Областное бюджетное профессиональное образовательное учреждение
«Курский электромеханический техникум»
(ОБПОУ «КЭМТ»)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по учебной дисциплине
ОП.13 Технические методы и средства защиты информации
для студентов специальности
09.02.01 Компьютерные системы и комплексы
(базовая подготовка, очная форма обучения)

Разработчик: Севрюкова Любовь Анатольевна,
преподаватель высшей квалификационной
категории ОБПОУ «КЭМТ»

2020

РАССМОТРЕНЫ
на заседании предметной (цикловой)
комиссии преподавателей профессионального
цикла по направлению подготовки
«Информатика и вычислительная техника»
Протокол № 7 от 17 января 2020 г.
Председатель П(Ц)К
_____ Ж.Н. Савенкова

Заведующая информационно-
компьютерным отделением
_____ И.В. Моршнева
«20» января 2020 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по учебной дисциплине
ОП.13 Технические методы и средства защиты информации
для студентов специальности
09.02.01 Компьютерные системы и комплексы
(базовая подготовка, очная форма обучения)

Разработчик: _____ Л.А. Севрюкова, преподаватель высшей квалификационной категории ОБПОУ «КЭМТ»

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина ОП.13 Технические методы и средства защиты информации является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.01 Компьютерные системы и комплексы, входящей в состав укрупненной группы специальностей 09.00.00 Информатика и вычислительная техника.

На учебную дисциплину отводится 72 аудиторных часа из них 36 часов – это практические занятия. Поэтому данная методическая разработка предназначена для проведения этих занятий.

Методические указания по выполнению практических работ по учебной дисциплине ОП.13 Технические методы и средства защиты информации разработаны для студентов второго курса специальности 09.02.01 Компьютерные системы и комплексы.

Задачей данной разработки является формирование практических навыков организации и проведения мероприятий по защите информации в компьютерных системах и комплексах.

Методическая разработка состоит из 18 практических работ, содержащих краткую теоретическую справку, задания для аудиторной работы, задания для самостоятельной работы, контрольные вопросы. На выполнение каждой работы отводится два аудиторных часа.

Самостоятельная работа представлена в двух вариантах с заданиями разных уровней сложности.

Для получения отметки «отлично», студент должен выполнить аудиторную работу и самостоятельную работу, состоящую из частей А, В, С. Отметка «хорошо» выставляется, если выполнена аудиторная работа и правильно решены часть А и В. «Удовлетворительно» студент получает, при правильно решенной аудиторной работе и части А в самостоятельной работе. Отметка «неудовлетворительно» ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя описание выполненных заданий;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Полученные практические навыки будут способствовать освоению студентами их профилирующих учебных дисциплин.

В результате освоения учебной дисциплины ОП.13 Технические методы и средства защиты информации студенты должны приобрести умения и знания, которые способствуют формированию профессиональных и общих компетенций.

Студент должен уметь:

– использовать средства операционных систем и сред для решения практических задач;

– использовать сервисные средства, поставляемые с операционными системами;

– решать задачи обеспечения защиты операционных систем;

– проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов;

– проводить системотехническое обслуживание компьютерных систем и комплексов.

знать:

– основные функции операционных систем;

– сопровождение операционных систем;

– особенности контроля и диагностики устройств аппаратно-программных систем;

– основные методы диагностики;

– аппаратное и программное конфигурирование компьютерных систем и комплексов;

– приемы обеспечения устойчивой работы компьютерных систем и комплексов.

1. ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ

№ п/п	Наименование практической работы (тема)	Количество аудиторных часов
1	2	3
1	Анализ методов и средств защиты информации и их классификации	2
2	Анализ физических методов и средств защиты информации и их классификации	2
3	Анализ программно-технических методов и средств защиты информации и их классификации. Создание дискреционной модели безопасности	2
4	Создание скрытой информации. Установка паролей	2
5	Разграничение прав доступа для пользователей локального компьютера и локальной сети	2
6	Настройка параметров политики аудита для событий	2
7	Настройка параметров политики аудита для локальных папок и файлов	2
8	Настройка параметров политики безопасности операционной системы	2
9	Архивация и восстановление системы	2
10	Предотвращение и исправление ошибок жесткого диска	2
11	Использование программы CrystalDiskInfo для проверки жесткого диска	2
12	Восстановление данных программными средствами	2
13	Дефрагментация носителей информации	2
14	Кодирование текстовой информации	2
15	Шифрование информации симметричными методами	2
16	Шифрование информации асимметричными методами	2
17	Установка и настройка параметров антивирусного программного обеспечения	2
18	Исследование работы антивирусного программного обеспечения	2
	Итого	36

Практическая работа № 1
Анализ методов и средств защиты информации и их классификации

Цель: выполнить анализ методов и средств защиты информации, выявить их достоинства и недостатки, проанализировать классификацию и особенности применения методов и средств защиты информации.

Средства обучения:

- методические рекомендации к практической работе № 1;
- персональный компьютер преподавателя;
- проектор.

Виды самостоятельной работы:

- анализ угроз информационной безопасности;
- анализ средств и методов защиты информации;
- анализ классификации средств и методов защиты информации.

Краткая теоретическая справка

Для защиты информации требуется организация целого комплекса мер, т.е. использование специальных средств, методов и мероприятий с целью предотвращения потери информации.

На общегосударственном уровне защита информации должна обеспечиваться в соответствии с концепцией национальной безопасности Российской Федерации, сформулированной в Федеральном законе «Об информации, информатизации и защите информации».

Объектом защиты может быть информация, ее носитель, информационный процесс, в отношении которого необходимо проводить защиту в соответствии с поставленными целями.

Угрозы безопасности информации

Под угрозой информационной безопасности в компьютерной системе понимают события или действия, которые могут вызвать изменения функционирования компьютерной системы, связанные с нарушением защищенности информации, обрабатываемой в ней.

Угрозы информационной безопасности могут быть случайными (непреднамеренными) или умышленными.

Умышленные угрозы делятся на пассивные и активные.

Источники случайных или непреднамеренных угроз:

- ошибки в программном обеспечении;
- выходы из строя аппаратных средств;
- неправильные действия пользователей.

Умышленные угрозы – преследуют цель нанесения ущерба пользователям компьютерных систем.

Пассивные угрозы – направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на функционирование компьютерной системы.

Активные угрозы – имеют целью нарушение нормального процесса функционирования компьютерной системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

Основные угрозы безопасности информации:

– раскрытие конфиденциальности информации (несанкционированный доступ к базам данных, прослушивание каналов и т.д.);
– компрометация информации;
– несанкционированное использование информационных ресурсов;
– ошибочное использование информационных ресурсов;
– несанкционированный обмен информацией и т.д.

Пути несанкционированного доступа к информации:

– перехват электронных излучений;
– применение подслушивающих устройств;
– хищение носителей информации и документальных отходов;
– чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
– копирование носителей информации с преодолением мер защиты;
– маскировка под зарегистрированного пользователя;
– использование программных ловушек;
– незаконное подключение к аппаратуре и линиям связи;
– внедрение и использование компьютерных вирусов и т.д.

Средства защиты информации

1. Инженерно-технические средства – реализуются в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на:

– аппаратные – устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой систем обработки данных по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры);

– физические – реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения и т.п.);

– программные средства – программы, специально предназначенные для выполнения функций, связанных с защитой информации;

– криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

2. Организационно-правовые средства – законодательные и нормативные документы в области информационной безопасности, которые на правовом уровне должны регулировать доступ к информации со стороны потребителей.

3. Морально-этические средства включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются.

Методы защиты информации

1. Управление доступом. Включает следующие функции защиты:

– идентификацию пользователя (присвоение персонального имени, кода, пароля и опознание пользователя по предъявленному идентификатору);

– проверку полномочий, соответствие дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту;

– разрешение и создание условий работы в пределах установленного регламента;

– регистрацию обращений к защищаемым ресурсам;

– реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

– криптографическое шифрование – готовое к передаче сообщение (текст, речь, графика) зашифровывается, т.е. преобразуется в шифрограмму.

Шифрование может быть симметричным и асимметричным.

Симметричное основывается на использовании одного и того же секретного ключа для шифрования и дешифрования.

Асимметричное характеризуется тем, что для шифрования используется один ключ, являющийся общедоступным, а для дешифрования – другой, являющийся секретным.

2. Механизм цифровой (электронной) подписи, основывающийся на алгоритмах асимметричного шифрования и включающий две процедуры: формирование подписи отправителя и ее распознавание (верификацию) получателем.

3. Механизмы контроля доступа осуществляют проверку полномочий объектов ИС (программ и пользователей) на доступ к ресурсам сети.

4. Механизмы обеспечения целостности данных (например, отправитель дополняет передаваемый блок данных криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке).

5. Механизмы управления маршрутизацией обеспечивает выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам и др.

Аудиторная работа

1. Дайте понятие защищаемой информации.
2. Перечислите виды угроз.
3. Дайте характеристику каждого вида угроз.
4. Дайте характеристику средств защиты информации.
5. Дайте характеристику методов защиты информации.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Определите, какая информация относится к защищаемой?

Задание 2. Перечислите виды угроз.

Задание 3. Дайте понятие организационно-правовых средств защиты информации.

Часть В

Задание 4. Заполните следующую таблицу. Впишите в пустые ячейки соответствующие виды угроз.

Виды угроз

Случайные угрозы	Умышленные угрозы	
	Пассивные	Активные

Часть С

Задание 5. Разработайте и начертите схему «Классификация средств защиты информации».

Задание 6. Заполните следующую таблицу:

Виды технических средств и их назначение

Виды технических средств	Средства, относящиеся к данному виду	Цель использования данных средств	Примеры средств

Вариант 2

Часть А

Задание 1. Перечислите объекты информационной системы, нуждающиеся в защите.

Задание 2. Какие угрозы называются случайными?

Задание 3. Дайте понятие морально-этических средств защиты информации.

Часть В

Задание 4. Предложенные ниже действия распределите по видам угроз безопасности информации, к которым они относятся. Задание оформите в виде таблицы.

1. Просмотр информации.
2. Скачивание информации.
3. Разглашение сведений, считанных из памяти информационной системы.
4. Дезорганизация работы информационной системы.
5. Блокирование информации.
6. Искажение информации.
7. Подмена программных ресурсов.
8. Использование программных ресурсов для создания информации разных типов.
9. Установка программных продуктов.
10. Уничтожение информации.

Часть С

Задание 5. Разработайте и начертите схему «Классификация методов защиты информации».

Задание 6. Заполните следующую таблицу:

Виды технических средств и их назначение

Виды технических средств	Средства, относящиеся к данному виду	Цель использования данных средств	Примеры средств

Контрольные вопросы:

1. Какую цель преследует защита информации?
2. Что понимают под эффективностью защиты информации?
3. Какие угрозы называются умышленными?
4. Какие угрозы называются пассивными?
5. Какие угрозы называются активными?
6. Что называется защитой информации?
7. Что представляет собой система защиты информации?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 2
Анализ методов и средств физической защиты информации и их классификации

Цель: выполнить анализ методов и средств физической защиты информации, выявить их достоинства и недостатки, проанализировать классификацию и особенности применения методов и средств физической защиты информации.

Средства обучения:

– методические рекомендации к практической работе № 2;

– персональный компьютер преподавателя;

– проектор.

Виды самостоятельной работы:

– анализ методов и средств физической защиты информации;

– анализ классификации средств и методов физической защиты информации.

Краткая теоретическая справка

Физические средства защиты – это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников.

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз.

По физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

– охранные и охранно-пожарные системы;

– охранное телевидение;

– охранное освещение;

– средства физической защиты.

Охранные системы

Охранные системы и средства охранной сигнализации предназначены для обнаружения попыток проникновения на объект защиты, в охраняемые зоны и помещения; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения.

Важнейшими элементами охранных систем являются датчики, обнаруживающие появление угрозы.

Датчики посредством каналов связи соединены с контрольно-приемным устройством пункта охраны и средствами тревожного оповещения.

Охранное телевидение

Особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя.

Источниками изображения (датчиками) в системах охранного телевидения являются видеокамеры.

Вторым по значимости элементом системы охранного телевидения является монитор. Часто используется один монитор с несколькими камерами, подсоединяемыми к нему поочередно средствами автоматического переключения по определенному регламенту.

Охранное освещение

Обязательной составной частью системы защиты любого объекта является охранное освещение. Различают два вида охранного освещения – дежурное и тревожное.

Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время – как на территории объекта, так и внутри здания.

Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и др.).

Защита элементов зданий и помещений

Хорошую физическую защиту оконных проемов помещений обеспечивают традиционные металлические решетки, а также специальное остекление на основе пластических масс, армированных стальной проволокой. Двери и окна охраняемого помещения оборудуются датчиками, срабатывающими при разрушении стекол, дверей, но не реагирующими на их колебания, вызванные другими причинами. Срабатывание датчиков вызывает сигнал тревоги.

Запирающие устройства

Запирающие устройства и специальные шкафы занимают особое место в системах ограничения доступа, поскольку они несут в себе признаки как систем физической защиты, так и устройств контроля

доступа. Они отличаются большим разнообразием и предназначены для защиты документов, материалов, магнитных и фотоносителей а также технических средств: ПЭВМ, калькуляторов, принтеров, ксероксов и др.

К запирающим устройствам можно отнести:

– специальные металлические шкафы для хранения ПЭВМ и другой техники. Такие шкафы снабжаются надежной двойной системой запирания: замком ключевого типа и трех- пятизначным комбинированным замком.

– замки с программируемым временем открывания с помощью механических или электронных часов.

Системы контроля доступа

Регулирование доступа в помещения или здания осуществляется, прежде всего, посредством опознавания службой охраны или техническими средствами.

Основанием допуска служит определенный метод опознавания и сравнения с разрешительными параметрами системы.

Наиболее распространенными являются атрибутные и персональные методы опознавания.

К атрибутным способам относятся средства подтверждения полномочий, такие, в частности, как документы (паспорт, удостоверение и др.), карты (фотокарточки, карты с магнитными, электрическими, механическими идентификаторами и др.) и иные средства (ключи, сигнальные элементы и др.).

Персональные методы – это методы определения лица по его независимым показателям: отпечаткам пальцев, геометрии рук, особенностям глаз и др. Персональные характеристики бывают статическими и динамическими.

Персональные способы наиболее эффективные. Во-первых, они полно описывают каждого отдельного человека. Во-вторых, невозможно или крайне трудно подделать индивидуальные характеристики.

Статические способы включают анализ физических характеристик – таких как отпечатки пальцев, особенности геометрии рук и др. Они достаточно достоверны и обладают малой вероятностью ошибок.

Динамические же способы используют изменяющиеся во времени опознавательные характеристики.

Способ опознавания человеком (вахтер, часовой) не всегда надежен из-за так называемого человеческого фактора, заключающегося в том, что человек подвержен влиянию многих внешних условий (усталость, плохое самочувствие, эмоциональный стресс, подкуп и др.). В противовес этому

находят широкое применение технические средства опознавания, такие, например, как идентификационные карты, опознавание по голосу, почерку, пальцам и др.

Обычно это пластиковые карты типа пропусков или жетонов. Карты вводятся в читающее устройство каждый раз, когда требуется войти или выйти из охраняемого помещения или получить доступ к чему-нибудь (сейфу, камере, терминалу и др.)

Системы опознавания по отпечаткам пальцев

В основу идентификации положено сравнение относительного положения окончаний и разветвлений линий отпечатка. Поисковая система ищет на текущем изображении контрольные элементы, определенные при исследовании эталонного образца. Для идентификации одного человека считается достаточным определение координат 12 точек.

Системы опознавания по голосу

Существует несколько способов выделения характерных признаков речи человека: анализ кратковременных сегментов, контрольный анализ, выделение статистических характеристик.

Системы опознавания по почерку

Системы опознавания по почерку считаются наиболее удобными для пользователя. Основным принципом идентификации по почерку является постоянство подписи каждого индивидуума, хотя абсолютного совпадения не бывает.

Система опознавания по геометрии рук

Для идентификации применяют анализ комбинации линий сгибов пальцев и ладони, линий складок, длины и толщины пальцев и др.

Технически это реализуется путем наложения руки на матрицу фотоячеек. Рука освещается мощной лампой, производится регистрация сигналов с ячеек, несущих информацию о геометрии.

Аудиторная работа

1. Дайте характеристику физических средств защиты информации.
2. Опишите классификацию физических средств защиты информации.
3. Дайте характеристику охранных и охранно-пожарных систем.
4. Дайте характеристику охранного телевидения.
5. Дайте характеристику охранного освещения.
6. Дайте характеристику систем контроля доступа.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Определите основное назначение физических средств защиты информации.

Задание 2. Дайте характеристику запирающих устройств.

Часть В

Задание 3. Физические системы защиты можно разделить на три основные группы. Схема представлена на рисунке.

Под каждой группой физических систем расположите перечисленные ниже задачи, которые решает данная группа систем:

– обеспечивает защиту объектов по периметру;

– реализует защиту документов, данных, файлов;

– обеспечивает защиту с использованием различных систем шкафов и хранилищ;

– реализует контроль проникновения на охраняемые территории;

– обеспечивает защиту зданий, помещений;

– обеспечивает защиту с использованием различных систем запирающих устройств;

– обеспечивает защиту элементов зданий и помещений.

Задание 4. Разработайте и начертите схему «Классификация систем контроля доступом».

Часть С

Задание 5. Заполните следующую таблицу:

Физические средства и системы защиты информации					
№ п/п	Группы средств или систем	Подгруппы средств или систем	Назначение	Основные элементы	Технология работы

Вариант 2

Часть А

Задание 1. Перечислите основные задачи физических средств защиты информации.

Задание 2. Перечислите надежные системы контроля доступа.

Часть В

Задание 3. Разработайте и начертите схему «Классификация физических средств защиты информации».

