время.

11 Сделать выводы по работе и ответить на контрольные вопросы:

1 Для чего необходимо шифровать данные?

2 Каким должен быть пароль для усложнения процесса взлома?

3 Какой метод взлома информации называют методом грубой силы?

4 Что такое радужная таблица?

5 Какой способ является самым простым?

6 В чем состоит метод атаки вредоносного программного ПО?

7 Что является главным помощником для взломщиков паролей?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7

Тема. Основные методы криптографической защиты информации.

Цель работы. Изучить основные методы криптографической зашиты информации.

Теоретическое введение

Основным видом криптографического преобразования информации в компьютерных системах является шифрование и дешифрование.

Криптография — наука о защите информации от несанкционированного получения ее посторонними лицами. Сфера интересов криптографии — разработка и исследование методов шифрования информации.

Шифрование – это преобразование информации из открытой формы в закрытую (зашифрованную). Существует и обратный процесс – расшифрование. Под шифрованием понимается такое преобразование информации, которое делает исходные данные нечитаемыми и трудно раскрываемыми без знания специальной секретной информации – ключа. В результате шифрования открытый текст превращается в шифрограмму и становится нечитаемым без использования дешифрирующего преобразования. Шифрограмма позволяет скрыть смысл передаваемого сообщения. Под **ключом** понимается «изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование» [ГОСТ Р 34.12-2015].

Дешифрование – обратный шифрованию процесс. При дешифрировании с использованием ключа зашифрованный текст (шифрограмма, шифровка) преобразуется в исходный открытый текст. Процесс получения криптоаналитиками открытого сообщения из криптограммы без заранее известного ключа называется вскрытием или взломом шифра.

Все современные методы шифрования делятся на одноключевые, или симметричные, и двухключевые, или асимметричные.

В симметричных криптографических системах ключи, используемые на передающей и приемной сторонах, полностью идентичны. Такой ключ несет в себе всю информацию о засекреченном сообщении и поэтому не должен быть известен никому, кроме двух участвующих в разговоре сторон. Противник, наблюдая зашифрованное сообщение (шифротекст), не может прочитать сообщение. Секретный канал, используемый для передачи секретного ключа от отправителя к получателю, должен исключать возможность утечки информации (рисунок 13).

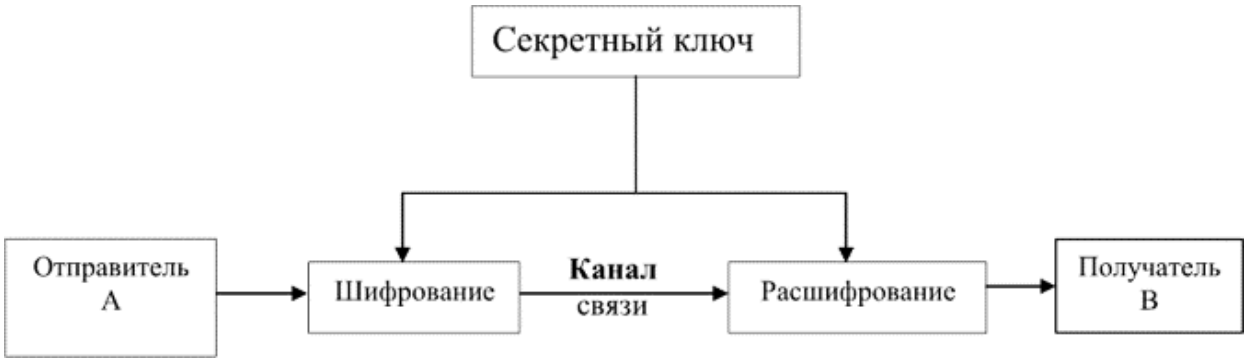


Рисунок 13 – Схема симметричного шифрования информации

В асимметричных криптографических системах для шифрования и дешифрования применяются различные ключи. Для шифрования информации, предназначенной конкретному получателю, используют уникальный открытый ключ получателя-адресата. Соответственно для дешифрова-

ния получатель использует парный секретный ключ. Для передачи открытого ключа от получателя к отправителю секретный канал не нужен. Вместо секретного канала используется аутентичный канал, гарантирующий подлинность источника передаваемой информации (открытого ключа отправителя) (рисунок 14). Аутентичный канал является открытым и доступен противнику.

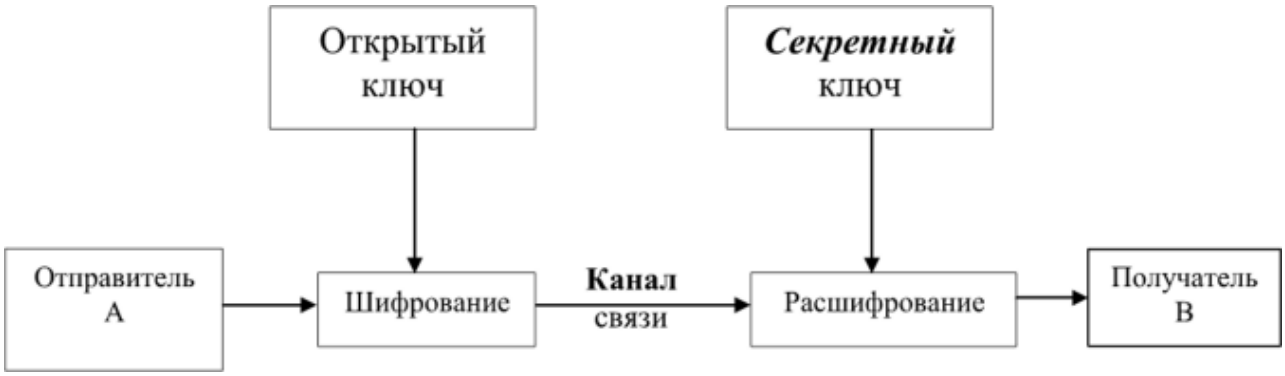


Рисунок 14 – Схема ассиметричного шифрования информации

Рассмотрим некоторые из способов шифрования информации.

Шифры подстановки

1 Шифр Цезаря

При использовании данного шифра каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита. Способы выбора ключей могут быть различны. В шифре Цезаря ключом служит произвольное число k, выбранное в интервале от 1 до 32. Каждая буква открытого текста заменяется буквой, стоящей на k знаков дальше нее в алфавите.

К примеру, пусть ключом будет число 5. Тогда буква А русского алфавита будет заменена буквой Е, буква Б – буквой Ж и так далее (смотреть таблицу 10).

Таблица 10 – Таблица для замены символов в шифре Цезаря

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д

Зашифруем слово «КРИПТОГРАФИЯ», используя полученный алфавит. Буква «К» исходного алфавита заменяется буквой «П» шифрованного алфавита, буква «Р» – «Х» и т.д. В результате получаем «ПХНФЧУИХЕЩНД».

2 Шифр Атбаш

«Атба́ш» – один из самых древних методов шифрования. Шифрование заключается в замене каждой буквы исходного текста на «симметричную» ей

букву алфавита, то есть первая алфавита заменялась на последнюю и наоборот, вторая буква – на предпоследнюю и наоборот и т. д. (таблица 11).