Задание 4. Выполните сравнительный анализ охранного телевидения и охранного освещения. Оформите анализ в виде таблицы.

Часть С

Задание 5. Заполните следующую таблицу:

Физические средства и системы защиты информации					
№ п/п	Группы средств или систем	Подгруппы средств или систем	Назначение	Основные элементы	Технология работы

Контрольные вопросы:

1. Что представляют собой физические средства защиты?
2. Каким недостатком обладает охранное освещение?
3. Почему способ «опознавание человеком» является не всегда надежным?
4. Какие способы контроля доступа не обеспечивают надежной защиты и почему?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 3
Анализ программно-технических методов и средств защиты информации и их классификации.
Создание дискреционной модели безопасности

Цель: проанализировать программно-технические методы и средства защиты информации, выявить их достоинства и недостатки, провести анализ классификации;

выполнить анализ принципов построения моделей разграничения доступа;

создать дискреционную модель разграничения доступа.

Средства обучения:

– методические рекомендации к практической работе № 3;

– персональные компьютеры;

– проектор.

Виды самостоятельной работы:

– анализ программно-технических средств и методов защиты информации;

– анализ классификации программно-технических средств и методов защиты информации;

– создание дискреционной модели разграничения доступа для стандартной КС с помощью средств операционной системы.

Краткая теоретическая справка

Модели безопасности компьютерных систем

Создание безопасности компьютерных систем сводится к разработке набора правил, определяющих множество допустимых действий в системе (политики безопасности). Системы, функционирующие в соответствии со строго определенным набором формализованных правил и реализующие какую-либо политику безопасности, называются моделями безопасности.

К наиболее эффективным и используемым в настоящее время моделям безопасности относятся модели систем: 1) дискреционного; 2) мандатного; 3) ролевого разграничения доступа. При описании моделей безопасности используют понятия субъект и объект. Под субъектом понимается индивид или группа индивидов, объект – защищаемая информация, чаще всего представленная в виде файлов, реже – в виде настроек различных систем и пр.

Модель систем дискреционного разграничения доступа характеризуется разграничением доступа между поименованными

субъектами и объектами. Для каждого субъекта должно быть задано явное и недвусмысленное перечисление допустимых операций (читать, писать и т. д.) над конкретным объектом. Субъект с определенным правом доступа к объекту может передать это право любому другому субъекту. Возможны, по меньшей мере, два подхода к построению дискреционного управления доступом: 1) каждый объект системы имеет привязанного к нему субъекта (владельца), который устанавливает права доступа к данному объекту; 2) система имеет одного выделенного субъекта – суперпользователя, который имеет право устанавливать права владения для всех остальных субъектов системы.

Модель систем мандатного разграничения доступа – это модель, в которой каждому субъекту и объекту присваиваются классификационные метки, отражающие место данного субъекта (объекта) в соответствующей иерархии. Посредством этих меток субъектам и объектам назначаются классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Для доступа субъекта к объекту первый должен предоставить системе классификационные метки этого объекта.

При организации мандатного принципа контроля возможны следующие подходы: 1) субъект может читать объект, только если иерархическая классификация субъекта не меньше, чем иерархическая классификация объекта, и неиерархические категории субъекта включают в себя все иерархические категории объекта; 2) субъект осуществляет запись в объект, только если классификационный уровень субъекта не больше, чем классификационный уровень объекта, и все иерархические категории субъекта включаются в неиерархические категории объекта.

Ролевое разграничение доступа представляет собой развитие политики дискреционного разграничения доступа, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли – совокупность прав доступа на объекты компьютерной системы. Задание ролей позволяет определить более четкие и понятные для пользователей компьютерной системы правила разграничения доступа. Такой подход часто используется в системах, для пользователей которых четко определен круг их должностных полномочий и обязанностей.

Классификация программно-технических методов и средств защиты информации

Для создания на предприятии (организации и пр.) безопасной информационной системы, необходимо, прежде всего, обеспечить работоспособность всех классов программно-технических методов и средств защиты информации:

- средства защиты от несанкционированного доступа (средства авторизации, мандатное управление доступом, избирательное управление доступом, управление доступом на основе ролей, аудит);
- системы анализа и моделирования информационных потоков;
- системы мониторинга сетей (системы обнаружения и предотвращения вторжений, системы предотвращения утечек конфиденциальной информации);
- анализаторы протоколов;
- антивирусные средства;
- межсетевые экраны;
- криптографические средства (шифрование, цифровая подпись);
- системы резервного копирования;
- системы бесперебойного питания (источники бесперебойного питания, резервирование нагрузки, генераторы напряжения);
- системы аутентификации (пароль, ключ доступа (физический или электронный), сертификат, биометрия);
- средства предотвращения взлома корпусов и краж оборудования;
- средства контроля доступа в помещение;
- инструментальные средства анализа систем защиты (мониторинговый программный продукт).

Безопасность на уровне операционных систем

Для защиты компьютерных систем необходимы усиленные меры идентификации и аутентификации пользователей, но в первую очередь необходимо все же обеспечить защиту с помощью встроенных средств операционной системы (ОС). Настройка средств безопасности осуществляется в соответствии с политикой безопасности – шаблоном, по которому можно выбирать и конфигурировать различные типы механизмов защиты, поддерживаемых операционной системой или ее приложениями, в соответствии с некоторой моделью разграничения доступа. В политике безопасности предписано каждого пользователя системы классифицировать по группам, что осуществляется посредством создания учетных записей пользователей – записей, содержащих все

сведения, определяющие пользователей в ОС. К этим сведениям относятся: имя пользователя и пароль, требуемые для входа пользователя в систему, имена групп, членом которых пользователь является, а также права и разрешения, которые он имеет при работе в системе и доступе к ее ресурсам. Существует минимум пять групп пользователей:

1. Администраторы (имеют полный доступ на управление компьютером);
2. Операторы архива (могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы, не могут изменять параметры безопасности);
3. Опытные пользователи (могут создавать учетные записи и группы пользователей, изменять и удалять созданные ими учетные записи и группы пользователей, создавать локальные группы и удалять пользователей из локальных групп, которые они создали, удалять пользователей из групп «Опытные пользователи», «Пользователи» и «Гости»);
4. Пользователи (могут выполнять наиболее распространенные задачи, например, запуск приложений, использование локальных и сетевых принтеров и т. д.);
5. Гости (для пользователей, не имеющих собственных учетных записей на компьютере).

При добавлении учетной записи пользователя его, как правило, относят к некоторой группе, тем самым пользователю предоставляются все разрешения и права, назначенные этой группе. На одном компьютере может быть создано неограниченное число учетных записей. Для добавления на компьютер нового пользователя или изменения учетной записи существующего пользователя необходимо войти в систему с учетной записью «Администратор» (или члена группы «Администраторы») (Пуск/ Панель управления/Администрирование/Управление компьютером/ Локальные пользователи и группы/Пользователи) и в окне со списком пользователей осуществить нужную операцию. Средствами реализации учетных записей пользователей обеспечивается защита от несанкционированного доступа к информации злоумышленника при его непосредственном контакте с системой. Но существуют угрозы, связанные с несанкционированным доступом к информации по сети. Такой доступ, как правило, осуществляется посредством: вирусов, кейло́геров (ки-ло́гер) (программа, считывающая нажатие клавиш) и радминов (программа, предназначенная для удаленного администрирования, но при этом может

использоваться для доступа к скрытой информации). Важно помнить, что как бы хорошо ни была защищена ОС, в ней периодически находятся уязвимые места, которыми может воспользоваться злоумышленник. В ОС Windows существует средство автоматического обновления, которое позволяет в автоматическом режиме устанавливать самые «свежие» обновления. Для включения автоматического обновления необходимо выполнить команды Пуск/Панель управления/Центр обеспечения безопасности Windows/Автоматическое обновление и выбрать пункт «Автоматически (рекомендуется)», выбрать день недели и время выполнения обновления.

Аудиторная работа

1. Дайте характеристику моделей безопасности.
2. Дайте характеристику программно-технических методов и средств защиты информации.
3. Опишите технологию создания дискреционной модели безопасности.
4. Опишите технологию создания учетной записи.
5. Продемонстрируйте поэтапное создание учетной записи.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Определите понятие модели безопасности.

Задание 2. Дайте характеристику модели мандатного разграничения доступа.

Задание 3. Перечислите программно-технические методы и средства защиты, обеспечивающие эффективную защиту информации.

Часть В

Задание 4. Ознакомьтесь с группами пользователей стандартной КС. Для этого выполните следующие действия:

– выполните включение КС, загрузите операционную систему под именем «Admin» (введите пароль выданный преподавателем);

– откройте диалоговое окно «Управление компьютером» (Пуск/Панель управления/Производительность и обслуживание/ Администрирование/Управление компьютером);

– в этом окне откройте папку «Локальные пользователи»;

– откройте папку «Группы»;

– заполните таблицу (для 6 основных групп):

№ п/п	Название группы	Описание

Задание 5. Откройте папку «Пользователи» и выпишите в отчет действующих пользователей. Закройте окно и вернитесь на панель управления.

Часть С

Задание 6. Создайте две учетные записи: для администрирования (Администратор1) и для работы (фамилия, имя). Установите для учетных записей следующие параметры:

– Администратор1: тип записи – администратор компьютера, пароль – 111111, подсказка – Цифра 1, изображение – по своему усмотрению;

– Рабочая учетная запись: тип записи – ограниченная запись, пароль – 222222, подсказка – Цифра 2, изображение – по своему усмотрению.

Задание 7. Выйдите на рабочий стол и выполните команду Пуск/Сменить пользователя. Проверьте, чтобы созданные вами пользователи отображались в списке пользователей.

Задание 8. Перезагрузите операционную систему для каждой созданной вами учетной записи и установите для каждого пользователя следующие параметры экрана:

– для учетной записи «Администратор1»: фоновый рисунок – Windows XP; заставка – метаморфозы (опции: смена цветов, вращения, превращения, две стороны, плавные оттенки, по сторонам); интервал – 1мин;

– для вашей учетной записи: параметры по вашему усмотрению.

Вариант 2

Часть А

Задание 1. Перечислите основные модели безопасности.

Задание 2. Дайте характеристику модели ролевого разграничения доступа.

Задание 3. Перечислите программно-технические методы и средства защиты, не обеспечивающие эффективную защиту информации.

Часть В

Задание 4. Ознакомьтесь с группами пользователей стандартной КС. Для этого выполните следующие действия:

– выполните включение КС, загрузите операционную систему под именем «Admin» (введите пароль выданный преподавателем);

– откройте диалоговое окно «Управление компьютером» (Пуск/Панель управления/Производительность и обслуживание/ Администрирование/Управление компьютером);

– в этом окне откройте папку «Локальные пользователи»;

– откройте папку «Группы»;

– заполните таблицу (для 6 основных групп):

№ п/п	Название группы	Описание

Задание 5. Откройте папку «Пользователи» и выпишите в отчет действующих пользователей. Закройте окно и вернитесь на панель управления.

Часть С

Задание 6. Создайте две учетные записи: для администрирования (Администратор2) и для работы (фамилия, имя). Установите для учетных записей следующие параметры:

– Администратор2: тип записи – администратор компьютера, пароль – 111111, подсказка – Цифра 1, изображение – по своему усмотрению;

– Рабочая учетная запись: тип записи – ограниченная запись, пароль – 222222, подсказка – Цифра 2, изображение – по своему усмотрению.

Задание 7. Выйдите на рабочий стол и выполните команду Пуск/Сменить пользователя. Проверьте, чтобы созданные вами пользователи отображались в списке пользователей.

Задание 8. Перезагрузите операционную систему для каждой созданной вами учетной записи и установите для каждого пользователя следующие параметры экрана:

– для учетной записи «Администратор2»: фоновый рисунок – Windows XP; заставка – метаморфозы (опции: смена цветов, вращения, превращения, две стороны, плавные оттенки, по сторонам); интервал – 1мин;

– для вашей учетной записи: параметры по вашему усмотрению.

Контрольные вопросы:

1. Что представляет собой субъект для модели безопасности?
2. Что представляет собой объект для модели безопасности?
3. Какими сведениями определяется пользователь в операционной системе?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 4

Создание скрытой информации. Установка паролей

Цель: освоить технологию скрытия информации для ее защиты;

освоить технологии создания паролей с помощью средств операционной системы и внешних средств.

Средства обучения:

- методические рекомендации к практической работе № 4;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- анализ методов и средств скрытия информации;
- создание скрытой информации;
- создание паролей.

Краткая теоретическая справка

Для того, чтобы сделать информацию недоступной для других пользователей можно скрыть папку или файл, в которой она содержится или установить на эту папку пароль.

Создание скрытой папки или файла

Для скрытия папки или файла необходимо вызвать контекстное меню этой папки и выбрать пункт «Свойства». В открывшемся диалоговом окне «Свойства» на вкладке «Общие» установить флажок в опции «Скрытый». После этого система спросит, нужно ли скрыть все содержимое этой папки или только одну папку. Выбирается нужный вариант.

Отображение скрытых папок

Для того чтобы просмотреть скрытые файлы и папки необходимо выполнить последовательность команд Пуск/Панель управления/Свойства папки. В открывшемся диалоговом окне «Свойства папок» нужно перейти на вкладку «Вид» и в меню «Скрытые файлы и папки» отметить опцию «Показывать скрытые файлы и папки». После нажатия кнопки «Применить» все скрытые папки становятся видимыми. Существует также другой способ сделать скрытую папку видимой. Открыть окно «Свойства папки» можно прямо из любого окна открытой папки (рис. 1).

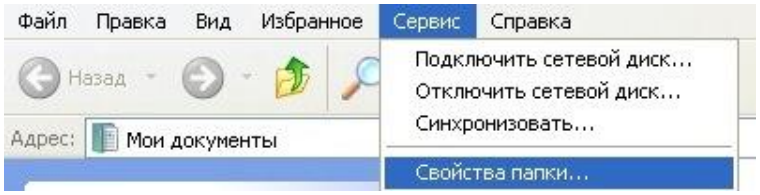

Рис. 1. Скриншот команд пункта меню «Сервис»

Установка паролей

В самой ОС есть возможность устанавливать уровни доступа различным группам пользователей, в том числе в сети. Кроме того, можно создать специальный файл-ключ с паролем и уже через него давать доступ к папкам.

В основном для паролирования папок в ОС используется внешний софт, выполняющий задачи по обеспечению информационной безопасности. В настоящее время существуют десятки бесплатных и платных программ, с помощью которых можно установить пароль на любой документ, архив или папку в системе:

- LocK-A-FoLdeR;
- Folder Lock Lite;
- Folder Protector;
- WinRaR;
- 7-ZIP.

Технология установки пароля на папку:

1. Вызвать контекстное меню папки, которую нужно запаролить и выбрать пункт «Свойства».

2. В открывшемся окне «Свойства папки» выбрать вкладку «Общие», а на ней в разделе «Атрибуты» выбрать кнопку «Другие» (рис. 2).

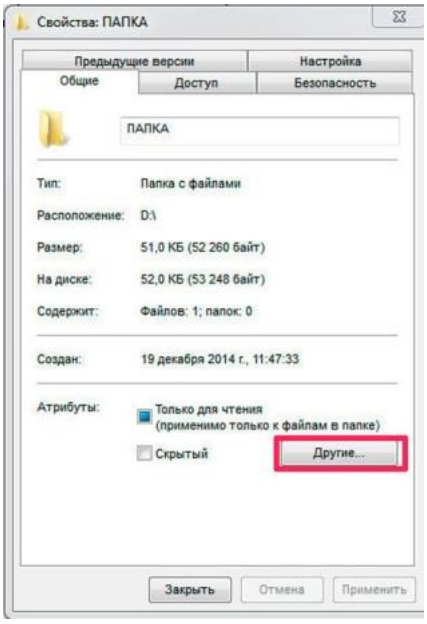

Рис. 2. Диалоговое окно «Свойства папки». Кнопка «Другие»

3. Откроется окно выбора дополнительных атрибутов. Установить флажок в опции «Шифровать содержимое для защиты данных» (рис. 3).

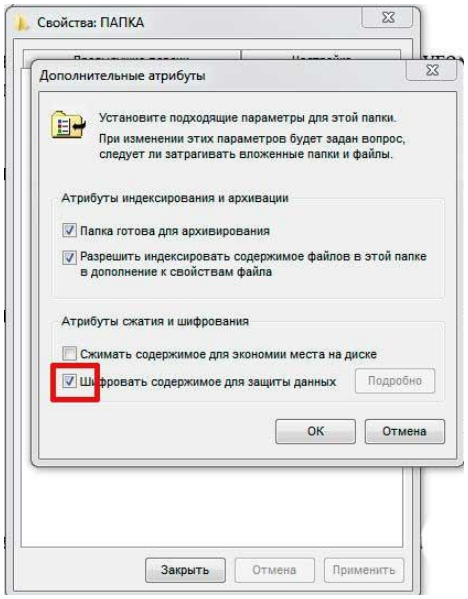

Рис. 3. Диалоговое окно «Дополнительные атрибуты».
Опция «Шифровать содержимое для защиты данных»

4. Подтвердить начало процесса шифрования, выбрав команду «Архивировать сейчас» (рис. 4).

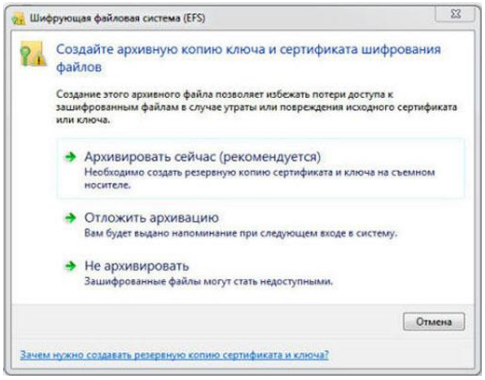

Рис. 4. Диалоговое окно «Шифрующая файловая система»

5. Дальше произойдёт автоматический запуск экспорта сертификатов.