Таблица 11 – Шифр Атбаш

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Е	Д	Г	В	Б	А

Зашифруем слово «КРИПТОГРАФИЯ», используя Атбаш. Буква «К» заменяется буквой «Х», буква «Р» – «П» и т.д. В результате получаем «ХПЧПНСЬПЯЛЧА».

3 Шифр Виженера

Данный шифр представляет собой серию шифров Цезаря, где сдвиг буквы зависит от кодового слова. Чтобы зашифровать сообщение шифром Виженера, используют квадрат Виженера (таблица 12). Квадрат состоит из 32 строк шрифтов Цезаря, начинающихся с нуля. На каждую дополнительную строку сдвиг увеличивается на 1.

Таблица 12 – Квадрат Виженера

	А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**
А	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Зашифруем слово «КРИПТОГРАФИЯ», для этого необходимо выбрать ключевое слово, например, «ГРУША», и по циклу записывать его (таблица 13).

Таблица 13 – Запись ключевого слова при использовании шифра Виженера

Исходное слово	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Ключ	Г	Р	У	Ш	А	Г	Р	У	Ш	А	Г	Р
Шифрограмма	Н	А	Ы	З	Т	С	У	Г	Ш	Ф	Л	П

Строки в таблице Виженера отвечают за ключевое слово, а столбцы – за исходное сообщение. Находим пересечение: строку буквы «К», и столбец «Г» – получается буква «Н». Строка «Р» и столбец «Р» дают букву «А».

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Шифры простой замены

1 Код Полибия

«Квадрат Полибия» представляет собой квадрат 5х6, столбцы и строки которого нумеруются цифрами от 1 до 6. В каждую клетку этого квадрата записывается одна буква (исключение: Е/Ё, И/Й, Ь/Ъ). Буквы расположены в алфавитном порядке (таблица 14). В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путём нахождения буквы, стоящей на пересечении строки и столбца.

Таблица 14 – Квадрат Полибия

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е/Ё
2	Ж	З	И/Й	К	Л	М
3	Н	О	П	Р	С	Т
4	У	Ф	Х	Ц	Ч	Ш
5	Щ	Ы	Ь/Ъ	Э	Ю	Я

Зашифруем слово «КРИПТОГРАФИЯ».

Исходное слово	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Строка	2	3	2	3	3	3	1	3	1	4	2	5
Столбец	4	4	3	3	6	2	4	4	1	2	3	6
Код	24	34	23	33	36	32	14	34	11	42	23	56

Получилась последовательность: 24 34 23 33 36 32 14 34 11 42 23 56.

2 Шифрующие таблицы Трисемуса

Таблица Трисемуса заполняется с помощью ключевого слова, повторяющиеся буквы которого отбрасываются. Затем таблица дополняется не вошедшими в нее буквами алфавита по порядку. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы.

При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква на последней строке – заменяется буквой из первой строки в том же столбце. Для русского алфавита шифрующая таблица может иметь размер 4х8 или 5х7 с добавлением пробела, точки и запятой (таблица 15).

Таблица заполнена с помощью ключевого слова «КРИПТОГРАФИЯ», при этом оставляем только ОДНО появление буквы, то есть убираем вторую «Р» и вторую «И». Буква фразы, которую необходимо зашифровать, заменяется символом, стоящим ниже.

Таблица 15 – Таблица Трисемуса

К	Р	И	П	Т	О	Г	А
Ф	Я	Б	В	Д	Е	Ж	З
Й	Л	М	Н	С	У	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Зашифруем фразу «ЗАЩИТА ИНФОРМАЦИИ». Буква «З» заменяется буквой «Ц». Буква «А» заменяется на «З», «Щ» на «И» и т. д. В итоге получается слово «ЦЗИБДЗБЪЙЕЯЩЗЮББ».

Открытый текст	З	А	Щ	И	Т	А	И	Н	Ф	О	Р	М	А	Ц	И	И
Шифрограмма	Ц	З	И	Б	Д	З	Б	Ъ	Й	Е	Я	Щ	З	Ю	Б	Б

3 Биграммный шифр Плейфейра

В целом, структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Процедура шифрования включает следующие шаги:

Шаг 1: Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если при шифровании в фразе используется нечетное количество букв, то можно в конце добавить дополнительную букву, символ, либо при шифровании записать непарную букву без изменений.

Шаг 2: Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм зашифрованного текста по следующим условиям:

Условие 1: Если обе буквы биграммы открытого текста *не попадают* на одну строку или столбец (как, например, буквы Р и В), тогда находят буквы *в углах прямоугольника*, определяемого данной парой букв. В нашем примере это буквы РВПЯ (таблица 16). Пара букв РВ отображается в пару ПЯ. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста.

Условие 2: Если обе буквы биграммы открытого текста принадлежат *одному столбцу* таблицы, то буквами шифртекста считаются буквы, которые лежат *под ними*. (Например, биграмма ИМ дает биграмму шифртекста БЩ.) Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца. (Например, биграмма ВЪ дает биграмму шифртекста НП.)

Условие 3: Если *обе буквы* биграммы открытого текста принадлежат *одной строке* таблицы, то буквами шифртекста считаются буквы, которые лежат *справа от них*. (Например, биграмма ЛУ дает биграмму шифртекста МХ.) Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке. (Например, биграмма ВЗ дает биграмму шифртекста ДФ).

Зашифруем фразу «ШИФРОВАНИЕ» с ключом «КРИПТОГРАФИЯ».

Составляем таблицу (таблица 16).

Таблица 16 – Таблица Плейфейра

К	Р	И	П	Т	О	Г	А
Ф	Я	Б	В	Д	Е	Ж	З
Й	Л	М	Н	С	У	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Разбиваем текст на биграммы: «ШИ ФР ОВ АН ИЕ» и шифруем согласно условиям.

Первая биграмма «ШИ» (выделена серым) превращается в «ЩР» по первому условию. Вторая биграмма «ФР» превращается в «ЯК» по первому условию. Третья биграмма «ОВ» превращается в «ПЕ» по первому условию. Четвертая биграмма «АН» превращается в «ПЦ» по первому условию. Пятая биграмма «ИЕ» превращается в «ОБ» по первому условию. Получаем результат, представленный в таблице 17.

Таблица 17 – Результат шифрования с помощью таблицы Плейфейра

Биграмма	ШИ	ФР	ОВ	АН	ИЕ
Шифрограмма	ЩР	ЯК	ПЕ	ПЦ	ОБ

Расшифрование происходит в таком же порядке.

Задания:

1 Зашифровать фразу «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА», используя шифр Цезаря при k=8.

2 Расшифровать ХПЧРНСЬПЯЛЧА, зная, что зашифровано шифром Атбаш.

3 Расшифровать фразу, используя шифр Виженера.

Ключ	Р	А	Б	О	Т	А		Р	А	Б	О	Т	А
Зашифрованное слово	Ь	Е	У	Ь	Ц	Ы		Ч	А	Ъ	Ц	Д	Ы
Открытый текст													

4 Зашифровать фразу «ЗАЩИТА ИНФОРМАЦИИ» кодом Полибия.

5 Расшифровать фразу «БКГЖДЩЙЯБЖККЙНМЛУЖЪЙЫКЖЫЬО» с помощью таблицы Трисемуса, используя ключ «ШИФРОВАНИЕ».

6 С помощью шифра Плейфейра зашифровать фразу «УГРОЗЫ БЕЗОПАСНОСТИ» с ключом «СИСТЕМА».