6. В следующем окне отметить переключатель выбора расширения PFX файла-ключа (рис. 5).

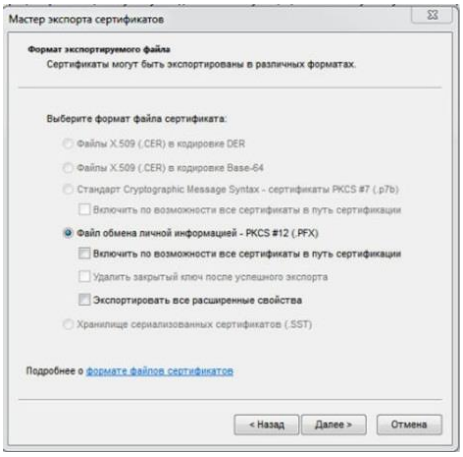

Рис. 5. Диалоговое окно «Мастер экспорта сертификатов»

7. Задать пароль для файла-ключа (рис. 6).

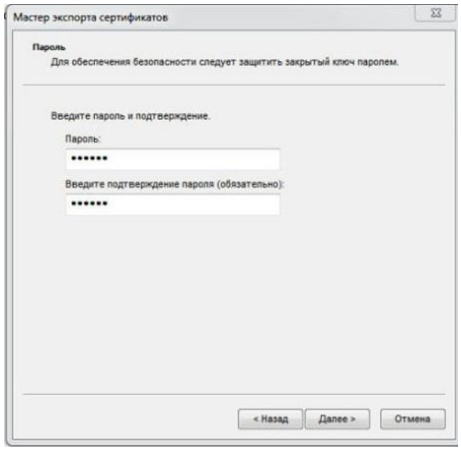

Рис. 6. Диалоговое окно «Мастер экспорта сертификатов». Установка пароля

8. Экспортировать данные в файл-ключ. Для этого нажать кнопку «Обзор» и выбрать место хранения и название файла-ключа с расширением. Нажать «Далее» (рис. 7).

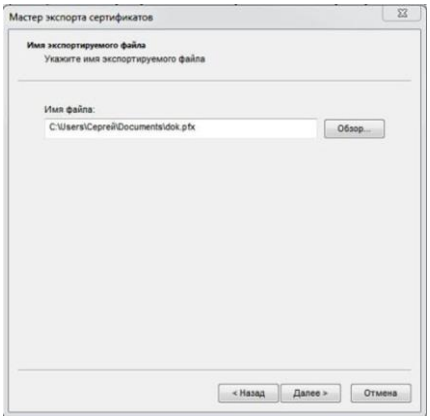

Рис. 7. Диалоговое окно «Мастер экспорта сертификатов».
Выбор места хранения и файла-ключа

9. В последнем открытом окне, завершающем создание файла-ключа, нажмите кнопку «Готово».

Теперь никто из посторонних не сможет воспользоваться информацией, находящейся в зашифрованной папке, без знания пароля и наличия файла-ключа.

Такой способ защиты применим только в том случае, если в ОС используется файловая система NTFS.

Установка пароля с помощью программы WinRaR

Удобная бесплатная программа для архивирования данных и установки пароля на файлы и папки. Необходимые документы можно просматривать прямо из архива.

Технология установки пароля:

1. После запуска программы выбрать папку для архивирования и щёлкнуть кнопку «Добавить».

2. Поскольку при установке WinRaR основные пункты меню этого архиватора сразу добавляются в системное контекстное меню ОС, то добавить папку в архив можно и с помощью контекстного меню.

3. В открывшемся окне вписать имя, которое получит заархивированная папка. По умолчанию устанавливается действующее название. Здесь же выбирается тип архива, после чего нужно перейти на вкладку «Дополнительно» (рис. 8).

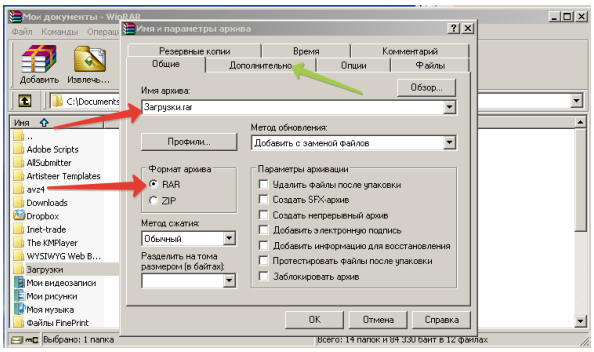

Рис. 8. Диалоговое окно «Имя и параметры архива»

4. На вкладке «Дополнительно» нажать кнопку «Установить пароль» (рис. 9).

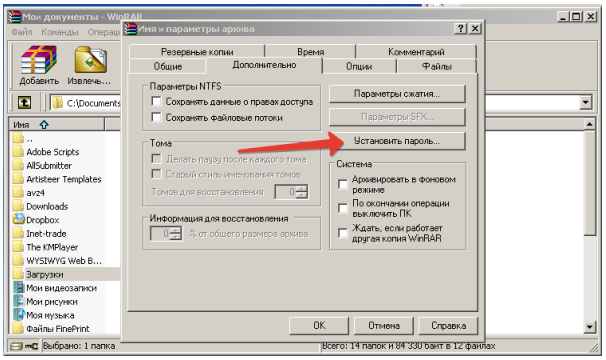

Рис. 9. Вкладка «Дополнительно» диалогового окна «Имя и параметры архива»

5. В открывшемся ДО ввести пароль и его подтверждение (рис. 10).

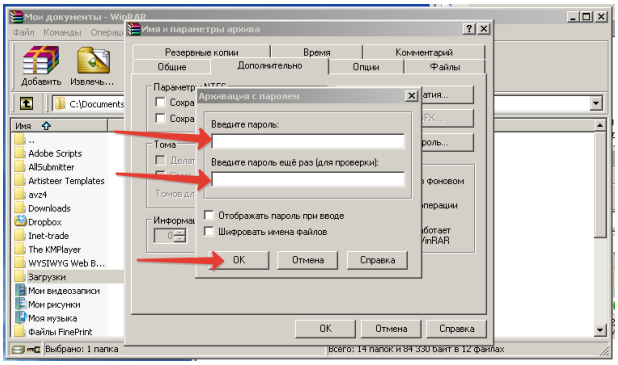

Рис. 10. Диалоговое окно «Архивация с паролем»

На этом архивирование и паролирование папки закончено.

После использования программ-архиваторов удаляйте исходную папку.

Аудиторная работа

1. Опишите этапы скрытия и отображения папки или файла.
2. Продемонстрируйте процесс скрытия и отображения папки или файла.

3. Опишите этапы технологии создания пароля для папки или файла.
4. Продемонстрируйте процесс создания пароля для папки или файла

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Опишите технологию скрытия папки или файла.

Задание 2. Перечислите программы позволяющие установить пароль для папки или файла.

Часть В

Задание 3. Постройте схему создания пароля с помощью программы WinRar.

Часть С

Задание 4. Загрузите ОС под своей учетной записью. На рабочем столе создайте папку, в качестве имени папки используйте свою фамилию. В папке создайте текстовый документ «Анкета» и разместите в нем следующую информацию:

– фамилия, имя, отчество;
– дата рождения;
– домашний адрес;
– телефон.

Задание 5. Загрузите операционную систему под другой учетной записью (Student). Проверьте, просматривается ли ваша папка? Ответ обоснуйте и поместите в отчет (другим пользователям пароль вашей учетной записи не известен).

Задание 6. Скопируйте вашу папку на диск D:\Группы\Группа КСК-21.

Задание 7. Сделайте папку скрытой. Отобразите папку. Продемонстрируйте процесс скрытия и отображения папки преподавателю.

Задание 8. Создайте пароль для вашей папки, используя для этого средство WinRar. В качестве пароля используйте свое имя. Исходную папку удалите.

Задание 9. Проверьте: доступна ли ваша папка другим пользователям. Результат отметьте в отчете.

Задание 10. Продемонстрируйте выполненную работу преподавателю.

Вариант 2

Часть А

Задание 1. Опишите технологию отображения скрытой папки или файла.

Задание 2. Опишите способы открытия диалогового окна «Свойства папки».

Часть В

Задание 3. Постройте схему создания пароля средствами операционной системы.

Часть С

Задание 4. Загрузите ОС под своей учетной записью. На рабочем столе создайте папку, в качестве имени папки используйте свою фамилию. В папке создайте текстовый документ «Анкета» и разместите в нем следующую информацию:

– фамилия, имя, отчество;
– дата рождения;
– домашний адрес;
– телефон.

Задание 5. Загрузите операционную систему под другой учетной записью (Student). Проверьте, просматривается ли ваша папка? Ответ обоснуйте и поместите в отчет (другим пользователям пароль вашей учетной записи не известен).

Задание 6. Скопируйте вашу папку на диск D:\Группы\Группа КСК-21.

Задание 7. Сделайте папку скрытой. Отобразите папку. Продемонстрируйте процесс скрытия и отображения папки преподавателю.

Задание 8. Создайте пароль для вашей папки, используя для этого средство WinRar. В качестве пароля используйте свое имя. Исходную папку удалите.

Задание 9. Проверьте: доступна ли ваша папка другим пользователям. Результат отметьте в отчете.

Задание 10. Продемонстрируйте выполненную работу преподавателю.

Контрольные вопросы:

1. В ходе работы были скрыты несколько папок. Можно ли отобразить только одну из них?
2. Чем визуально отличается папки, для которой создан пароль в программе WinRar от обычной папки?
3. Перечислите программы (кроме WinRar), позволяющие создавать пароли для папок и файлов?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 5
Разграничение прав доступа для пользователей локального компьютера и локальной сети

Цель: освоить технологию установки разграниченного доступа к информации для пользователей персонального компьютера и пользователей локальной сети;

установить разрешения для пользователей локального компьютера, настроить простой и расширенный доступы для пользователей локальной сети.

Средства обучения:

- методические рекомендации к практической работе № 5;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- просмотр действующих разрешений;
- установка разрешений использования информации;
- настройка простого доступа для пользователей локальной сети;
- настройка расширенного доступа для пользователей локальной сети.

Краткая теоретическая справка

Если компьютеры объединены в локальную сеть, то возникает необходимость настройки доступа к дискам и папкам компьютеров.

В локальной сети нельзя предоставить общий доступ к какому-либо отдельному файлу: чтобы сделать файл доступным для других пользователей сети, необходимо открыть общий доступ к папке, в которой он хранится.

В сетях существует два режима организации общего доступа:

– простой общий доступ к ресурсам компьютера;

– расширенный общий доступ к ресурсам компьютера.

Простой общий доступ к файлам и папкам

Простой общий доступ к файлам и папкам установлен по умолчанию. Убедиться в этом можно, выполнив команды Пуск/Панель управления/Свойства папки/вкладка «Вид». Опция «Использовать простой общий доступ к файлам (рекомендуется)» должна быть активной (рис. 1).

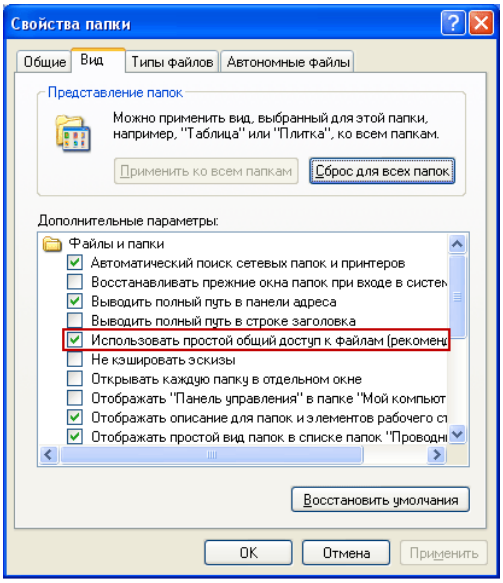

Рис. 1. Диалоговое окно «Свойства папки». Вкладка «Вид»

Если опция не активна, значит, на компьютере используется расширенный общий доступ.

Чтобы открыть общий доступ к какой-либо папке или диску, нужно на требуемом объекте вызвать контекстное меню, выбрать пункт «Свойства», перейти на вкладку «Доступ» (рис. 2).

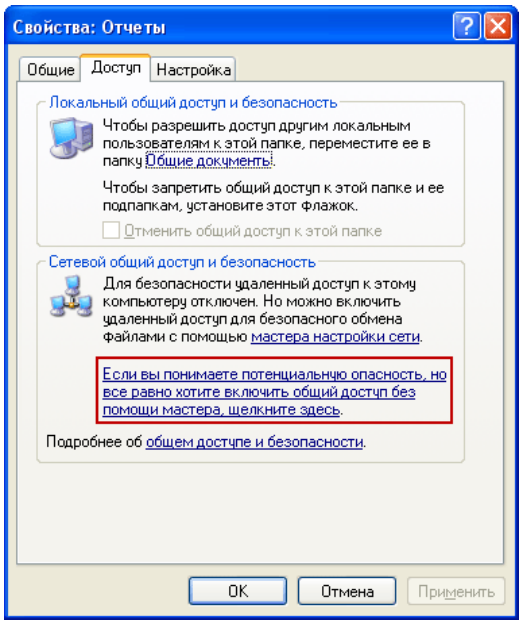

Рис. 2. Диалоговое окно «Свойства». Вкладка «Доступ»

Если доступ устанавливается в первый раз, то нужно будет нажать на следующую ссылку: «Если вы понимаете потенциальную опасность, но все равно хотите включить общий доступ без помощи мастера, щелкните здесь» (рис. 2).

А затем выбрать пункт «Просто включить общий доступ к файлам» (рис. 3).

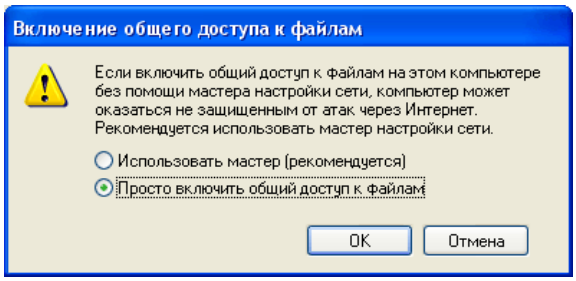

Рис. 3. Диалоговое окно «Включение общего доступа к файлам»

В открывшемся окне установить флажок в опции «Открыть общий доступ к этой папке» (рис. 4).

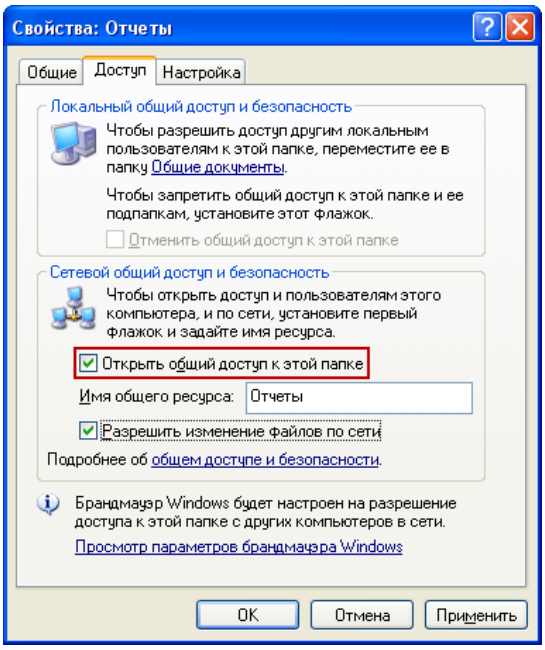

Рис. 4. Диалоговое окно «Свойства». Вкладка «Доступ»

Таким образом, пользователям сети будет открыт доступ к файлам, содержащимся в данной папке, в режиме «Только чтение». Изменить файлы, находящиеся в этой папке, или записать в нее свои файлы не возможно.

В поле «Имя общего ресурса» можно ввести сетевое имя папки, под которым она будет отображаться в списке общих ресурсов локальной сети.

Если установить флажок в опции «Разрешить изменение файлов по сети», тогда пользователи смогут копировать в эту папку свои файлы, а так же изменять содержащиеся в ней документы.

Чтобы пользователи сети могли получать доступ к общим папкам – на компьютере, где они расположены, необходимо включить учетную запись «Гость». Это позволит получать доступ к общей папке любому пользователю с любого компьютера, входящего в сеть.

Общий доступ к файлам и папкам обычно устанавливается при работе в домашней сети. Однако в локальной сети какой-либо организации требуется более серьезное разграничение прав пользователей. В этом случае необходимо включать Расширенный общий доступ к файлам и папкам.

Расширенный общий доступ к файлам и папкам

Для установки расширенного общего доступа к файлам и папкам компьютеров сети, необходимо выполнить команды Пуск/Панель управления/Свойства папки/вкладка Вид и снять флажок напротив пункта «Использовать простой общий доступ к файлам (рекомендуется)». Учетную запись «Гость» в целях безопасности также необходимо отключить.

Разрешение общего доступа для папок в расширенном режиме происходит также, как и в простом: Выбираем нужную папку или диск правой кнопкой мыши, выбираем команду «Свойства», вкладку «Доступ» и активируем переключатель «Открыть общий доступ к этой папке» (рис. 5).

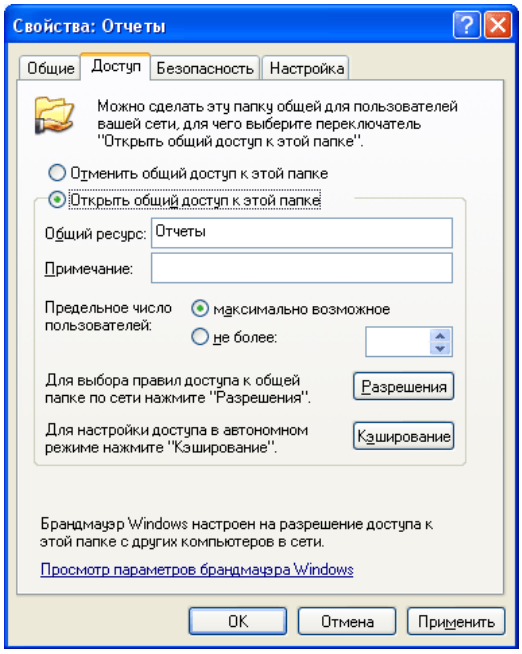

Рис. 5. Диалоговое окно «Свойства». Вкладка «Доступ»

В поле «Общий ресурс» можно ввести сетевое имя папки, под которым она будет отображаться в списке общих ресурсов локальной сети.

В поле «Примечание» можно ввести описание папки (например, «рабочие документы» и т.п.).

Разграничение прав доступа

Разграничение прав доступа – это создание определенных правил, в соответствии с которыми пользователи сети (каждый индивидуально или группа пользователей) смогут совершать определенные действия с содержимым общей папки: полный доступ, изменение, либо только чтение ее содержимого.

Чтобы задать эти правила, используется кнопка «Разрешения». Эта кнопка открывает окно «Разрешения» для папки (рис. 6).

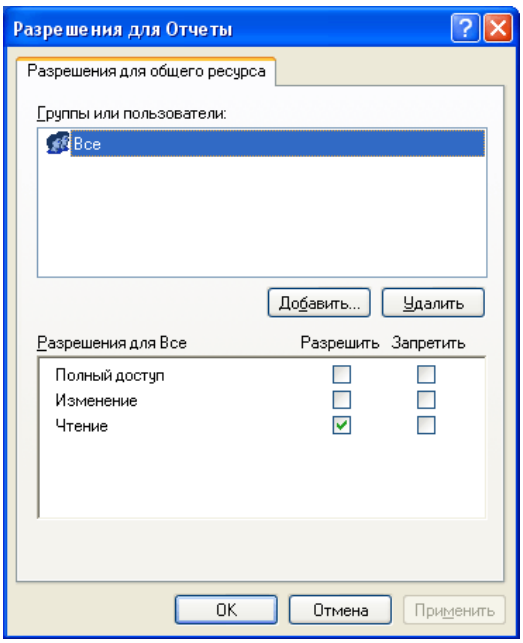

Рис. 6. Диалоговое окно «Разрешения»

В этом окне можно добавить пользователя или группу в список и определить для него разрешения, установив флажки напротив соответствующих пунктов.

Чтобы добавить пользователей и задать для них разрешения нужно нажать кнопку «Добавить». В следующем окне кнопку «Дополнительно» (рис. 7).

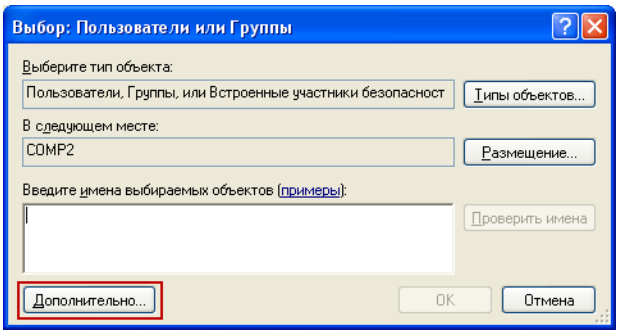

Рис. 7. Диалоговое окно «Выбор: Пользователи или группы»

В следующем открывшемся окне кнопку «Поиск» (рис. 8).

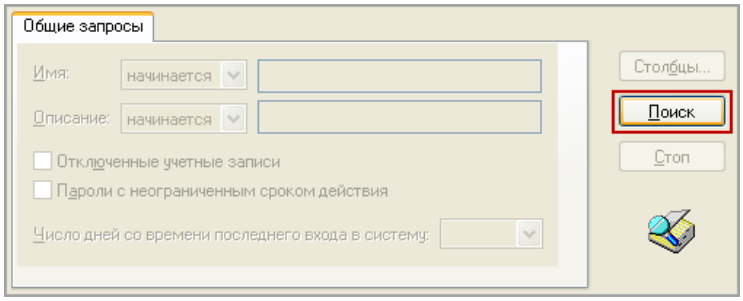

Рис. 8. Диалоговое окно «Общие запросы»

В нижней части окна «Выбор: Пользователи или Группы» выбрать имя пользователя или группы (рис. 9).

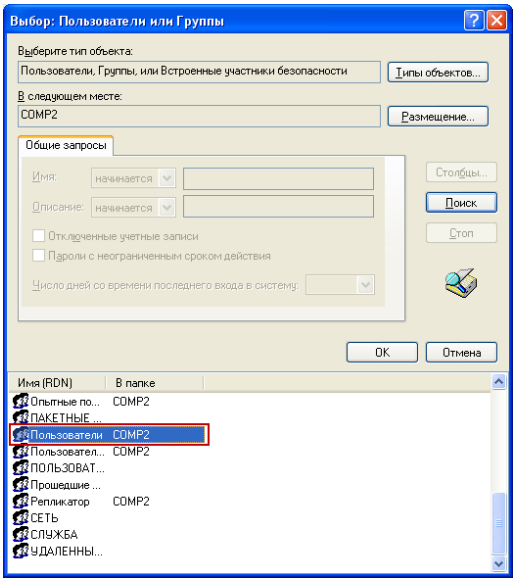

Рис. 9. Диалоговое окно «Выбор: Пользователи или Группы»

В следующем окне «Разрешения» устанавливаются права на чтение и изменение файлов в данной папке с помощью флажков в соответствующих опциях (рис. 10).

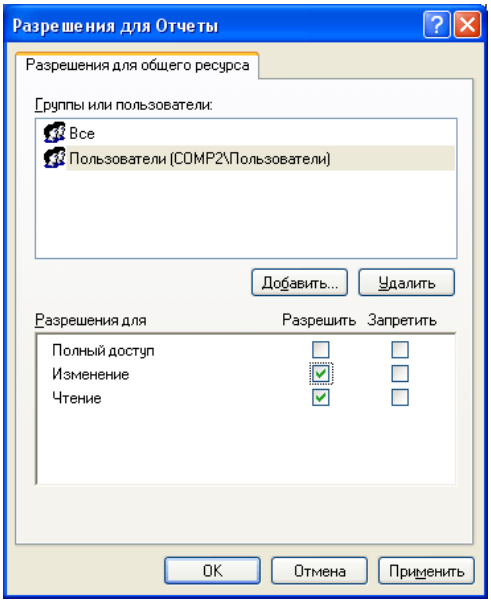

Рис. 10. Диалоговое окно «Разрешения»

Чтобы увидеть все ресурсы компьютера, открытые для общего доступа необходимо открыть папку «Сетевое окружение» на любом ПК сети. Затем выбрать пункт «Отобразить компьютеры рабочей группы». При двойном «щелчке» мышкой на имени любого компьютера – отобразятся его ресурсы, открытые для общего доступа другим компьютерам сети.

Аудиторная работа

1. Опишите технологию установки простого общего доступа к файлам или папкам.

2. Продемонстрируйте технологию установки простого общего доступа к файлам или папкам.

3. Опишите технологию установки расширенного общего доступа к файлам или папкам.

4. Продемонстрируйте технологию установки расширенного общего доступа к файлам или папкам.

5. Опишите технологию просмотра действующих разрешений пользователя или группы пользователей.

6. Продемонстрируйте технологию просмотра действующих разрешений пользователя или группы пользователей.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Назовите режимы организации общего доступа.

Задание 2. Опишите последовательность действий, которые необходимо выполнить для просмотра действующих разрешений.

Задание 3. Опишите назначение вкладки «Безопасность» диалогового окна «Свойства» (рис. 11). Перечислите элементы управления, расположенные на этой вкладке и опишите их назначение.

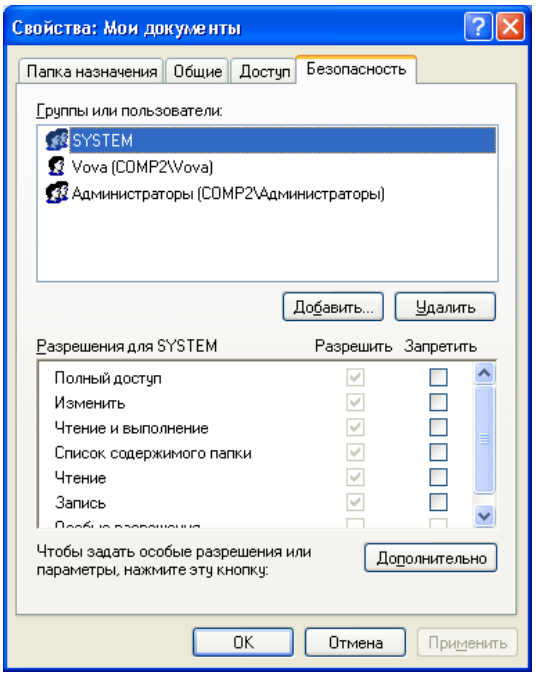

Рис. 11. Диалоговое окно «Свойства». Вкладка «Безопасность»

Часть В

Задание 4. Опишите последовательность действий, которые необходимо выполнить для установки расширенного общего доступа к файлу или папке для пользователей локальной сети.

Задание 5. Загрузите операционную систему, используя свою учетную запись. Откройте папку «КСК-21» и разархивируйте свою рабочую папку. Создайте две копии этой папки, добавив к их именам цифры 1 и 2.

Задание 6. Откройте окно «Свойства папки» для первой из ваших папок. Запишите в отчет названия содержащихся в этом окне вкладок.

Задание 7. Если в окне отсутствует вкладка «Безопасность», то добавьте ее. Используйте для этого учетную запись администратора.

Задание 8. Откройте еще раз окно «Свойства папки». Убедитесь в том, что вкладка «Безопасность» отображается в окне. Просмотрите действующие разрешения для вашей папки и заполните следующую таблицу:

№ п/п	Возможные разрешения	Пользователи		
		Администратор1	Student	Ваша учетная запись

Часть С

Задание 9. Выберите пользователя «Student». Установите для этого пользователя все разрешения кроме «Создание папок/дозапись данных», «Создание файлов/запись данных», «Смена разрешений», «Смена владельца», «Удаление».

Задание 10. Просмотрите действующие разрешения для пользователя «Student» и убедитесь, что установленные вами параметры применены. Продемонстрируйте выполненную работу преподавателю.

Задание 11. Установите для второй папки простой общий доступ по локальной сети. Имя для папки в сети установите – «Рабочая».

Задание 12. Установите для третьей папки расширенный общий доступ по локальной сети. Имя для папки в сети установите – «Общая», пометьте, что эта папка содержит рабочие документы. Установите следующие разрешения для пользователей:

- Администратор: полный доступ;
- Student: нет доступа.

Задание 13. Продемонстрируйте выполненную работу преподавателю.

Задание 14. Удалите вкладку «Безопасность» из диалогового окна «Свойства папки».

Вариант 2

Часть А

Задание 1. Дайте понятие простого общего доступа.

Задание 2. Опишите последовательность действий, которые необходимо выполнить для установки простого общего доступа к файлу или папке для пользователей локальной сети.

Задание 3. Опишите назначение вкладки «Доступ» диалогового окна «Свойства» (рис. 5). Перечислите элементы управления, расположенные на этой вкладке и опишите их назначение.

Часть В

Задание 4. Опишите последовательность действий, которые необходимо выполнить для установки необходимых разрешений пользователям локального компьютера.

Задание 5. Загрузите операционную систему, используя свою учетную запись. Откройте папку «КСК-21» и разархивируйте свою рабочую папку. Создайте две копии этой папки, добавив к их именам цифры 1 и 2.

Задание 6. Откройте окно «Свойства папки» для первой из ваших папок. Запишите в отчет названия содержащихся в этом окне вкладок.

Задание 7. Если в окне отсутствует вкладка «Безопасность», то добавьте ее. Используйте для этого учетную запись администратора.

Задание 8. Откройте еще раз окно Свойства папки. Убедитесь в том, что вкладка Безопасность отображается в окне. Просмотрите действующие разрешения для вашей папки и заполните следующую таблицу:

№ п/п	Возможные разрешения	Пользователи		
		Администратор2	Student	Ваша учетная запись

Часть С

Задание 9. Выберите пользователя «Student». Установите для этого пользователя все разрешения кроме «Создание папок/дозапись данных», «Создание файлов/запись данных», «Смена разрешений», «Смена владельца», «Удаление».

Задание 10. Просмотрите действующие разрешения для пользователя «Student» и убедитесь, что установленные вами параметры применены. Продемонстрируйте выполненную работу преподавателю.

Задание 11. Установите для второй папки простой общий доступ по локальной сети. Имя для папки в сети установите – «Рабочая».

Задание 12. Установите для третьей папки расширенный общий доступ по локальной сети. Имя для папки в сети установите – «Общая», пометьте, что эта папка содержит рабочие документы. Установите следующие разрешения для пользователей:

– Администратор: полный доступ;

– Student: нет доступа.

Задание 13. Продемонстрируйте выполненную работу преподавателю.

Задание 14. Удалите вкладку «Безопасность» из диалогового окна «Свойства папки».

Контрольные вопросы:

1. Что представляет собой управление доступом?
2. Что представляют собой разрешения?
3. Какая файловая система не позволяет установить разграничение доступа для объектов персонального компьютера?
4. В чем заключается отличие простого общего доступа к объектам локальной сети от расширенного?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 6

Настройка параметров политики аудита для категории события

Цель: освоить технологию установки параметров политики аудита событий для конкретной компьютерной системы;

настроить параметры журнала безопасности;

выполнить анализ событий с помощью журнала безопасности.

Средства обучения:

– методические рекомендации к практической работе № 6;
– персональные компьютеры;
– проектор.

Виды самостоятельной работы:

– просмотр локальных политик;
– установка параметров политики аудита;
– просмотр журнала безопасности;
– настройка параметров журнала безопасности.

Краткие теоретические сведения

Аудит

Процедура аудита применительно к ОС заключается в регистрации в специальном журнале, называемом журналом аудита или журналом безопасности, событий, которые могут представлять опасность для ОС. Пользователи системы, обладающие правом чтения журнала аудита, называются аудиторами.

Журнал аудита может содержать всю необходимую информацию. К числу событий, которые могут представлять опасность для ОС, обычно относят следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смену привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

Требования к аудиту

Подсистема аудита ОС должна удовлетворять следующим требованиям.

1. Добавлять записи в журнал аудита может только ОС.

2. Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, в том числе и сама ОС.

3. Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией.

4. Очищать журнал аудита могут только пользователи-аудиторы. После очистки журнала в него автоматически вносится запись о том, что журнал аудита был очищен, с указанием времени очистки журнала и имени пользователя, очистившего журнал. ОС должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле.

5. При переполнении журнала аудита ОС аварийно завершает работу («зависает»). После перезагрузки работать с системой могут только аудиторы. ОС переходит к обычному режиму работы только после очистки журнала аудита.

В процессе аудита используются три средства управления: политика аудита, параметры аудита в объектах, а также журнал безопасности, куда заносятся события, связанные с безопасностью.

Политика аудита

Политика аудита – это совокупность правил, определяющих, какие события должны регистрироваться в журнале аудита. Для обеспечения надежной защиты ОС в журнале аудита должны обязательно регистрироваться следующие события:

– попытки входа/выхода пользователей из системы;

– попытки изменения списка пользователей;

– попытки изменения политики безопасности, в том числе и политики аудита.

Окончательный выбор событий, которые должны регистрироваться в журнале аудита, возлагается на аудиторов.

Политика аудита настраивает в системе определенного пользователя и группы аудит активности. Для того чтобы отконфигурировать политики аудита, в редакторе управления групповыми политиками необходимо выполнить команды Конфигурация компьютера/Конфигурация Windows/ Параметры безопасности/Локальные политики/Политика аудита. (По умолчанию параметр политики аудита для рабочих станций установлен на «Не определено».)

Для определения параметр политики нужно выполнить двойное нажатие левой кнопкой мыши на нужном параметре и установить флажки в опциях «Определить следующие параметры политики»: «Успех» или «Отказ» или обоих типов событий одновременно (рис. 1).

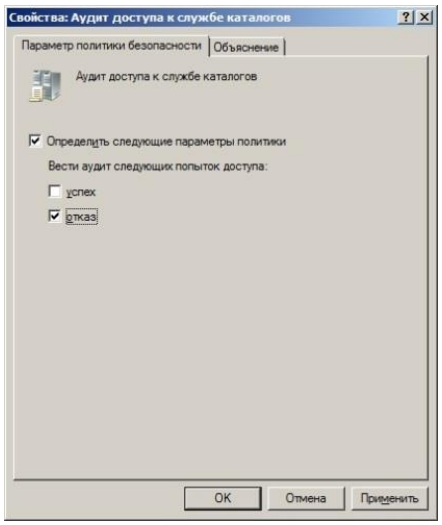

Рис. 1. Диалоговое окно «Свойства: Аудит доступа к службе каталогов»

После настройки политики аудита события будут заноситься в журнал безопасности.

Политики аудита

1. *Аудит входа в систему*

Текущая политика определяет, будет ли операционная система выполнять аудит каждой попытки входа пользователя в систему или выхода из нее.

2. *Аудит доступа к объектам*

Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active Directory. (К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом.)

3. *Аудит доступа к службе каталогов*

При помощи этой политики безопасности можно определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне «Дополнительные параметры безопасности» свойств объекта Active Directory. Аудит создается только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данном списке.

4. *Аудит изменения политики*

Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учетной записи или доверия.

5. Аудит изменения привилегий

Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей.

6. Аудит отслеживания процессов

Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам.

7. Аудит системных событий

Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики можно узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени.

8. Аудит событий входа в систему

При помощи этой политики аудита можно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учетных данных. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удаленного входа, причем события выхода из системы не записываются.