7 Зашифровать свои фамилию, имя и отчество всеми изученными шифрами с произвольными ключами. Ключи не должны повторять те, которые использовались в примерах.

8 Ответить на контрольные вопросы:

1 Что такое шифрограмма?

3 Какие существуют шифры?

4 Для чего нужна криптография?

4 В чем отличие симметричных шифров от асимметричных?

5 Как происходит расшифрование текста, зашифрованного шифром Вижинера?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8

Тема. Работа с командной строкой WINDOWS.

Цель работы. Изучить встроенные утилиты операционной системы Microsoft Windows для работы с файловой системой и диагностики сетевых подключений.

Теоретическое введение

Знакомство с обработчиком команд Windows начинаем со списка основных команд, который получаем с помощью директивы «help». Набираем ее в командной строке и делаем запуск на выполнение нажатием клавиши «Enter». Список состоит из двух колонок – названия команды и ее описания.

Получить подробную справку для команды можно двумя способами:

help [*имя_команды*] или имя_команды /?

Например, получаем справку по chkdsk:

help chkdsk или chkdsk /?

Чтобы избежать повторного набора, пользуемся буфером команд, который листается с помощью комбинаций клавиш ↑ или ↓.

Команда «cls» предназначена для очистки экрана.

Далее разберем основные команды для работы с файлами: dir, cd, mkdir, rmdir, del, copy. При этом следует помнить, что символ ***** означает, что вместо символа может быть любое количество символов, а символ **?** означает, что вместо символа может быть только один символ.

Команда «dir» используется для просмотра содержимого папки (каталога). Если вы хотите увидеть в текущей папке только исполняемые файлы с расширением .exe, вам необходимо набрать строку:

```
dir *.exe
```

Команда «cd» – используется для смены текущей папки. «cd», далее [имя_папки или C:\полный_путь].

Чтобы попасть на уровень выше по дереву каталогов: cd..

Чтобы попасть в корневой каталог: cd \

Команды «mkdir» – [имя_папки] и «rmdir» [имя_папки].

«mkdir» занимается созданием папок (каталогов), а «rmdir» – удаляет ее:

```
mkdir test
rmdir /S test
```

Команды «del» [имя_файла] и «copy» [имя_файла] [путь_куда_скопировать] предназначены, соответственно, для того, чтобы удалять и копировать файлы. Также с помощью команды «copy» можно переименовать файл или создать его с содержимым.

Например, чтобы создать текстовый файл с текстом «Привет, мир!» можно ввести:

copy “Привет, мир!” > file.txt

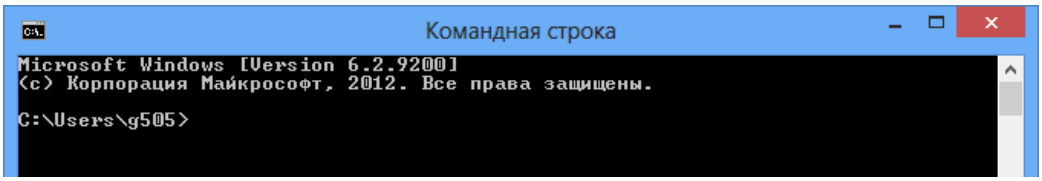
Файл будет создан в текущей папке и иметь формат .txt

Задания:

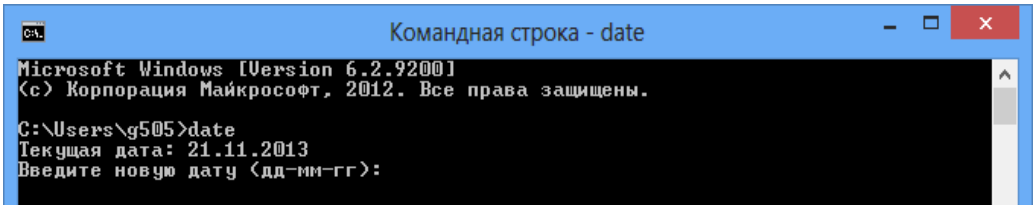
Отчет выполнения работы должен содержать скришоты этапов выполнения заданий.

1 Создайте на рабочем столе папку Test.

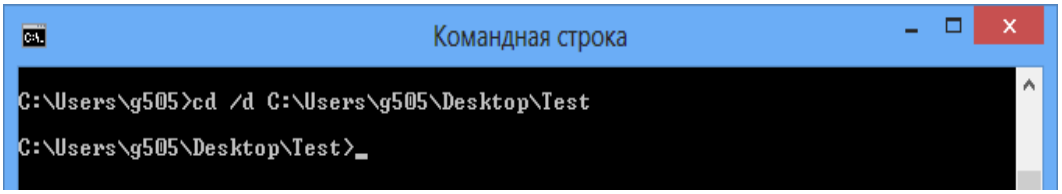
2 Запустите командную строку cmd.exe («Пуск» – ввод с клавиатуры «cmd» без кавычек).



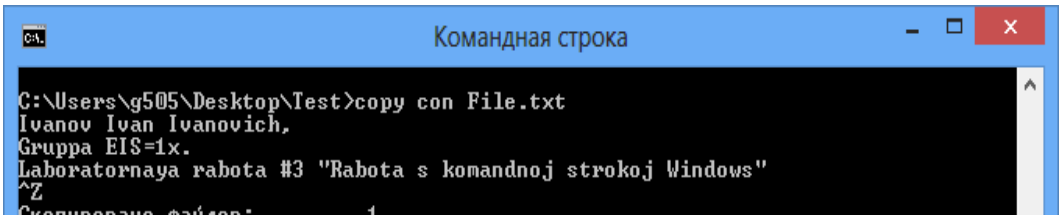
3 Проверьте системные дату и время с помощью команд «date» и «time» без кавычек. Для этого в командной строке наберите нужную команду и нажмите Enter.



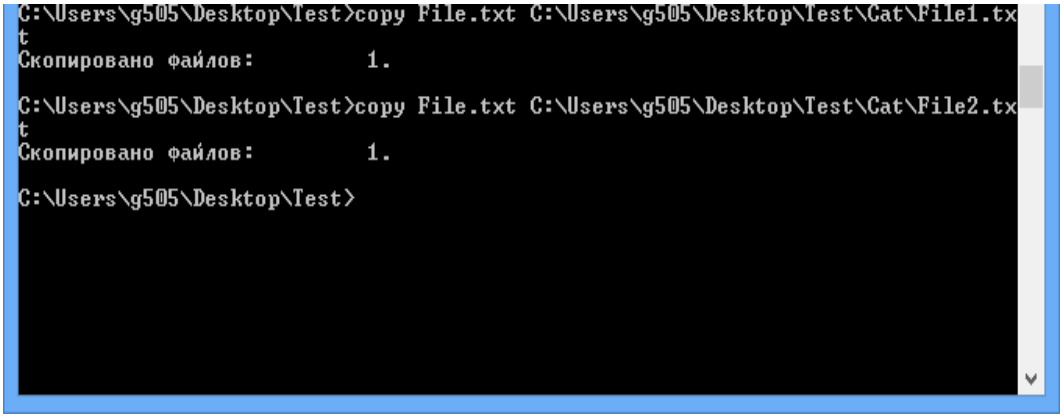
4 С помощью утилиты «cd» измените текущий каталог на каталог «Test», созданный Вами ранее.