9. Аудит управления учетными записями

Эта последняя политика тоже считается очень важной, так как именно при помощи нее можно определить, необходимо ли выполнять аудит каждого события управления учетными записями на компьютере.

Аудиторная работа

1. Дайте понятия аудита и журнала безопасности.
2. Перечислите виды аудита.
3. Дайте характеристику каждого вида аудита.
4. Опишите технологию настройки параметров аудита событий.
5. Продемонстрируйте процесс настройки параметров аудита событий.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Укажите причины, вызывающие необходимость использования аудита.

Задание 2. Перечислите элементы представленного диалогового окна (рис. 2) и опишите их назначение.

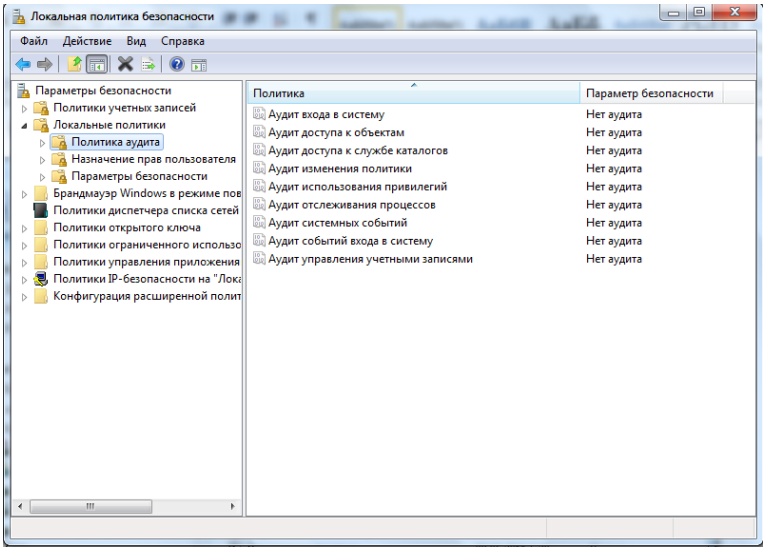

Рис. 2. Диалоговое окно «Локальная политика безопасности»

Задание 3. Загрузите операционную систему, используя учетную запись «Администратор1».

Задание 4. Откройте диалоговое окно «Локальная политика безопасности» (Пуск/Панель управления/Производительность и обслуживание/Администрирование/Локальная политика безопасности).

Задание 5. В дереве консоли просмотрите параметры безопасности и запишите в отчет отображенные здесь политики.

Задание 6. Откройте папку «Локальные политики» и выберите политику аудита. Запишите в отчет возможные виды политики аудита.

Часть В

Задание 7. Настройте аудит входа в систему, аудит доступа к объектам, аудит событий входа в систему так, чтобы в журнале безопасности отмечались события как успешные так и не успешные.

Задание 8. Определите, в чем заключается отличие аудита входа в систему от аудита событий входа в систему (можно воспользоваться вкладкой «Объяснение»). Запишите в отчет.

Задание 9. Закройте окно «Локальная политика безопасности».

Задание 10. Откройте журнал безопасности (Пуск/Панель управления/Производительность и обслуживание/Администрирование/ Просмотр событий).

Задание 11. В дереве консоли выберите «Безопасность». Выпишите в отчет следующие сведения:

– количество событий, отмеченных в журнале;
– какие сведения о событиях отображаются в журнале безопасности;

– перечислите типы событий;

– количество успешных событий и количество отказов;

– номера событий.

Задание 12. Выполните сохранение файла журнала в свою рабочую папку с именем «Аудит 1.txt».

Задание 13. Очистите журнал безопасности.

Часть С

Задание 14. Закройте диалоговые окна и выполните попытку перезагрузки системы под своей учетной записью, указав неверный пароль. Повторите попытку с верным паролем.

Задание 15. Откройте свою рабочую папку и просмотрите файл «Анкета». Закройте окна и перезагрузите систему под администратором.

Задание 16. Просмотрите журнал безопасности. Выпишите в отчет сведения, указанные в задании 11.

Задание 17. Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит 2.txt».

Задание 18. Очистите журнал безопасности и отмените все настройки аудита, выполненные вами. Продемонстрируйте преподавателю выполненную работу.

Вариант 2

Часть А

Задание 1. Перечислите события, в результате которых может быть нанесен вред операционной системе.

Задание 2. Перечислите элементы представленного диалогового окна (рис. 3) и опишите их назначение.

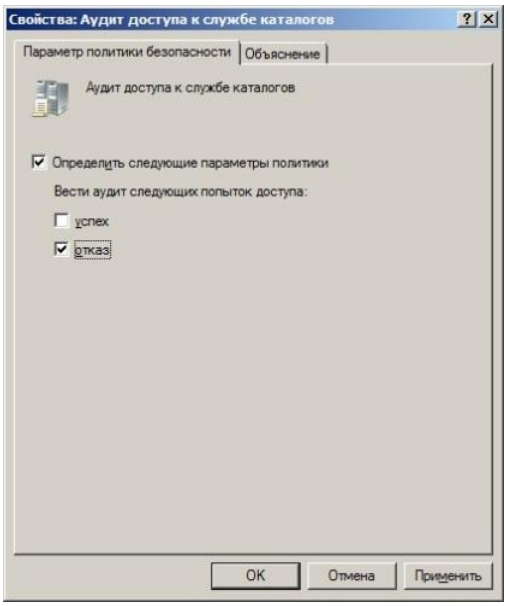

Рис. 3. Диалоговое окно «Свойства: Аудит доступа к службе каталогов»

Задание 3. Загрузите операционную систему, используя учетную запись «Администратор2».

Задание 4. Откройте диалоговое окно «Локальная политика безопасности» (Пуск/Панель управления/Производительность и обслуживание/Администрирование/Локальная политика безопасности).

Задание 5. В дереве консоли просмотрите параметры безопасности и запишите в отчет отображенные здесь политики.

Задание 6. Откройте папку «Локальные политики» и выберите политику аудита. Запишите в отчет возможные виды политики аудита.

Часть В

Задание 7. Настройте аудит входа в систему, аудит доступа к объектам, аудит событий входа в систему так, чтобы в журнале безопасности отмечались события как успешные так и не успешные.

Задание 8. Определите, в чем заключается отличие аудита входа в систему от аудита событий входа в систему (можно воспользоваться вкладкой «Объяснение»). Запишите в отчет.

Задание 9. Закройте окно «Локальная политика безопасности».

Задание 10. Откройте журнал безопасности (Пуск/Панель управления/Производительность и обслуживание/Администрирование/ Просмотр событий).

Задание 11. В дереве консоли выберите «Безопасность». Выпишите в отчет следующие сведения:

- количество событий, отмеченных в журнале;
- какие сведения о событиях отображаются в журнале безопасности;
- перечислите типы событий;
- количество успешных событий и количество отказов;
- номера событий.

Задание 12. Выполните сохранение файла журнала в свою рабочую папку с именем «Аудит 1.txt.»

Задание 13. Очистите журнал безопасности.

Часть С

Задание 14. Закройте диалоговые окна и выполните попытку перезагрузки системы под своей учетной записью, указав неверный пароль. Повторите попытку с верным паролем.

Задание 15. Откройте свою рабочую папку и просмотрите файл «Анкета». Закройте окна и перезагрузите систему под администратором.

Задание 16. Просмотрите журнал безопасности. Выпишите в отчет сведения, указанные в задании 11.

Задание 17. Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит 2.txt».

Задание 18. Очистите журнал безопасности и отмените все настройки аудита, выполненные вами. Продемонстрируйте преподавателю выполненную работу.

Контрольные вопросы:

1. Что представляет собой процедура аудита?
2. Кто такие аудиторы?
3. Что представляет собой политика аудита?
4. Назовите пользователей, которые могут устанавливать параметры политики аудита?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 7
Настройка параметров политики аудита для локальных папок и файлов

Цель: настроить параметры политики аудита локальных принтеров, файлов и папок;

настроить параметры журнала безопасности;

выполнить анализ событий для локальных папок и файлов с помощью журнала безопасности.

Средства обучения:

– методические рекомендации к практической работе № 7;

– персональные компьютеры;

– проектор.

Виды самостоятельной работы:

– установка параметров политики локальных принтеров, файлов и папок для отдельных пользователей;

– просмотр журнала безопасности;

– настройка параметров журнала безопасности.

Краткая теоретическая справка

Администратор компьютера или аудитор можете применить в системе аудит доступа пользователей к файлам, папкам и принтерам.

Включение аудита доступа пользователей к файлам, папкам и принтерам

Информационные записи системного аудита заносятся в журнал событий «Безопасность». Для включения системного аудита необходимо выполнить следующие действия:

1. В меню «Пуск» выберите пункт «Панель управления», затем ссылку «Производительность и обслуживание» и открыть группу программ «Администрирование».
2. Открыть элемент «Локальная политика безопасности».
3. Развернуть элемент «Локальные политики».
4. Выбрать папку «Политика аудита».
5. Открыть параметр «Аудит доступа к объектам».
6. Для отслеживания удачных попыток доступа к файлам, папкам и принтерам установить флажок в опции «Успех».
7. Для отслеживания неудачных попыток доступа к файлам, папкам и принтерам установить флажок в опции «Отказ».
8. Для отслеживания всех попыток доступа к объектам аудита установить оба флажка.

Указание файлов, папок и принтеров в качестве объектов аудита

После включения аудита доступа к объектам можно указать, для каких файлов, папок и принтеров необходимо проводить отслеживание доступа. Для этого выполняются следующие действия:

1. В Проводнике выбрать файл или папку, которую необходимо отслеживать. Для аудита принтера перейти в системную папку «Принтеры и факсы», выбрав соответствующий пункт в меню «Пуск».

2. Вызвать контекстное меню выбранного объекта и запустить команду «Свойства».

3. Перейти на вкладку «Безопасность» и нажать кнопку «Дополнительно».

4. Перейдите на вкладку «Аудит» и нажать кнопку «Добавить».

5. В поле «Введите имена выбираемых объектов» указать имя пользователя или группы, которую необходимо отслеживать при доступе к данному объекту. Можно проверить вводимое имя на наличие в списке пользователей компьютера, нажав кнопку «Дополнительно», а затем кнопку «Поиск» в окне «Выбор: Пользователь, Компьютер или Группа».

6. Установить требуемые флажки для отслеживания успешных и неудачных попыток при выполнении соответствующих действий.

Возможные проблемы

– Для получения возможности аудита доступа к файлам и папкам данные объекты должны располагаться на разделе с файловой системой NTFS.

– Если КС является членом домена, и на уровне домена применены собственные политики аудита, данные политики имеют более высокий приоритет по сравнению с настройками локальной политики.

Аудиторная работа

1. Опишите технологию включения аудита доступа пользователей к файлам, папкам и принтерам.

2. Продемонстрируйте процесс включения аудита доступа пользователей к файлам, папкам и принтерам.

3. Опишите технологию указания файлов, папок и принтеров в качестве объектов аудита.

4. Продемонстрируйте описанную технологию.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Укажите причины, вызывающие необходимость использования аудита локальных файлов, папок и принтеров.

Задание 2. Загрузите операционную систему, используя учетную запись «Администратор1».

Задание 3. Настройте аудит для категории событий доступа к объектам (успех и отказ).

Задание 4. Настройте политику аудита своей рабочей папки для пользователя «Student»:

– контекстное меню/Свойства/Безопасность/Дополнительно/ Аудит;

– кнопка Добавить/Дополнительно/Поиск/Student;

– в окне «Элемент аудита» установите опции успеха и отказа для позиций: «Обзор папок/Выполнение файлов», «Содержание папки/Чтение данных», «Создание файлов/Запись данных».

Часть B

Задание 5. Просмотрите журнал безопасности. Отметьте в отчете, какие события отображаются в ЖБ. Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит_Папка1.txt».

Задание 6. Загрузите операционную систему для учетной записи «Test». Откройте свою рабочую папку. Создайте в ней текстовый файл «Расписание_6.03». Разместите в файле информацию о расписании на сегодня.

Задание 7. Просмотрите журнал безопасности. Отметьте в отчете, какие изменения произошли в ЖБ (какие события добавлены в ЖБ). Выпишите появившиеся номера событий.

Задание 8. Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит_Папка2.txt».

Задание 9. Зайдите в систему под своей учетной записью. В своей рабочей папке создайте текстовый файл «Расписание_7.03». Разместите в файле информацию о расписании на завтра.

Часть C

Задание 10. Просмотрите журнал безопасности. Отметьте в отчете, какие изменения произошли в ЖБ (какие события добавлены в ЖБ). Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит_Папка3.txt».

Задание 11. Загрузите систему под учетной записью «Student». Откройте любую папку, расположенную в папке «Группы». Создайте в ней папку «Аудит».

Задание 12. Просмотрите ЖБ. Отметьте в отчете, какие изменения произошли в ЖБ (какие события добавлены в ЖБ).

Задание 13. Сохраните файл ЖБ в своей рабочей папке с именем «Аудит_Папка4.txt».

Задание 14. Проанализируйте изменения ЖБ в ходе выполнения работы и сделайте вывод: как работает политика аудита папок и файлов, в чем разница между аудитом событий и аудитом папок и файлов.

Задание 15. Очистите журнал безопасности и отмените все настройки аудита, выполненные вами. Продемонстрируйте преподавателю выполненную работу.

Вариант 2

Часть А

Задание 1. Опишите проблемы, которые могут возникнуть при настройке аудита файлов, папок и принтеров.

Задание 2. Загрузите операционную систему, используя учетную запись «Администратор2».

Задание 3. Настройте аудит для категории событий доступа к объектам (успех и отказ).

Задание 4. Настройте политику аудита своей рабочей папки для пользователя «Student»:

– контекстное меню/Свойства/Безопасность/Дополнительно/ Аудит;

– кнопка Добавить/Дополнительно/Поиск/Student;

– в окне «Элемент аудита» установите опции успеха и отказа для позиций: «Обзор папок/Выполнение файлов», «Содержание папки/Чтение данных», «Создание файлов/Запись данных».

Часть В

Задание 5. Просмотрите журнал безопасности. Отметьте в отчете, какие события отображаются в ЖБ. Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит_Папка1.txt».

Задание 6. Загрузите операционную систему для учетной записи «Test». Откройте свою рабочую папку. Создайте в ней текстовый файл «Расписание_6.03». Разместите в файле информацию о расписании на сегодня.

Задание 7. Просмотрите журнал безопасности. Отметьте в отчете, какие изменения произошли в ЖБ (какие события добавлены в ЖБ). Выпишите появившиеся номера событий.

Задание 8. Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит_Папка2.txt».

Задание 9. Зайдите в систему под своей учетной записью. В своей рабочей папке создайте текстовый файл «Расписание_7.03». Разместите в файле информацию о расписании на завтра.

Часть С

Задание 10. Просмотрите журнал безопасности. Отметьте в отчете, какие изменения произошли в ЖБ (какие события добавлены в ЖБ).

Сохраните файл журнала безопасности в своей рабочей папке с именем «Аудит_Папка3.txt».

Задание 11. Загрузите систему под учетной записью «Student». Откройте любую папку, расположенную в папке «Группы». Создайте в ней папку «Аудит».

Задание 12. Просмотрите ЖБ. Отметьте в отчете, какие изменения произошли в ЖБ (какие события добавлены в ЖБ).

Задание 13. Сохраните файл ЖБ в своей рабочей папке с именем «Аудит_Папка4.txt».

Задание 14. Проанализируйте изменения ЖБ в ходе выполнения работы и сделайте вывод: как работает политика аудита папок и файлов, в чем разница между аудитом событий и аудитом папок и файлов.

Задание 15. Очистите журнал безопасности и отмените все настройки аудита, выполненные вами. Продемонстрируйте преподавателю выполненную работу.

Контрольные вопросы:

1. Что представляет собой политика аудита локальных файлов и папок?
2. Опишите назначение опции «Успех».
3. Опишите назначение опции «Отказ».

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 8

Настройка параметров политики безопасности операционной системы

Цель: установить параметры политики безопасности для конкретной операционной системы.

Средства обучения:

- методические рекомендации к практической работе № 8;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- установка параметров политики учетных записей;
- установка параметров политики паролей;
- установка параметров политики блокировки учетных записей;
- установка параметров локальной политики;
- назначение прав пользователей;
- установка параметров безопасности.

Краткая теоретическая справка

Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т.е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в ОС.

Описание параметров политики безопасности

Политика безопасности включает в себя следующие области безопасности:

1. Политики учетных записей. Позволяет настраивать Политику паролей, политику блокировки учетной записи.
2. Локальные политики. Настройка локальных политик включает настройку параметров политики аудита, политики назначения прав пользователя и параметры безопасности.
3. Журнал событий. Позволяет настраивать параметры журналов событий приложений, системных событий, событий безопасности и событий службы каталогов.
4. Политики открытого ключа. Включает настройку параметров шифрующей файловой системы (EFS).
5. Политики ограниченного использования программ.
6. Политики безопасности IP на локальный компьютер.

Для настройки параметров безопасности необходимо открыть диалоговое окно «Локальные параметры безопасности» (Пуск/Панель управления/Администрирование).

Настройка параметров политики учетных записей

Настройка параметров политики учетных записей выполняется администратором в узле «Политики учетных записей» оснастки «Локальная безопасность».

В узле «Политика паролей» вынесены отдельно настройки, связанные с ограничениями на используемые пароли: «Максимальный срок действия пароля», «Минимальный срок действия пароля», «Минимальная длина пароля», «Требовать не повторяемости паролей», «Не запоминать прежние пароли».

Политика учетных записей включает следующие параметры: «Политика блокировки учетных записей», «Блокировка учетной записи», «Пороговое значение блокировки», «Сброс счетчика блокировки через».

Права пользователей

При выборе узла «Назначение прав пользователя» в правой части окна открывается список определенных прав, а так же каким группам пользователей данное право предоставлено. Чтобы зайти в настройки права пользователя, необходимо «щелкнуть» мышкой дважды на выбранном пункте из списка.

Основные права: «Доступ к компьютеру по сети», «Архивирование файлов и каталогов», «Изменять системное время», «Управление аудитом и журналом безопасности»

Параметры безопасности

Проблема обеспечение безопасности компьютера связана с работой в сети, где существует большое количество различного рода опасностей, атак, вирусов и т.п. и особенно если компьютер подключен к сети Интернет.

Узел «Параметры безопасности» позволяет администратору вручную настраивать уровни безопасности. Чтобы изменить любой из параметров безопасности, нужно открыть диалоговое окно, позволяющее модифицировать значение параметра.

Для повышения защиты компьютера от различного рода атак по сети Интернет следует настраивать следующие параметры:

1. Напоминать пользователям об истечении срока действия пароля.
2. Пользователям можно написать любое пожелание при входе в систему, в целях администрирования. Параметр «Текст сообщения для пользователей при входе в систему».

3. Запретить пользователям установку драйвера принтера (по умолчанию - отключен). Рекомендуется включать.

4. Очистка страничного файла виртуальной памяти (по умолчанию - отключен). Рекомендуется включить. После этого система всегда при выключении компьютера будет удалять файл подкачки. Но тут есть свой минус - система будет долго выключаться.

Аудиторная работа

1. Опишите технологию установки параметров политики паролей.
2. Продемонстрируйте процесс установки параметров политики паролей.
3. Опишите технологию установки параметров политики блокировки учетных записей.
4. Продемонстрируйте процесс установки параметров политики блокировки учетных записей.
5. Опишите технологию назначения прав пользователей.
6. Продемонстрируйте процесс назначения прав пользователей.
7. Опишите технологию установки параметров безопасности.
8. Продемонстрируйте процесс установки параметров безопасности.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Перечислите задачи, которые позволяет решать политика безопасности.

Задание 2. Заполните таблицу:

Виды политики безопасности	Назначение	Возможные настройки	Назначение настроек

Часть В

Задание 3. Настройте политику паролей следующим образом:

- максимальный срок действия пароля – 30 дней;
- минимальная длина пароля – 8 символов;
- минимальный срок действия пароля – 3 дня;
- пароли должны отвечать требованиям – вкл.;
- требовать неповторимости пароля – 2 хранимых пароля.

Сделайте скриншот диалогового окно с выполненными вами настройками и поместите его в текстовый документ. Сохраните документ в своей рабочей папке с именем «Отчет_ПР8_Фамилия».

Задание 4. Настройте параметры политики блокировки учетных записей следующим образом:

– блокировка учетной записи – вкл.;
– пороговое значение блокировки – 3 ошибки;
– сброс счетчика блокировки через – 30 мин.

Скопируйте диалоговое окно с выполненными вами настройками в текстовый документ «Отчет_ПР8_Фамилия».

Часть С

Задание 5. Настройте параметры политики прав пользователей следующим образом:

– доступ к компьютеру по сети – добавить свою учетную запись;
– изменять системное время - добавить свою учетную запись.

Скопируйте диалоговое окно с выполненными вами настройками в текстовый документ «Отчет_ПР8_Фамилия».

Задание 6. Настройте параметры политики безопасности следующим образом:

– напомнить пользователям об истечении срока действия пароля – 2 дня;
– текст сообщения для пользователей при входе в систему – Успехов в новом рабочем дне;
– запретить пользователям установку драйвера принтера – разрешить.

Скопируйте диалоговое окно с выполненными вами настройками в текстовый документ «Отчет_ПР8_Фамилия.

Вариант 2

Часть А

Задание 1. Дайте понятие параметров безопасности.

Задание 2. Заполните таблицу:

Виды политики безопасности	Назначение	Возможные настройки	Назначение настроек

Часть В

Задание 3. Настройте политику паролей следующим образом:

– максимальный срок действия пароля – 25 дней;
– минимальная длина пароля – 6 символов;
– минимальный срок действия пароля – 2 дня;
– пароли должны отвечать требованиям – вкл.;
– требовать неповторимости пароля – 3 хранимых пароля.

Сделайте скриншот диалогового окно с выполненными вами настройками и поместите его в текстовый документ. Сохраните документ в своей рабочей папке с именем «Отчет_ПР8_Фамилия».

Задание 4. Настройте параметры политики блокировки учетных записей следующим образом:

– блокировка учетной записи – вкл.;
– пороговое значение блокировки – 2 ошибки;
– сброс счетчика блокировки через – 40 мин.

Скопируйте диалоговое окно с выполненными вами настройками в текстовый документ «Отчет_ПР8_Фамилия».

Часть С

Задание 5. Настройте параметры политики прав пользователей следующим образом:

– доступ к компьютеру по сети – добавить свою учетную запись;
– изменять системное время - добавить свою учетную запись.

Скопируйте диалоговое окно с выполненными вами настройками в текстовый документ «Отчет_ПР8_Фамилия».

Задание 6. Настройте параметры политики безопасности следующим образом:

– напомнить пользователям об истечении срока действия пароля – 1 день;
– текст сообщения для пользователей при входе в систему – Успехов в новом рабочем дне;
– запретить пользователям установку драйвера принтера – разрешить.

Скопируйте диалоговое окно с выполненными вами настройками в текстовый документ «Отчет_ПР8_Фамилия».

Контрольные вопросы:

1. Что представляет собой параметры политики безопасности?
2. Запишите последовательность команд для открытия окна настройки параметров политики безопасности.

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

– порядковый номер и наименование практической работы;

– цель практической работы;

– ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;

– ответы на контрольные вопросы и вывод о выполненном задании.

Практическая работа № 9
Архивация и восстановление данных

Цель: освоить технологию настройки параметров архивации и восстановления системы;

выполнить архивацию и восстановление системы.

Средства обучения:

– методические рекомендации к практической работе № 9;

– персональные компьютеры;

– проектор.

Виды самостоятельной работы:

– настройка параметров архивации;

– архивация данных;

– настройка параметров восстановления данных;

– использование архива Backup для восстановления работоспособности системы.

Краткая теоретическая справка

Для создания полноценной системы защиты КС необходимо настроить сопровождение программного обеспечения.

Процедура сопровождения программного обеспечения требует:

– контролировать безопасность информационных процессов с целью выявления компьютерных вирусов, сбоев и отказов функционирования программ и запуска неавторизованных программ и процессов;

– контролировать целостность программного обеспечения (неавторизованную модификацию) на предмет выявления программных закладок, недокументированных функций и других программных дефектов;

– обеспечивать восстановление программ с эталонных копий (возможно, с привлечением сил и средств фонда алгоритмов и программ предприятия), их обновление, замену и другие вопросы, касающиеся жизненного цикла программного обеспечения.

Для безопасности программного обеспечения используют процедуры архивирования и резервирования данных.

Резервирование – это создание копии данных с целью повышения избыточности. В случае потери оригинального файла его можно восстановить из резервной копии.

Операция архивации отличается тем, что вместо копии в архив помещается сам файл, например, он стал не нужен (финансовый отчёт компании за прошлый год). Это позволяет освободить диск для свежих данных, а при необходимости работы с такими старыми данными файл возвращается из архива.

Резервное копирование – традиционный способ обеспечения работоспособности системы на случай порчи или утраты информационно-программного ресурса КС.

Архивация данных и ОС

В состав ОС Windows входит специальная программа для архивации и восстановления данных. С ее помощью могут быть сохранены, а потом восстановлены и системные установки Windows. Один из способов запуска программы: Пуск/Программы/Стандартные/Служебные/Архивация данных.

При запуске программа переходит в режим мастера архивации, но использовать мастер архивации необходимо в расширенном режиме. Для этого в первом же окне мастера нужно выбрать ссылку «Расширенный режим».

В следующем окне мастера архивации следует указать какие данные подлежат архивированию. Если нужно сделать полный архив всей системы вместе с установленными программами, то следует пометить галочкой папки «Documents and Settings», «Program Files», «Windows».

Далее надо указать название и местоположение архивного. Дополнительно можно снять флажок с пункта «Автоматически архивировать защищенные системные файлы вместе с состоянием системы» (в этом случае архив займет 10-20 Мб, если флажок не снимать, то для резервной копии потребуется на диске более 300 Мб). На следующем этапе указывается тип архива, например, «Обычный». Далее кнопки «Ok» и «Архивировать».

Типы архивации

Копирующая архивация

После завершения операции обычного архивирования, система присваивает файлу метку, что он добавлен в архив (точнее, у него снимается атрибут «Архивный»).

Копирующая архивация

У файлов, добавляемых в архив, атрибут «*Архивный»* не снимается. Применяется, если необходимо сохранить состояние отдельных файлов.

Ежедневная архивация

Будут сохранены все файлы, которые изменялись в течение дня до выполнения ежедневной архивации. Атрибут «Архивный» не снимается.

Добавочная архивация

В архив будут добавлены только те файлы, которые были созданы или изменены со времени последнего обычного или добавочного архивирования. Атрибут «Архивный» снимается (система считает файл уже архивированным).

Разностная архивация

В архив будут добавлены все файлы, созданные или измененные после обычной или добавочной архивации. Файлы не будут отмечены как архивированные (атрибут «Архивный» остается). Для восстановления необходим последний обычный архив и последний разностный.

Помимо типа архивации, можно задавать и ее способы. Например, произвести проверку данных после копирования.

Восстановление данных из резервной копии

Если система запускается успешно, то восстановить систему можно с помощью мастера архивации данных, выполнив команды меню Пуск/Программы/Стандартные/Служебные/Архивация данных.

На первом этапе выбрать переключатель «Восстановить данные».

На следующем этапе указать архивный файл. Кнопка «Восстановить».

В окне подтверждения восстановления кнопка «Дополнительно» открывает окно дополнительных параметров. Это окно содержит опции:

– *Восстановление безопасности* – восстановление параметров безопасности для восстанавливаемых файлов и папок. В параметры безопасности входят разрешения на доступ, записи аудита и сведения о владельце. Опция доступна, только если архивация данных проводилась с тома NTFS и восстановление Windows проводится также на том NTFS.

– *Восстановление точек соединения, а также ссылок для файлов и папок ниже соединения на исходное размещение* – восстановление точек

соединения на жестком диске, а также данных, на которые указывают эти точки соединения. Если этот флажок не установлен, точки соединения будут восстановлены, но данные, на которые они указывают, будут недоступны.

– *Сохранить существующие точки подключения томов* – если этот флажок установлен, в ходе восстановления не будет выполняться замена точек подключения томов, имеющихся в разделе или на томе, на который выполняется восстановление. Обычно при восстановлении системы его следует помечать и при восстановлении данных на целом диске, в томе или разделе. При этом сохраняются текущие размещения томов. Если восстанавливать файлы на исходное местоположение, текущие данные состояния системы будут заменены на восстанавливаемые. Если восстановление ОС идет на альтернативное местоположение, будут восстановлены только реестр и системные загрузочные файлы.

Аудиторная работа

1. Проведите сравнительный анализ понятий «Архивация» и «Резервирование».
2. Опишите технологию архивации данных и системных настроек Windows.
3. Продемонстрируйте процесс архивации данных.
4. Опишите технологию восстановления данных.
5. Продемонстрируйте процесс восстановления данных.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Перечислите основные задачи процедуры сопровождения программного обеспечения.

Задание 2. Заполните таблицу:

Типы архивации	Назначение	Наличие атрибута «Архивный»	Восстановление данных (указать файлы, необходимые для восстановления данных)

Часть В

Задание 3. Разработайте и начертите схему процесса архивации (указать все этапы архивации, включая запуск программы и дополнительные настройки).

Задание 4. Выполните обычную архивацию папки «Windows». Архивацию выполняйте в режиме мастера архивации. Архив сохраните в своей рабочей папке. Имя архива – «Архив_Фамилия_Windows». Сделайте

скриншоты каждого этапа настройки архивации и сохраните их в текстовом файле «Отчет_ПР9_Фамилия» в своей рабочей папке.

Часть С

Задание 5. Работа с отчетом.

Просмотрите отчет о выполнении архивации. Сохраните отчет в своей рабочей папке с именем «Отчет по архивации». Дайте ответы на следующие вопросы:

- Сколько времени длилась архивация?
- Сколько файлов обработано?
- Сколько места занимает архив?
- Какие были сбои архивации? Укажите причины сбоев.
- Какая операция, кроме архивации, выполнялась?

Задание 6. Выполните восстановление данных с помощью созданного вами архива. Восстановление выполняйте в режиме мастера. Сделайте скриншоты каждого этапа настройки восстановления данных и сохраните их в текстовом файле «Отчет_ПР9_Фамилия» в своей рабочей папке.

Вариант 2

Часть А

Задание 1. Дайте понятие архивации и резервного копирования.

Задание 2. Заполните таблицу:

Типы архивации	Назначение	Наличие атрибута «Архивный»	Восстановление данных (указать файлы, необходимые для восстановления данных)

Часть В

Задание 3. Разработайте и начертите схему процесса восстановления (указать все этапы восстановления, включая дополнительные настройки).

Задание 4. Выполните обычную архивацию папки «Program Files». Архивацию выполняйте в режиме мастера архивации. Архив сохраните в своей рабочей папке. Имя архива – «Архив_Фамилия_Windows». Сделайте скриншоты каждого этапа настройки архивации и сохраните их в текстовом файле «Отчет_ПР9_Фамилия» в своей рабочей папке.

Часть С

Задание 5. Работа с отчетом.

Просмотрите отчет о выполнении архивации. Сохраните отчет в своей рабочей папке с именем «Отчет по архивации». Дайте ответы на следующие вопросы:

- Сколько времени длилась архивация?

– Сколько файлов обработано?
– Сколько места занимает архив?
– Какие были сбои архивации? Укажите причины сбоев.
– Какая операция, кроме архивации, выполнялась?

Задание 6. Выполните восстановление данных с помощью созданного вами архива. Восстановление выполняйте в режиме мастера. Сделайте скриншоты каждого этапа настройки восстановления данных и сохраните их в текстовом файле «Отчет_ПР9_Фамилия» в своей рабочей папке.

Контрольные вопросы:

1. В чем заключается отличие операции резервирования от операции архивации?
2. Какую функцию выполняет опция «Всегда запускать в режиме мастера»?
3. Как необходимо хранить резервные копии и архивные файлы?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

– порядковый номер и наименование практической работы;
– цель практической работы;
– ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
– ответы на контрольные вопросы;
– вывод о выполненном задании.

Практическая работа № 10

Предотвращение и исправление ошибок жесткого диска

Цель: выполнить проверку жесткого диска на наличие ошибок и устранить ошибки встроенными средствами операционной системы.

Средства обучения:

– методические рекомендации к практической работе № 10;

– персональные компьютеры;

– проектор.

Виды самостоятельной работы:

– определение видов ошибок и причин их вызывающих;

– выявление ошибок жесткого диска;

– устранение ошибок жесткого диска;

– использование встроенных средств операционной системы для проверки жесткого диска на наличие ошибок и их устранение.

Краткая теоретическая справка

Неблагоприятные факторы, влияющие на работу жестких дисков:

Обычный износ и поломки. Когда ПК работает, жесткий диск вращается со скоростью от 5400-10000 оборотов в минуту. Даже если пользователь ничего не делает, диск работает. Только по этой причине большинство жестких дисков через несколько лет попросту изнашиваются.

Удары и сотрясения. Жесткий диск имеет головки чтения и записи. Эти головки плавают на воздушной подушке прямо над вращающимися дисками. Удар или тряска достаточной интенсивности может привести к удару головок о поверхность дисков, что может повредить данные. Если это окажется особенно важная область данных, жесткий диск может в целом выйти из строя.

Перенапряжения. В нормальных условиях амплитуда питающего напряжения относительно постоянна. Однако компьютер может подвергаться значительным перенапряжениям. Эти перенапряжения могут нарушить организацию данных жесткого диска.

Перебои питания. Если питание пропадает во время работы в Windows, почти всегда теряются определенные данные, а в некоторых (крайне редких) случаях может быть нарушен доступ к жесткому диску.

Вирусы. К сожалению, вирусы в наше время очень распространены. Некоторые из них неопасные - они выводят остроумные сообщения или заставляют символы «выпадать» из экрана, но большинство из них уничтожают ценные данные.

Плохие программы. Некоторые недоработанные программы могут выходить из-под контроля и уничтожать большие массивы данных жесткого диска.

Для предотвращения потери данных в результате появления ошибок и поломок диска неплохо регулярно выполнять резервное копирование файлов и держать под рукой загрузочный диск. Однако Windows располагает программой «Проверка диска», которая проверяет диск на наличие ошибок и автоматически их исправляет. Эта программа не способна восстановить полностью разрушенный жесткий диск, но, по крайней мере, позволяет узнать, когда ему грозит опасность.

«Проверка диска» выполняет пакет тестов жесткого диска, включая поиск недопустимых имен файлов, недопустимых данных и меток времени файлов, дефектных секторов и недопустимых структур сжатия. В файловой системе программа «Проверка диска» отыскивает следующие ошибки:

- потерянные кластеры;
- дефектные кластеры;
- кластеры с перекрестными ссылками.

Потерянный кластер – это кластер, который, согласно файловой системе, связан с файлом, но не имеет ссылок на какую-либо запись в каталоге файлов. Потерянные кластеры обычно возникают в результате сбоя программ, перенапряжение и перебоев питания.

Если утилита «Проверка диска» обнаруживает потерянные кластеры, она предлагает удалить их или преобразовать в файлы корневой папки диска с именами FILE0000.CHK, FILE0001.CHK и т.д. Эти файлы можно просмотреть на предмет полезных данных и попытаться спасти их. Обычно эти файлы непригодны для использования, и большинство пользователей их просто удаляет.