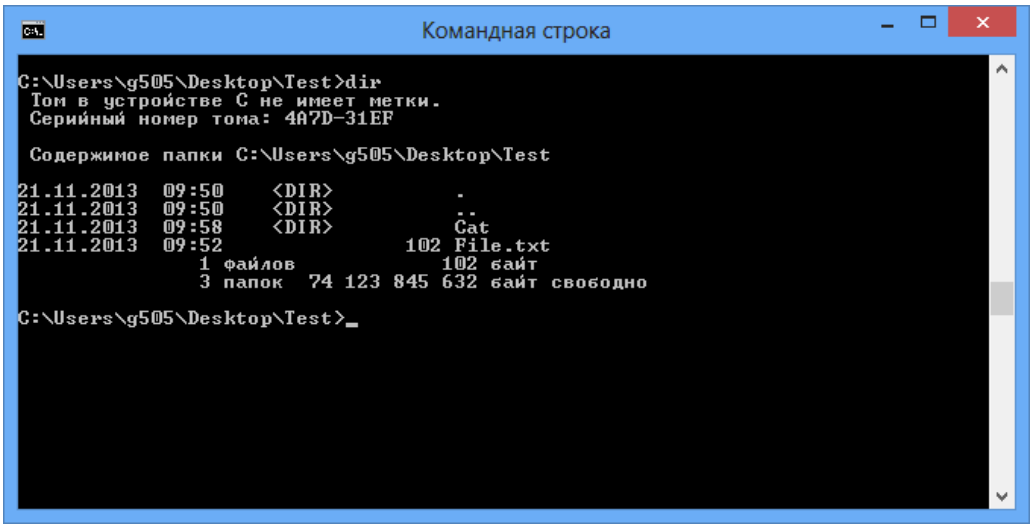
5 С помощью команды «md» создайте каталог с именем «Cat».



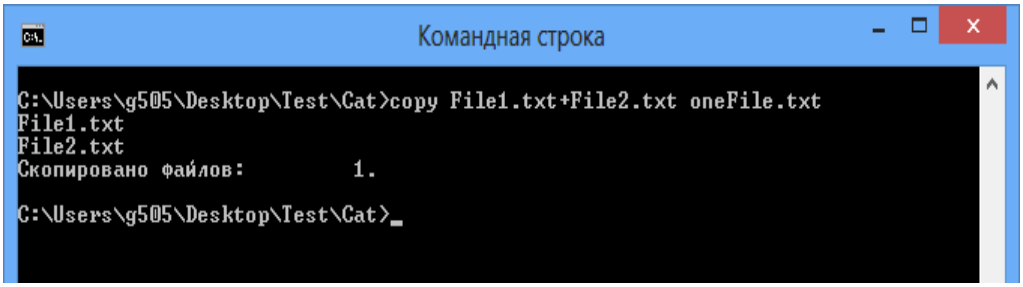
6 Используя команду «copy con», создайте файл с именем «File.txt». (Команда «copy con» означает копирование с консоли, т. е. с клавиатуры). После данной команды введите следующий текст: Ваши Ф.И.О., группа и название практической работы. Закройте файл сочетанием клавиш «Ctrl+Z».



7 С помощью команды «dir» просмотрите список созданных объектов в папке «Test». Команда в общей сложности фиксирует 3 каталога (папки), т. к. первая метка указывает на текущий каталог, обозначенный точкой, вторая – на предыдущий каталог (две точки).

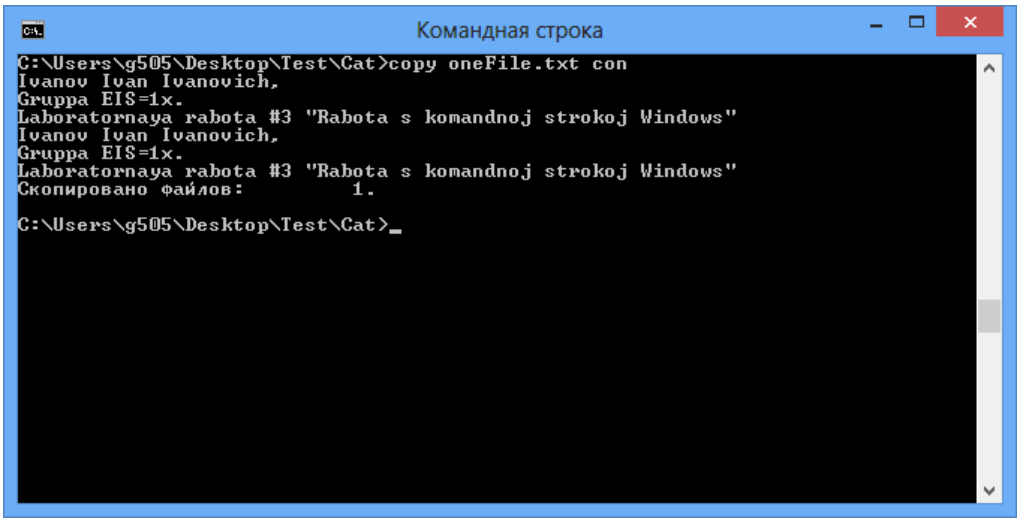


8 В каталоге «Cat» с помощью команды «copy» создайте две копии файла «File.txt» – «File1.txt» и «File2.txt».



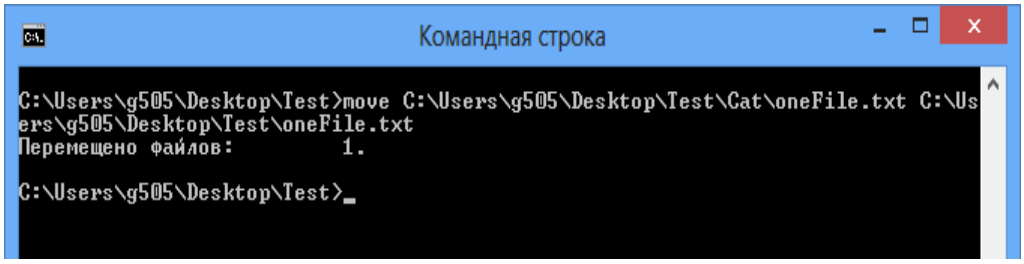
9 Объедините файлы «File1.txt» и «File2.txt» в файл «oneFile.txt» с помощью команды «copy».

10 Просмотрите полученный файл «oneFile» с помощью утилиты

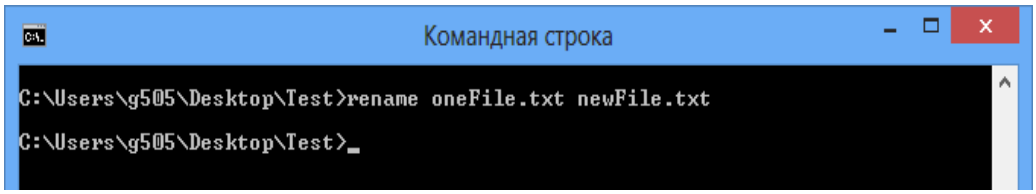


«copy».

11 С помощью команды «move» переместите файл «oneFile.txt» в папку «Test».

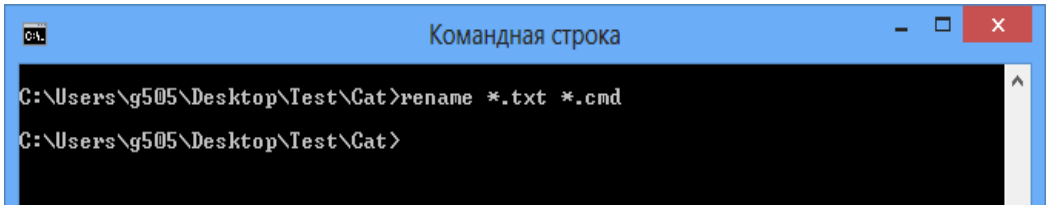


12 С помощью команды «rename» переименуйте файл «oneFile.txt» в «newFile.txt».



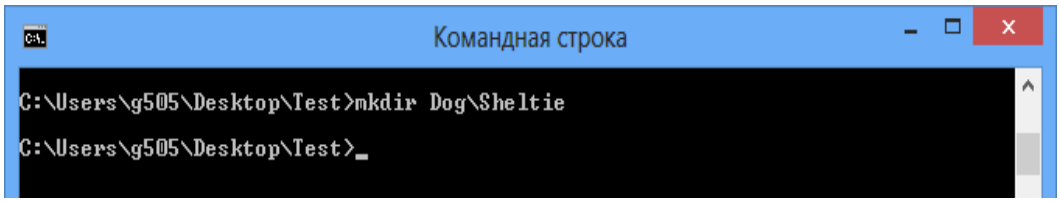
13 С помощью той же команды смените расширения у всех файлов в каталоге «Cat».

14 Измените расширение файлов на исходное.



15 Создайте в папке «Test» две цепочки вложенных каталогов с помощью команды» mkdir»:

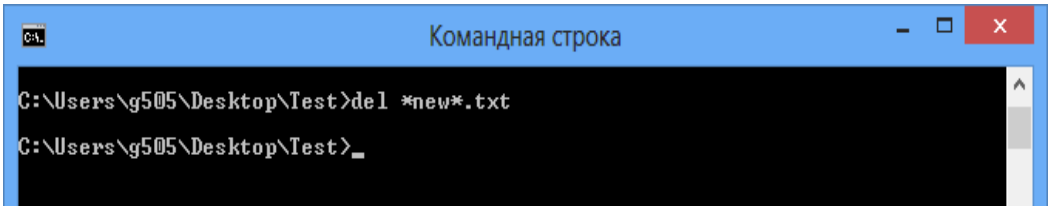
а) каталог «Dog», содержащий каталоги «Bulldog» и «Sheltie»;



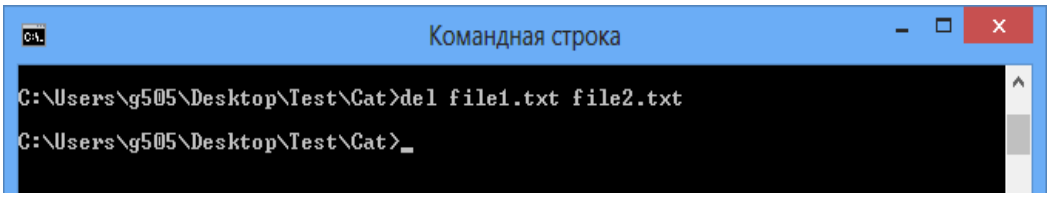
б) каталог «Bird», содержащий каталоги «Flying» и «Non-flying». Каталог «Non-flying» содержит два подкаталога: «Ostrich» и «Penguin».

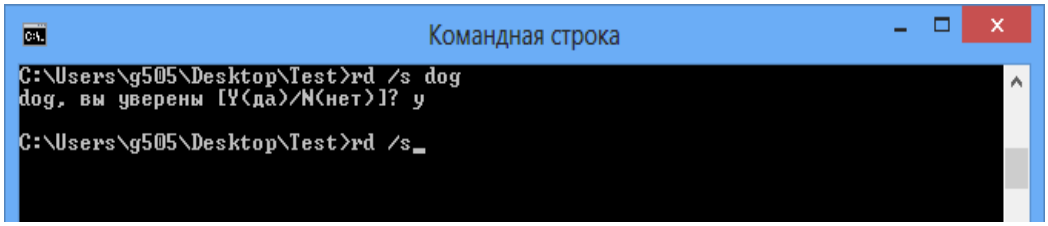
16 Используя команду «tree», постройте дерево каталогов папки «Test».

17 Удалите все файлы, содержащие в названии слово «new», из каталога «Test» посредством утилиты «del».



18 Удалите все файлы из каталога «Cat».





19 Удалите каталоги «Bird» и «Dog» с помощью команды «rd /s».

При работе с сетью используют команды работы с сетью – инструмент, который необходим, в основном, системным администраторам и пользователям для решения различных сетевых задач.

1 Утилита «ipconfig»

Утилита «ipconfig» служит для отображения параметров текущих сетевых подключений, а также для управления клиентскими сервисами DHCP и DNS.

Синтаксис ввода:

ipconfig [/all] [/renew [адаптер]] [/release [адаптер]]

При вводе команды могут использоваться ключи (дополнительные параметры). Список наиболее часто употребляемых параметров представлен в таблице 1. При вводе команды «ipconfig» без параметров выводится только IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

Таблица 17 – Список наиболее часто употребляемых ключей при вызове утилиты «ipconfig»

Ключ	Описание
/all	Отображение полной информации по всем сетевым подключениям.
/release	Сброс текущих параметров сетевого подключения и освобождение сетевого адреса, предоставленного DHCP сервером.
/renew	Обновление параметров сетевого подключения.
/?	Отображает справку в командной строке.

На рисунке 15 показаны результаты ввода команды «ipconfig» с ключом «/all» для компьютера с одним активным сетевым подключением.