Дефектным считается кластер, попадающий в одну из следующих трех категорий:

– запись файловой системы указывает на кластер 1. Это недопустимо, так как номера кластеров диска начинаются с 2;

– запись файловой системы указывает на номер кластера, превышающий общее число кластеров диска;

– запись файловой системы со значением 0 (что обычно обозначает неиспользуемый кластер), которая является частью цепочки кластеров.

При обнаружении дефектных кластеров программа предлагает преобразовать эти потерянные фрагменты файлов в файлы. Если дать положительный ответ, программа будет усекать файл путем замены

дефектного кластера маркером EOF (End of File - конец файла), а затем превращать потерянные фрагменты в файлы. В результате, вероятно, получатся усеченные части файлов, которые можно просматривать и пытаться сложить вместе. Но, скорее всего, эти файлы придется удалять.

Кластеры с перекрестными ссылками – это кластеры, которые каким-то образом оказались связанными с двумя различными файлами (или дважды с одним и тем же файлом).

Проверка диска предлагает удалить дефектные файлы, копировать кластер с перекрестными ссылками в каждый дефектный файл либо игнорировать все файлы с перекрестными ссылками. В большинстве случаев надежнее всего будет копировать кластер с перекрестными ссылками в каждый дефектный файл. Тогда, по крайней мере, один из дефектных файлов будет пригоден для использования.

Подготовка к выполнению программы «Проверка диска»

Для выполнения программы «Проверка диска» нужно выбрать команды меню Пуск/Программы/Стандартные/Служебные программы/ Проверка диска.

В открывшемся диалоговом окне в списке «Выберите диски, которые следует проверить», выделить один или несколько дисков, для которых требуется проверка.

Группа «Проверка» содержит две опции, которые определяют способ проверки дисков:

– *Стандартная.* Этот тест выявляет ошибки файловой системы, недопустимые имена, даты и время создания файлов, а также ошибки сжатия. В большинстве случаев этот тест занимает лишь несколько секунд.

– *Полная.* Этот тест выполняет стандартную проверку, а затем сканирует поверхность диска для выявления дефектных секторов. В зависимости от размера диска, этот тест может продолжаться час или два. Если выбран режим проверки «Полная», становится активной кнопка «Настройки». Эта кнопка открывает диалоговое окно «Режим проверки поверхности диска». Это диалоговое окно содержит следующие элементы управления:

– *Выполнить проверку следующих областей.* Переключатели этой группы определяют части физического диска, подвергаемые проверке:

- *системная область* – содержит главную загрузочную запись и другие структуры системы. Хотя программа «Проверка диска» не способна исправлять ошибки в этой области, указание на наличие ошибки может послужить сигналом, что диску угрожает сбой;

- *область данных* - содержит файлы и папки. Если «Проверка диска» обнаруживает здесь дефектные секторы, то может переместить данные на исправную часть диска и пометить секторы как дефектные (bad), чтобы никакие программы не использовали их в будущем.

– *Не производить проверку поверхности на запись.* Программа «Проверка диска» обычно выявляет дефектные секторы путем считывания каждого сектора и записи данных снова на диск. Если цикл чтения/записи выполняется успешно, сектор исправен. Для ускорения процесса сканирования можно установить этот флажок. При этом не будет производиться запись данных снова на диск.

– *Не исправлять ошибочные секторы в скрытых и системных файлах.* Отдельные программы подразумевают хранение некоторых скрытых и системных файлов в определенных кластерах. Если какая-либо часть этих файлов перемещается, работа программы может быть нарушена. Если установить этот флажок, программа «Проверка диска» не будет перемещать обнаруженные в скрытых и системных файлах дефектные секторы. (Конечно, если скрытый или системный файл содержит дефектный сектор, использующая файл программа может не работать, поэтому, пожалуй, лучше не устанавливать этот флажок.)

Выполнение тестирования

Перед выполнением программы «Проверка диска» остается решить, как она должна обрабатывать выявленные ошибки. Если требуется вывод сообщений об ошибках, чтобы пользователь мог принять решение об их обработке, нужно снять флажок «Исправлять ошибки автоматически».

Для запуска программы «Проверка диска» используется кнопка «Запуск». Программа начнет проверку диска. Индикатор состояния в нижней части окна будет иллюстрировать продвижение этого процесса. Когда программа обнаружит ошибку (а флажок «Исправлять ошибки автоматически» не установлен), появится диалоговое окно, в котором будет отображаться обнаруженная ошибка и предполагаемые действия. Для дополнительных настроек предназначена кнопка «Дополнительно».

Аудиторная работа

1. Дайте характеристику ошибок жесткого диска, ведущих к потере информации.

2. Опишите технологию проверки диска с помощью утилиты «Chkdsk».

3. Продемонстрируйте процесс проверки диска с помощью утилиты «Chkdsk».

4. Опишите технологию проверки диска посредством программы «Проверка диска».

5. Продемонстрируйте процесс проверки диска посредством программы «Проверка диска».

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Перечислите проявление неисправностей операционной системы, которые могут свидетельствовать о наличии ошибок на жестком диске.

Задание 2. Назовите виды ошибок и дайте их краткую характеристику.

Часть В

Задание 3. Заполните следующую таблицу:

Правила защиты жесткого диска

№ п/п	Правила	Приемы использования правил

Часть С

Задание 4. Выполните проверку диска D:. Используйте для этого программу «Проверка диска». Настройте программу так, чтобы выводились сведения об ошибках (см. теорию). Сделайте копии всех этапов запуска и настройки программы и сохраните их в текстовом документе. Текстовый документ сохраните в своей рабочей папке с именем «Отчет_ПР10_Фамилия».

В ходе выполнения проверки на экране будут появляться сообщения об ошибках. Запишите в отчет сведения о найденных ошибках. Запишите в отчет также итоговые результаты проверки диска. Сделайте скриншот итоговых результатов и разместите его в документе «Отчет_ПР10_Фамилия».

Вариант 2

Часть А

Задание 1. Перечислите причины возникновения ошибок на жестком диске.

Задание 2. Перечислите операции, которые выполняет программа Проверка диска.

Часть В

Задание 3. Заполните следующую таблицу:

Правила защиты жесткого диска

№ п/п	Правила	Приемы использования правил

Часть С

Задание 4. Выполните проверку диска С:. Используйте для этого программу «Проверка диска». Настройте программу так, чтобы выводились сведения об ошибках (см. теорию). Сделайте копии всех этапов запуска и настройки программы и сохраните их в текстовом документе. Текстовый документ сохраните в своей рабочей папке с именем «Отчет_ПР10_Фамилия».

В ходе выполнения проверки на экране будут появляться сообщения об ошибках. Запишите в отчет сведения о найденных ошибках. Запишите в отчет также итоговые результаты проверки диска. Сделайте скриншот итоговых результатов и разместите его в документе «Отчет_ПР10_Фамилия».

Контрольные вопросы:

1. Какие стандартные средства проверки дисков вы знаете?
2. Дайте понятие потерянного кластера.
3. Дайте понятие дефектного кластера.
4. Дайте понятие кластеров с перекрестными ссылками.
5. Какие виды проверок диска существуют?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;

– ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;

– ответы на контрольные вопросы;

– вывод о выполненном задании.

Практическая работа № 11
Использование программы CrystalDiskInfo для проверки жесткого диска

Цель: выполнить проверку жесткого диска на наличие ошибок с помощью программы CrystalDiskInfo;

провести анализ технических характеристик жесткого диска;

выявить имеющиеся ошибки жесткого диска.

Средства обучения:

– методические рекомендации к практической работе № 11;

– персональные компьютеры;

– проектор.

Виды самостоятельной работы:

– определение видов ошибок и причин их вызывающих;

– выявление ошибок жесткого диска;

– устранение ошибок жесткого диска;

– использование программы CrystalDiskInfo для проверки жесткого диска на наличие ошибок и их устранение.

Краткая теоретическая справка

Среди множества утилит, которые предоставляют информацию о работе винчестера, большим объемом выдаваемых данных характеризируется программа CrystalDiskInfo. Данное приложение выполняет глубокий S.M.A.R.T.-анализ дисков. **S.M.A.R.T.** (**S**elf-**M**onitoring, **A**nalysis and **R**eporting **T**echnology), что в переводе означает - технология самоконтроля, анализа и отчётности предназначена для оценки внутреннего состояния диска и предсказания его возможных неисправностей. Контролируется достаточно большой набор параметров, на основе которых можно сделать вывод о состоянии жесткого диска.

Структура окна программы

После запуска программы на экране открывается окно-приложение, содержащее следующие элементы:

1. Панель дисков. На панели отображаются все диски, которые программа нашла в системе.

2. Панель основных характеристик. Содержит основные характеристики жесткого диска: производитель, полное название модели, объем, общее время работы и многое другое.

3. Панель индикаторов. На панели размещаются два индикатора, которые отображают общее состояние жесткого диска: индикатор технического состояния и индикатор температуры. Программа CrystalDiskInfo сама оценивает значения всех контролируемых параметров и выдает заключение об общем состоянии устройства и его температуре.

4. Панель параметров. На этой панели выводятся данные об основных параметрах, на основании которых CrystallDiskInfo делает вывод о состоянии жесткого диска. Программа анализирует каждый параметр и отмечает его состояние цветовым индикатором.

Просмотр информации о дисках

Обычно вся информация о жестком диске, на котором установлена операционная система, открывается сразу же после запуска программы. Программа отображает как техническую информацию (наименование диска, объем, температура, и т.д.), так и данные S.M.A.R.T.-анализа. Существует четыре варианта отображения параметров жесткого диска в программе CrystallDiskInfo: «хорошо», «внимание», «плохо» и «неизвестно». Каждая из этих характеристик отображается соответствующим цветом индикатора:

– «Хорошо» – синий или зеленый цвет (в зависимости от выбранной цветовой схемы);
– «Внимание» – желтый;
– «Плохо» – красный;
– «Неизвестно» – серый.

Данные оценки отображаются как относительно отдельных характеристик жесткого диска, так и ко всему накопителю в целом.

Если программа CrystalDiskInfo отмечает все элементы синим или зеленым цветом – с диском все в порядке. Если же присутствуют элементы, помеченные желтым, и, тем более красным цветом, то следует серьезно задуматься о ремонте накопителя.

Если требуется просмотреть информацию не о системном диске, а о каком-то другом накопителе, подключенном к компьютеру (включая внешние диски), то следует выбрать пункт меню «Диск», и в появившемся списке выбрать нужный носитель.

Запуск агента

Программа также предоставляет возможность запустить в системе собственного агента, который будет работать в трее в фоновом режиме, постоянно отслеживая состояние жесткого диска, и выводить сообщения только в том случае, если на нем обнаружатся неполадки. Для того, чтобы запустить агента, нужно в меню «Сервис» выбрать пункт «Запуск агента (в области уведомлений)».

В том же разделе меню «Сервис» пункт «Автозапуск» позволяет настроить приложение CrystalDiskInfo таким образом, что оно будет постоянно запускаться при загрузке операционной системы.

После проведения этих действий программа будет автоматически включаться после загрузки Windows, а её иконка будет отображаться в трее возле часов, где в маленькой иконке будет отображена текущая температура жесткого диска.

Регулирование работы жесткого диска

Приложение CrystalDiskInfo имеет некоторые возможности для регулирования работы жесткого диска. Для того, чтобы воспользоваться данной функцией, нужно в меню «Сервис», выбрать пункт «Дополнительно», а затем «Управление AAM/APM».

В открывшемся окне можно управлять двумя характеристиками жесткого диска – шумом и энергопитанием, перетаскивая ползунок из одной стороны в другую.

Кроме того, в том же подразделе «Дополнительно» можно выбрать параметр «Автонастройка AAM/APM». В этом случае, программа сама будет определять оптимальные значения шумности и энергопитания.

Аудиторная работа

1. Опишите структуру окна программы CrystalDiskInfo.
2. Дайте характеристику элементов окна программы CrystalDiskInfo.
3. Опишите технологию работы программы CrystalDiskInfo.
4. Продемонстрируйте процесс работы программы CrystalDiskInfo.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Опишите назначение программы CrystalDiskInfo.

Задание 2. Заполните следующую таблицу:

Структура окна программы CrystalDiskInfo

№ п/п	Основные панели окна программы	Элементы управления, расположенные на панели	Назначение элементов

Часть B

Задание 3. Загрузите операционную систему под своей административной учетной записью. Скопируйте со съемного носителя папку «Crystaldisk.zip». Разархивируйте архив в свою рабочую папку. Загрузите программу «CrystalDiskInfo».

Задание 4. Сделайте копию открывшегося окна программы и сохраните ее в текстовом файле «Отчет_ПР11_Фамилия» в своей рабочей папке.

Задание 5. Внимательно просмотрите сведения, отображающиеся в окне программы, и запишите в отчет следующие сведения:

– техническое состояние жесткого диска;

– температура;

– серийный номер;

– количество и имена разделов жесткого диска;

– скорость вращения;

– общее время работы;

– атрибуты, отмеченные индикатором желтого цвета. Что это означает?

– атрибуты, отмеченные индикатором красного цвета. Что это означает?

– атрибуты, отмеченные индикатором серого цвета. Что это означает?

Часть C

Задание 6. Постройте графики для следующих категорий данных: температура воздушного потока, часы работы. Сделайте скриншоты полученных графиков и разместите их в документе «Отчет_ПР11_Фамилия».

Задание 7. Настройте программу так, чтобы состояние диска отображалось в системном трее. Сделайте скриншот настроек и скриншот панели задач и разместите их в документе «Отчет_ПР11_Фамилия».

Задание 8. Выполните настройку программы так, чтобы она сама определяла оптимальные значения шумности и электропитания. Сделайте скриншот настроек и поместите его в документе «Отчет_ПР11_Фамилия».

Задание 9. Измените внешний вид окна программы. Сделайте скриншот окна и поместите его в документе «Отчет_ПР11_Фамилия».

Вариант 2

Часть А

Задание 1. Опишите элементы окна программы CrystalDiskInfo.

Задание 2. Заполните следующую таблицу:

Возможности программы CrystalDiskInfo

№ п/п	Название операции	Назначение	Последовательность выполнения	Особенности

Часть В

Задание 3. Загрузите операционную систему под своей административной учетной записью. Скопируйте со съемного носителя папку «Crystaldisk.zip». Разархивируйте архив в свою рабочую папку. Загрузите программу «CrystalDiskInfo».

Задание 4. Сделайте копию открывшегося окна программы и сохраните ее в текстовом файле «Отчет_ПР11_Фамилия» в своей рабочей папке.

Задание 5. Внимательно просмотрите сведения, отображающиеся в окне программы, и запишите в отчет следующие сведения:

– техническое состояние жесткого диска;

– температура;

– серийный номер;

– количество и имена разделов жесткого диска;

– скорость вращения;

– общее время работы;

– атрибуты, отмеченные индикатором желтого цвета. Что это означает?

– атрибуты, отмеченные индикатором красного цвета. Что это означает?

– атрибуты, отмеченные индикатором серого цвета. Что это означает?

Часть С

Задание 6. Постройте графики для следующих категорий данных: температура воздушного потока, часы работы. Сделайте скриншоты полученных графиков и разместите их в документе «Отчет_ПР11_Фамилия».

Задание 7. Настройте программу так, чтобы состояние диска отображалось в системном трее. Сделайте скриншот настроек и скриншот панели задач и разместите их в документе «Отчет_ПР11_Фамилия».

Задание 8. Выполните настройку программы так, чтобы она сама определяла оптимальные значения шумности и электропитания. Сделайте скриншот настроек и поместите его в документе «Отчет_ПР11_Фамилия».

Задание 9. Измените внешний вид окна программы. Сделайте скриншот окна и поместите его в документе «Отчет_ПР11_Фамилия».

Контрольные вопросы:

1. Можно ли с помощью программы CrystalDiskInfo проверить внешний диск. Если да, то как это сделать?
2. Можно ли контролировать состояние жесткого диска, находясь не за данным компьютером? Если да, то как это сделать.

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 12
Восстановление данных программными средствами

Цель: освоить технологию восстановления данных программными средствами;

выполнить восстановление утерянных данных с помощью программы «Recuva».

Средства обучения:

- методические рекомендации к практической работе № 12;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- выполнение анализа утерянных файлов;

– определение файлов, которые можно восстановить;
– выполнение расширенного анализа данных;
– восстановление данных.

Краткая теоретическая справка

Существует множество программ для восстановления данных как платных, так и бесплатных. Все эти программы можно разделить на две группы: программы восстановления удаленных файлов и программы восстановления поврежденных данных.

Восстановление удаленных данных

Рассмотрим бесплатную программу «Recuva», которая поможет восстановить файлы после удаления с жесткого диска или другого носителя.

Достоинства программы:

- установочный файл «Recuva» весит чуть больше 4 Мб;
- инсталлированная утилита занимает на жестком диске 6 Мб;
- полностью бесплатная программа;
- русифицированный интерфейс;
- наличие мастера восстановления, позволяющего гибко настроить процедуру поиска удаленных файлов;
- возможность добавить в «Проводник» и «Корзину» опцию «Поиск удаленных файлов».

Опция «Поиск удаленных файлов» в Проводнике позволяет быстро запускать сканирование определенной папки, из которой были стерты данные.

Порядок восстановления:

1. При первом запуске появляется мастер восстановления. Можно отказаться от его использования и сразу получить доступ ко всем возможностям «Recuva».

2. Следующее окно – выбор типа файлов. Если утерян какой-то конкретный файл (документ, фотография, видео), то рекомендуется установить фильтр. Если нужно восстановить файлы разных форматов после форматирования накопителя, то устанавливают переключатель «Все файлы» (рис. 1).