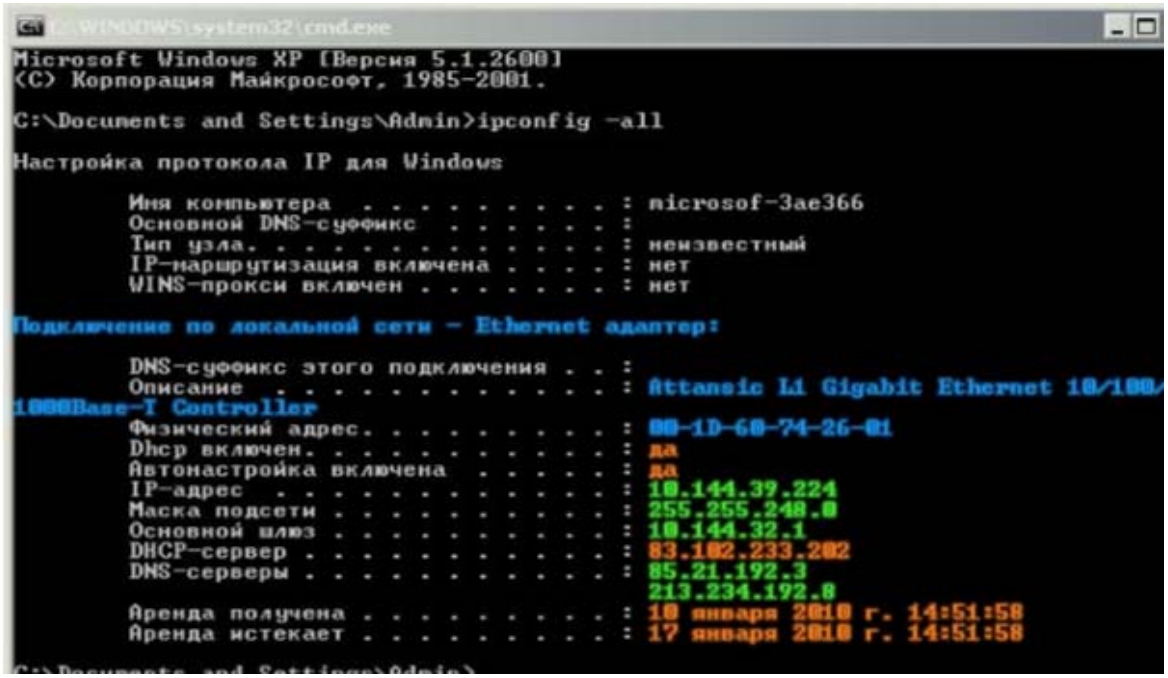


Рисунок 15 – Результаты ввода команды «ipconfig» с ключом «/all»

Результаты вывода можно условно разделить на три группы.

К первой группе (значения, выделенные синим цветом) относится общая информация о сетевом подключении:

– «Подключение по локальной сети» – имя сетевого подключения;

– «Ethernet адаптер» – тип адаптера;

– «Attansic L1 Gigabit Ethernet 10/100/1000Base-T Controller» – описание адаптера;

– «00-1D-60-74-26-01» – физический адрес (MAC-адрес) адаптера.

Ко второй группе (значения, выделенные зеленым цветом) относится информация о сетевых настройках подключения:

– «10.144.39.224» – сетевой адрес (IP-адрес) подключения;

– «255.255.248.0» – маска подсети;

– «10.144.32.1» – адрес шлюза;

– «85.21.192.3», «213.234.192.8» – адреса серверов DNS.

К третьей группе (значения, выделенные оранжевым цветом) относится информация о деталях аренды адреса у DHCP сервера:

– «Dhcp включен: да» – функция получения параметров у DHCP сервера включена;

– «Автонастройка включена: да» – функция авто-настройки подключения включена;

– «83.102.233.202» – адрес DHCP сервера, у которого получены параметры;

– «10 января 2010 г. 14:51:58» – дата получения параметров;

– «17 января 2010 г. 14:51:58» – дата истечения аренды сетевого адреса.

2 Утилита «ping»

Утилита «ping» предназначена для проверки работоспособности соединения между двумя устройствами на уровне протокола IP (сетевом уровне). Утилита выполняет проверку, посылая на указанный сетевой адрес эхо-запросы (ICMP Echo-Request) протокола ICMP и фиксирует получение эхо-ответов (ICMP Echo-Reply).

Синтаксис ввода:

ping [-t] [-a] [-n счетчик] [имя_конечного_устройства]

При вводе команды могут использоваться ключи (дополнительные параметры). Список наиболее часто употребляемых параметров представлен в таблице 17.

Таблица 17 – Список наиболее часто употребляемых ключей при вызове утилиты «ping»

Ключ	Описание
/t	Задает для команды ping отправку эхо-запросов к точке назначения до тех пор, пока команда не будет прервана. Для прерывания команды и вывода статистики нажмите комбинацию CTRL+BREAK. Для прерывания команды ping и выхода из нее нажмите клавиши CTRL+C
/a	Задает разрешение DNS имени по IP-адресу назначения, либо IP-

	адрес по DNS имени назначения. В случае успешного выполнения выводится имя и IP-адрес удалённого устройства
/n	Задает число отправляемых эхо-запросов
/?	Отображает справку в командной строке

На рисунке 16 показаны результаты успешного выполнения команды «ping».

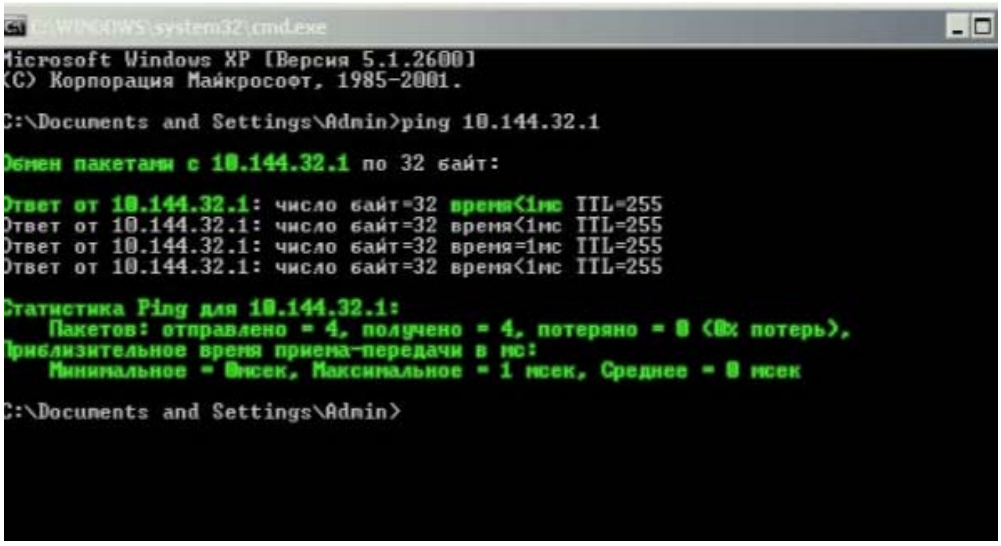


Рисунок 16 – Успешное выполнение команды «ping»

Полученные результаты можно интерпретировать следующим образом.

– «Обмен пакетами с 10.144.32.1» – локальное устройство начало посылать удалённому устройству эхо запросы;

– «Ответ от 10.144.32.1» – от удалённого устройства пришёл эхо-ответ;

– «Время <1 мс» – RTT (Round Trip Time) – время, затраченное на отправку эхо-запроса и получение эхо-ответа;

– «Статистика Ping для 10.144.32.1: Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0 % потерь), Приблизительное время приема-передачи в мс: Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек» – статистика результата выполнения команды «ping».

Если сообщение с эхо-ответом не получено в пределах заданного интервала, то выдается сообщение об ошибке "Превышен интервал ожидания для запроса". Интервал по умолчанию равен 4 секунды.

Причины отсутствия эхо-ответа могут быть следующими:

1 удалённое устройство не обрабатывает эхо-запросы или не отправляет эхо-ответы из соображений безопасности;

2 осуществить взаимодействие между устройствами невозможно из-за проблем в каналах связи;
3 одно из устройств работает некорректно;
4 качество линий связи настолько низкое, что эхо-ответы не приходят в течение интервала ожидания;
5 удаленный хост не существует.

На рисунке 17 показаны результаты выполнения команды «ping» для несуществующего хоста.

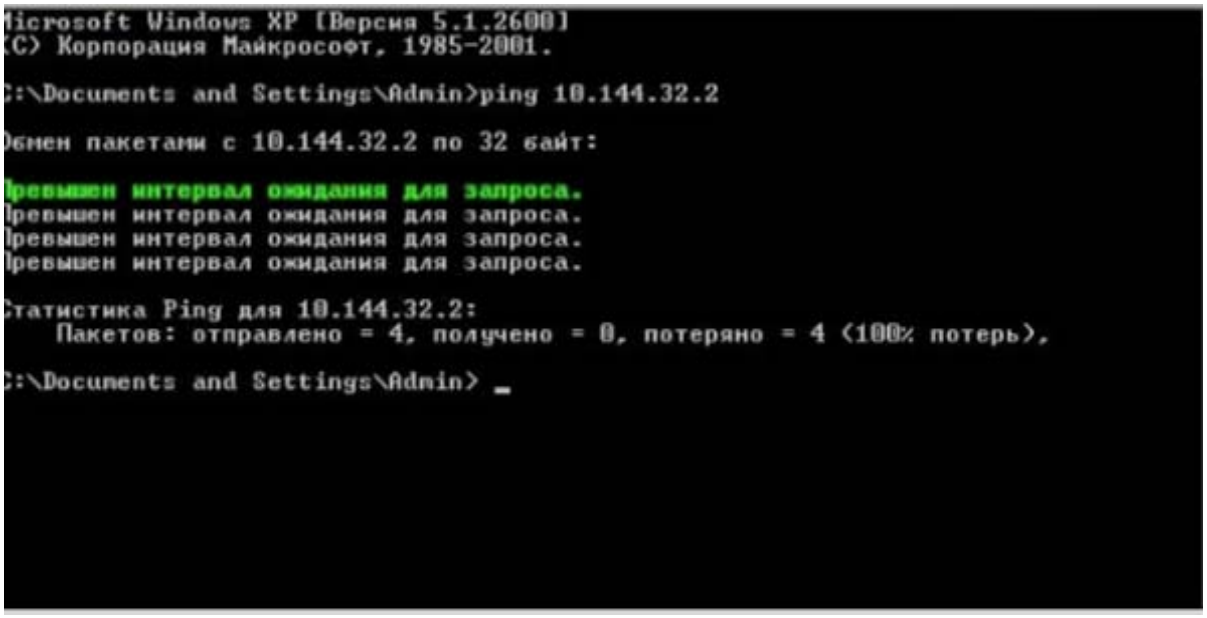


Рисунок 17 – Неудачное выполнение команды «ping»

3 Утилита «traceroute»

Утилита «traceroute» определяет путь, по которому проходят пакеты между локальным и удалённым устройствами. Полученный путь представляет собой список ближайших интерфейсов устройств, работающих на сетевом уровне, находящихся на пути между устройствами. Утилита используется для локализации проблем, или для сбора информации о наличии устройств в сети. Работа утилиты, так же как и работа утилиты «ping», основана на отправке эхо-запросов.

Синтаксис ввода:

tracert [-d] [-h число] [имя_конечного_устройства]

При вводе команды могут использоваться ключи (дополнительные параметры). Список наиболее часто употребляемых параметров представлен в таблице 18.

Таблица 18 – Список наиболее часто употребляемых ключей при вызове утилиты «traceroute»

Ключ	Описание
/d	Предотвращает попытки команды tracert разрешения IP-адресов промежуточных устройств в имена. Увеличивает скорость вывода результатов команды tracert.
/h	Задает максимальное количество переходов на пути при поиске удалённого устройства.
/?	Отображает справку в командной строке.

На рисунке 18 показан результат выполнения команды «tracert» до информационного ресурса *www.ya.ru*.

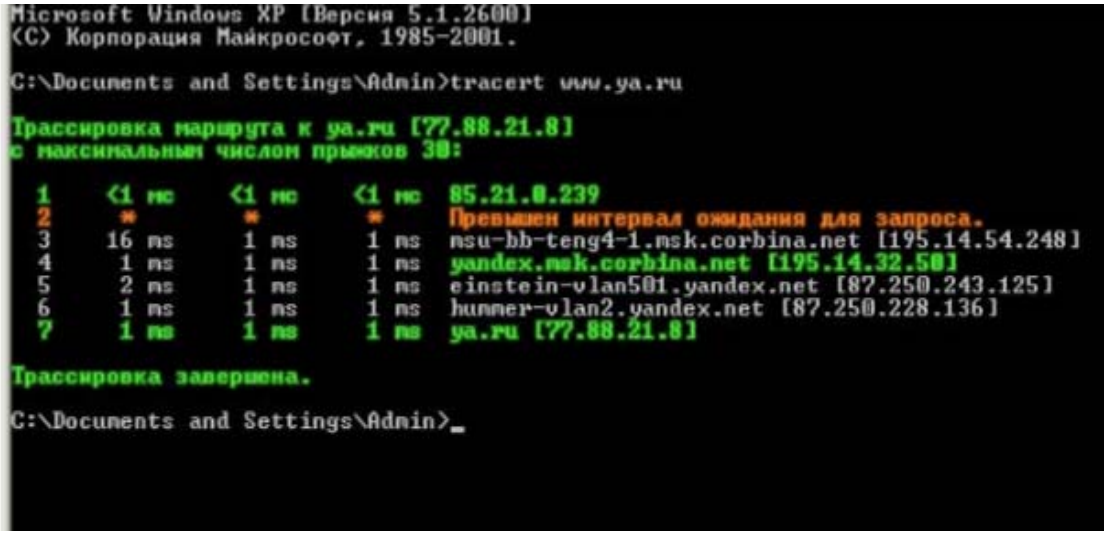


Рисунок 18 – Результаты трассировки до информационного ресурса www.ya.ru

Полученные результаты можно интерпретировать следующим образом.

«Трассировка маршрута к ya.ru [77.88.21.8] с максимальным числом прыжков 30:» – локальное устройство начало посылать удалённому устройству эхо-запросы. Максимальное количество промежуточных устройств, которые могут встретиться на пути, равно 30. Если количество промежуточных устройств превысит 30 – трассировка окажется неудачной.

Далее следует вывод ответов, полученных от промежуточных устройств. Формат вывода выглядит следующим образом:

X Y Y Y Имя [IP-адрес],

где X – номер промежуточного устройства;

Y – время через которое получен эхо-ответ от промежуточного устройства (3 эхо-запроса отправляются последовательно). В случае, если эхо-ответ не получен по истечении интервала ожидания, вместо времени выводится * (астерик);

Имя – DNS имя промежуточного устройства;

IP-адрес – сетевой адрес промежуточного устройства. В случае, если DNS имя промежуточного устройства невозможно получить, выводится только сетевой адрес.

Ниже приведена интерпретация записи рисунка 4.

– «4 1 ms 1 ms 1 ms yandex.msk.corbina.net [195.14.32.50]» – получены все три эхо-ответа от первого промежуточного устройства. Время отклика во всех 3х случаях не превышает 1 миллисекунду.

– Сетевой адрес устройства 195.14.32.50.

– Имя устройства yandex.msk.corbina.net.

4 Утилита «arp»

Служит для вывода и изменения записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet. Для каждого сетевого адаптера Ethernet, установленного в компьютере, используется отдельная таблица.

Синтаксис ввода:

arp [-a [IP_адрес] [-N MAC_адрес]]

При вводе команды могут использоваться ключи (дополнительные параметры). Список наиболее часто употребляемых параметров представлен в таблице 19.

Таблица 19 – Список наиболее часто употребляемых ключей при вызове утилиты «arp»

Ключ	Описание
/a	Вывод содержимого ARP всех адаптеров.
/N	Вывод содержимого ARP кэша определённого адаптера.
/?	Отображает справку в командной строке.

На рисунке 19 показан результат выполнения команды «arp».

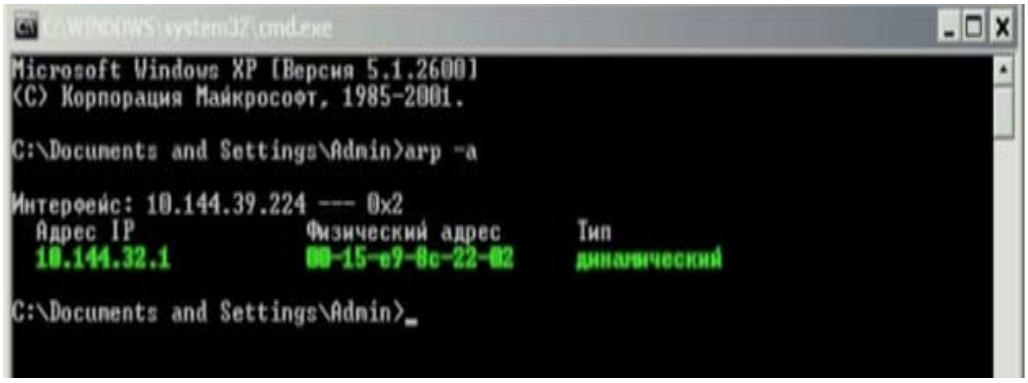


Рисунок 19 – Результат выполнения команды «arp»

Полученные результаты можно интерпретировать следующим образом:

– устройство с сетевым адресом (адрес IP) 10.144.32.1 и физическим адресом 00-15-e9-8c-22-02;

– «Тип Динамический» – данная запись была создана автоматически, когда локальному устройству понадобилось обратиться к устройству с адресом 10.144.32.1. Если в течение 5 минут после создания записи устройства не будут взаимодействовать – запись будет удалена.

Задания:

Отчет выполнения работы должен содержать скришоты этапов выполнения заданий.

1 С помощью утилиты «ipconfig» определить и записать в отчет следующую информацию:

– название сетевого подключения;

– тип используемого адаптера;

– MAC-адрес адаптера;

– IP-адрес сетевого подключения;

– сетевую маску;

– основной шлюз;

– IP-адрес DNS-сервера;

– IP-адрес DHCP-сервера.

2 С помощью утилиты «ping» проверить доступность следующих устройств:

– сервер DHSP;

– сервер DNS;

– информационный ресурс kgsu.ru.

Используя дополнительные ключи, сделать так, чтобы количество посылаемых эхо-запросов равнялось вашему номеру в списке + 5. Для каждого устройства и информационного ресурса записать в отчёт следующую информацию:

– процент потерь;

– среднее время приёма передачи.

3 С помощью утилиты «tracert» проверить доступность следующих устройств:

– информационный ресурс www.kgsu.ru;

– информационный ресурс www.ya.ru.

Используя дополнительные ключи, сделать так, чтобы утилита не определяла DNS имена промежуточных устройств. Записать в отчёт следующую информацию:

– количество промежуточных устройств;

– IP-адрес всех промежуточных устройств.

4 С помощью команды «arp» определить и записать в отчет MAC-адреса следующих устройств:

– основной шлюз;

– 3 любых компьютера.

6 Ответить на контрольные вопросы:

1 Команда «DIR» и ее возможности.

2 Получение информации о конкретной команде.

3 Использование команды «COPY».

4 Как можно объединить несколько файлов в один?

5 Основные утилиты для диагностики сети.

6 Что такое «прыжок (хоп)» в результатах выполнения утилиты «TRACERT»?

7 Для чего используется утилита «PING»?

8 В чем отличие утилит «PING» и «TACERT»?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Галатенко В. А. Основы информационной безопасности : курс лекций / В. А. Галатенко. – Москва : Интернет-Университет Информационных технологий, 2006. – 208 с.

2 Куприянов А. И. Основы защиты информации / А. И. Куприянов. – Москва : Издательский центр «Академия», 2009. – 256 с.

3 Мельников В. П. Информационная безопасность и защита информации / В. П. Мельников. – Москва : Издательский центр «Академия», 2008. – 336 с.

4 Методические указания к выполнению лабораторных работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». Часть 1 / В. В. Москвин, Е. Н. Полякова. – Курган : Изд-во Курганского гос. ун-та, 2017. – 52 с.

5 Методические указания к выполнению лабораторных работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». Часть 2 / В. В. Москвин, Е. Н. Полякова. – Курган : Изд-во Курганского гос. ун-та, 2017. – 41 с.

6 Новоструев А. В. Тезаурус в сфере информационной безопасности / А. В. Новоструев, В. М. Солодвников, А. А. Терентьева : учебное пособие. – Курган : Изд-во Курганского гос. ун-та, 2014. – 471 с.

7 Основы информационной безопасности / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия-Телеком, 2006.

8 Расторгуев С. П. Основы информационной безопасности / С. П. Расторгуев. – Москва : Издательский центр «Академия», 2009.

9 Стандарты информационной безопасности : методические указания к практическому занятию для студентов направлений 10.05.03 и 10.03.01 / сост. В. В. Москвин. – Курган : Изд-во Курганского гос. ун-та, 2018. – 29 с.

10 Ярочкин В. И. Информационная безопасность / В. И. Ярочкин. – Москва : Академический проект, 2008. – 544 с.

Рекомендуемые источники

1 Астахова А. В. Информационные системы в экономике и защита информации на предприятиях – участниках ВЭД: учеб. пособие / А. В. Астахова. – Санкт-Петербург : Троицкий мост, 2014.

2 Груздева Л. М. Информационные технологии в профессиональной деятельности: метод. указания по выполнению практических работ /

Л. М. Груздева, С. Л. Лобачев, А. А. Чеботарева. – Москва : Юридический институт МИИТа, 2015.

3 Информационные технологии в юридической деятельности / под ред. В. Д. Элькина. – Москва : Издательство «Юрайт», 2013.

4 Информационные технологии в юриспруденции: учеб. пособие / под ред. С. Я. Казанцев. – 2-е изд., перераб. и доп. – Москва : Академия, 2012.

5 Карпов В. И. Основы теории обеспечения безопасности личности, общества и государства: учеб. пособие / В. И. Карпов, О. Н. Новокшанов, Д. Б. Павлов. – Москва : Юридический институт МИИТа, 2010.

6 Мельников В. П. Информационная безопасность и защита информации: учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – 6-е изд. – Москва : Академия, 2012.

7 Чеботарева А. А. Информационное право : учеб. пособие / А. А. Чеботарева. – Москва : Юридический институт МИИТа, 2014.

СОДЕРЖАНИЕ

Человечкова Анна Владимировна

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические рекомендации
к выполнению практических работ
по дисциплине «Основы информационной безопасности»
для студентов очной формы обучения
10.05.03 «Информационная безопасность автоматизированных систем»,
09.03.03 «Прикладная информатика»,
09.03.04 «Программная инженерия»

Редактор В. А. Лисина

БИЦ Курганского государственного университета.
640020, г. Курган, ул. Советская, 63/4.
Курганский государственный университет.