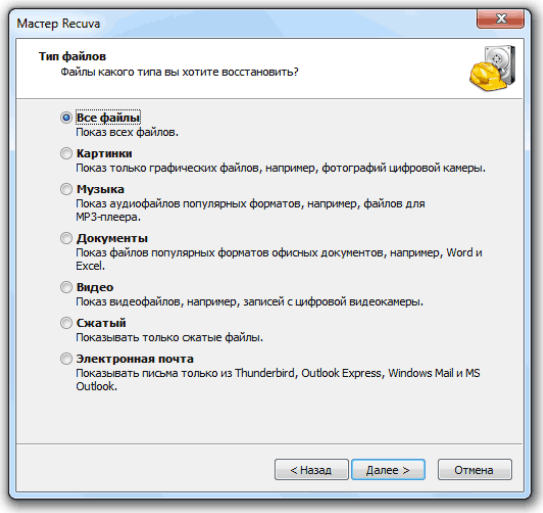

Рис. 1. Диалоговое окно «Мастер Recuva». Выбор типа данных

3. Размещение файла. Размещение файла лучше указать как можно более точно, чтобы ускорить поиск (рис. 2).

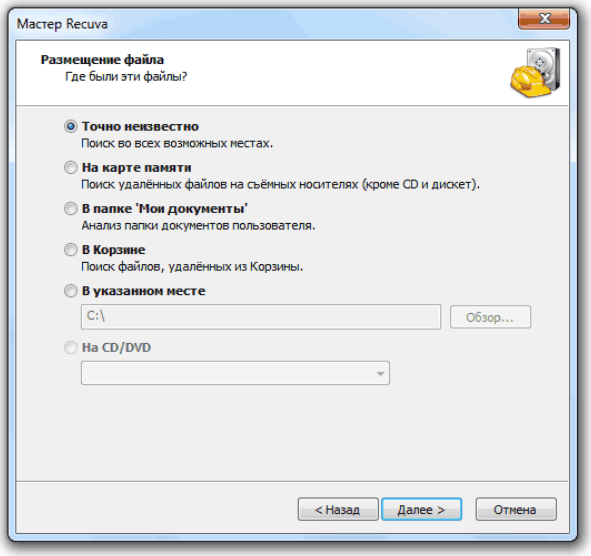

Рис. 2. Диалоговое окно «Мастер Recuva». Размещение файла

4. Углубленный анализ. Если данные были утеряны в результате форматирования, необходимо отметить опцию «Углубленный анализ» (рис. 3). Сканирование займет чуть больше времени, зато программа найдет больше файлов.

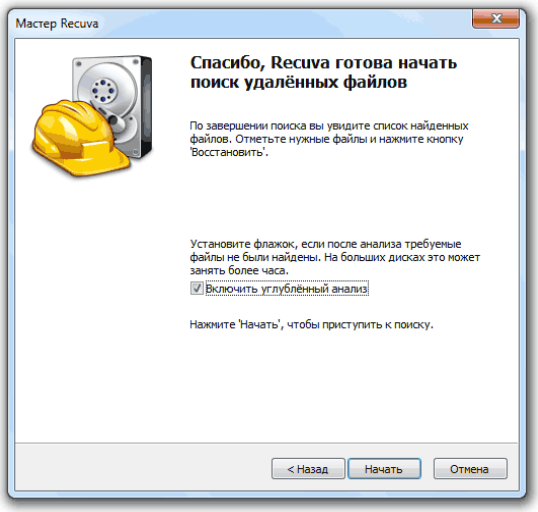

Рис. 3. Диалоговое окно «Мастер Recuva». Выбор углубленного анализа

5. Выбор файлов для восстановления. После завершения сканирования в окне программы отображается список найденных данных. Каждый файл помечается цветным кружком.

Цвет обозначает степень повреждения:

- зеленый – нет повреждений, файл готов к восстановлению;
- желтый – есть проблемы, файл может не открываться;
- красный – данные повреждены, восстановлению не подлежат.

Для восстановления файлов, нужно отметить их флажком и нажать кнопку «Восстановить». При восстановлении необходимо указать папку, которая находится на другом накопителе.

6. Использование расширенного режима. Чтобы перейти к расширенному режиму «Recuva», при запуске программы нужно отказаться от услуг мастера. В расширенном режиме необходимо указать, какие носители сканировать. Кнопка «Настройки» открывает диалоговое окно «Сервис».

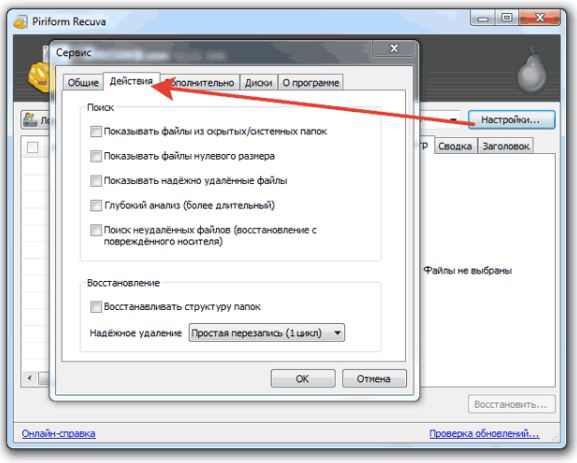

Рис. 4. Диалоговое окно «Сервис». Вкладка «Действия»

В этом окне на вкладке «Действия» можно установить опции: показ скрытых/системных файлов, файлов нулевого размера, надежно удаленных данных и неудаленных данных с поврежденного носителя. Эти опции позволяют увеличить эффективность сканирования и восстановить больше информации.

Недостатки программы:

– очень долгий (несколько часов) процесс проведения углублённого анализа данных при поиске и восстановлении файлов, даже если заданы упрощённые условия поиска (по типу файла и месту размещения);

– восстановление только файлов, состояние которых на момент нахождения программой идентифицировано как «Отличное» (файлы в среднем и плохом состоянии не восстановятся);

– невозможность восстановления файлов с момента удаления которых прошло достаточно много времени;

– невозможность восстановления файлов, поверх которых были записаны новые данные.

Аудиторная работа

1. Опишите структуру окна программы «Recuva».
2. Дайте характеристику элементов окна программы «Recuva».
3. Опишите технологию восстановления данных.
4. Продемонстрируйте процесс восстановления данных.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Заполните следующую таблицу:

Программа «Recuva»

Возможности программы	Достоинства программы	Недостатки программы

Задание 2. Загрузите операционную систему под своей административной учетной записью. Скопируйте со съемного носителя установочный файл программы «Recuva» в свою рабочую папку. Установите программу. При установке программы выберите русский язык.

Задание 3. Загрузите программу. Настройте анализ утерянных данных, пользуясь услугами мастера так, чтобы осуществлялся поиск файлов всех типов в «Корзине». Сделайте скриншоты всех этапов работы мастера и сохраните их в текстовом файле «Отчет_ПР12_Фамилия» в своей рабочей

папке. Запишите в отчет, сколько времени длился поиск и сколько файлов найдено?

Часть B

Задание 4. Выберите файлы типа «Документы» и восстановите их в папку D:\Группы\КСК21\Фамилия\Восстановленные файлы\Задание5.

Задание 5. Выполните анализ файлов всех типов, удаленных со всех разделов жесткого диска. Сделайте скриншоты этапов работы мастера и разместите их в документе «Отчет_ПР12_Фамилия». Запишите в отчет, сколько времени длился поиск и сколько файлов найдено?

Часть C

Задание 6. Восстановите графические файлы в папку D:\Группы\КСК21\Фамилия\ Восстановленные файлы\Задание7.

Задание 7. Откройте диалоговое окно «Сервис». Сделайте скриншоты всех вкладок этого окна и сохраните их в документе «Отчет_ПР12_Фамилия».

Задание 8. Выпишите в отчет какие настройки позволяет выполнять диалоговое окно «Сервис».

Вариант 2

Часть A

Задание 1. Внимательно рассмотрите представленное на рисунке диалоговое окно (рис. 5).

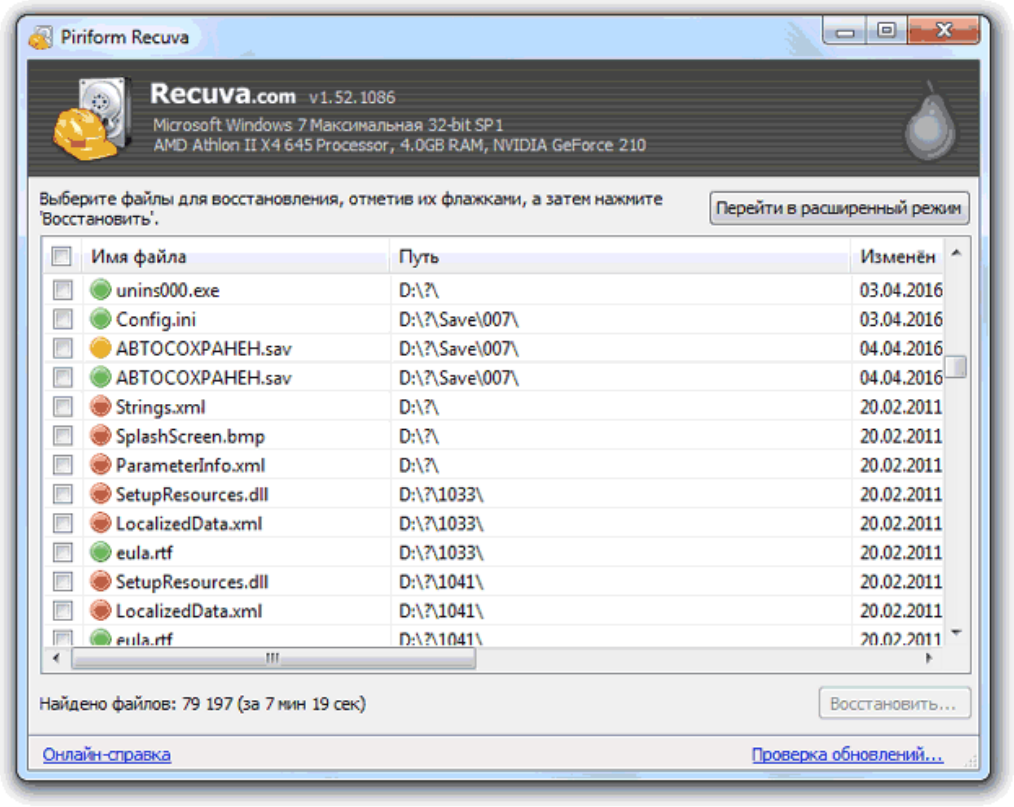

Рис. 5. Диалоговое окно программы

Дайте ответы на следующие вопросы:

– Окно какой программы вы видите на рисунке?

– Какой этап работы программы изображен на рисунке?

– Что можно сказать об операционной системе, установленной на ПК?

– Какая информация о ПК отображена в окне?

– Какие параметры анализа данных были установлены пользователем в данном случае?

– Какие файлы можно восстановить, а какие нельзя?

Задание 2. Загрузите операционную систему под своей административной учетной записью. Скопируйте со съемного носителя установочный файл программы «Recuva» в свою рабочую папку. Установите программу. При установке программы выберите русский язык.

Задание 3. Загрузите программу. Настройте анализ утерянных данных, пользуясь услугами мастера так, чтобы осуществлялся поиск файлов всех типов в «Корзине». Сделайте скриншоты всех этапов работы мастера и сохраните их в текстовом файле «Отчет_ПР12_Фамилия» в своей рабочей папке. Запишите в отчет, сколько времени длился поиск и сколько файлов найдено?

Часть В

Задание 4. Выберите файлы типа «Документы» и восстановите их в папку D:\Группы\КСК21\Фамилия\Восстановленные файлы\Задание5.

Задание 5. Выполните анализ файлов всех типов, удаленных со всех разделов жесткого диска. Сделайте скриншоты этапов работы мастера и разместите их в документе «Отчет_ПР12_Фамилия». Запишите в отчет, сколько времени длился поиск и сколько файлов найдено?

Часть С

Задание 6. Восстановите графические файлы в папку D:\Группы\КСК21\Фамилия\ Восстановленные файлы\Задание7.

Задание 7. Откройте диалоговое окно «Сервис». Сделайте скриншоты всех вкладок этого окна и сохраните их в документе «Отчет_ПР12_Фамилия».

Задание 8. Выпишите в отчет какие настройки позволяет выполнять диалоговое окно «Сервис».

Контрольные вопросы:

1. Опишите назначение программы «Recuva».
2. Как отмечается степень повреждения файлов?
3. Назовите причины, по которым файл не может быть восстановлен?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 13
Дефрагментация диска

Цель: выполнить дефрагментацию диска с помощью стандартных средств операционной системы.

Средства обучения:

- методические рекомендации к практической работе № 13;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- выполнение анализа фрагментации разделов жесткого диска;
- работа с отчетом по фрагментации разделов жесткого диска;
- выполнение дефрагментации разделов жесткого диска;
- работа с отчетом по дефрагментации разделов жесткого диска.

Краткая теоретическая справка

Структура жесткого диска

Жесткий диск, как и другие магнитные накопители, имеет дорожкообразную структуру, т.е. магнитный диск разбит на кольца разного диаметра начиная с внешнего края. Кольца, называемые дорожками,

состоят из секторов. Количество дорожек и секторов определяется форматом диска**.** Формат диска задается при его изготовлении и его изменить нельзя. Число дорожек жесткого диска 300 – 1000 и более. Независимо от числа дорожек они идентифицируются номером, начиная с нулевой внешней дорожки. Дорожка разбивается на равные секторы. Процесс разбития диска на секторы, называется форматированием. Число секторов на дорожке жестких дисков обычно составляет 17 - 150. Стандартный размер сектора - 512 байт и производители ПК редко отходят от такого размера.

Сектор - наименьшая адресуемая единица обмена данными дискового устройства с оперативной памятью.

Операционная система при работе с диском использует, как правило, собственную единицу дискового пространства, называемую кластером.

Стандартный размер кластера обычно 512 байт. (Но сейчас уже существует новый размер в 4 кб.)

Кластер — это единица хранения данных на диске в файловой системе. Кластер может содержать один или несколько секторов. Размер кластера можно изменить при форматировании.

Фрагментация

Файл записывается на диск не целиком, а «раскладывается» в кластеры. Т.е. файл разбивается на кусочки, соответствующие размеру кластера.

Изначально, пока на диске имеется достаточное количество свободного места, файл записывается в кластеры последовательно – один за другим. По мере заполнения носителя может возникать дефицит последовательных кластеров, (особенно в случае записи файлов большого размера) в этом случае система начинает искать свободные ячейки и распределять части файла по ним. Говорят, что файл фрагментирован.

Процесс разделения данных на отдельные части называется фрагментацией.

При считывании фрагментированного файла требуется время, чтобы найти все его части на диске и собрать их. Все это значительно снижает производительность компьютера и ресурс жесткого диска.

Дефрагментация

Дефрагментация диска предназначена для собирания разбросанных частей файлов в непрерывные последовательные кластеры. Можно сказать, что система попытается собрать фрагментированный файл в единое целое. Пустые разрозненные кластеры при этом процессе также будут соединены

в последовательные цепочки. Кроме этого, при дефрагментации большинство данных будут перемещены ближе к началу диска. Операция дефрагментации ускоряет запуск программ и загрузку данных. Перед началом процесса рекомендуется удалить неиспользуемые программы и данные.

Частота дефрагментации зависит от размера жесткого диска, от интенсивности его использования, от заполнения диска, от частоты установки и удаления программ.

В системе Windows есть стандартная программа, с помощью которой можно провести анализ выбранного локального диска на предмет необходимости его дефрагментации и непосредственно запуска самого процесса. Для запуска программы необходимо открыть диалоговое окно «Свойства диска». На вкладке «Сервис» нажать кнопку «Выполнить дефрагментацию»

В открывшемся окне дефрагментатора с помощью кнопки «Анализировать диск» запустить процесс проверки диска на степень фрагментации. После окончания анализа программа покажет, насколько фрагментирован диск. При степени фрагментации выше 15%, необходимо выполнить дефрагментацию диска.

Программу дефрагментации можно запустить также с помощью «Главного меню»: Пуск/Все программы/Стандартные/Служебные/ Дефрагментация диска.

Аудиторная работа

1. Охарактеризуйте понятия «Фрагментация» и «Дефрагментация».
2. Опишите технологию фрагментации диска.
3. Опишите технологию дефрагментации диска.
4. Продемонстрируйте процесс выполнения анализа диска на предмет фрагментации.
5. Продемонстрируйте процесс дефрагментации диска.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Опишите структуру жесткого диска.

Задание 2. Опишите процесс фрагментации диска.

Задание 3. Откройте программу дефрагментации диска. Выпишите в отчет состояние разделов жесткого диска. Сделайте скриншот первого этапа работы программы и сохраните его в текстовом файле «Отчет_ПР13_Фамилия» в своей рабочей папке.

Задание 4. Выполните анализ фрагментации раздела C:. Запишите в отчет требуется ли дефрагментация этого раздела. Выведите отчет о фрагментации раздела. Сохраните отчет в своей рабочей папке с именем «Анализ_Том C_Фамилия.txt».

Задание 5. Сделайте скриншот оценки использования диска до дефрагментации и разместите его в документе «Отчет_ПР13_Фамилия».

Часть B

Задание 6. Запустите процесс дефрагментации раздела C: жесткого диска. Сделайте два скриншота процесса дефрагментации (в начале и в конце процесса). Сделайте скриншот конечного результата. Скриншоты поместите в документ «Отчет_ПР13_Фамилия».

Задание 7. Выведите отчет о дефрагментации и сохраните его в своей рабочей папке с именем «Дефрагментация_Том C_Фамилия.txt».

Часть C

Задание 8. Сделайте сравнительную таблицу основных параметров раздела C: до и после дефрагментации (используйте файлы «Анализ_Том C_Фамилия.txt» и «Дефрагментация_Том C_Фамилия.txt»)

Вариант 2

Часть A

Задание 2. Внимательно рассмотрите представленное на рисунке изображение (рис. 1).

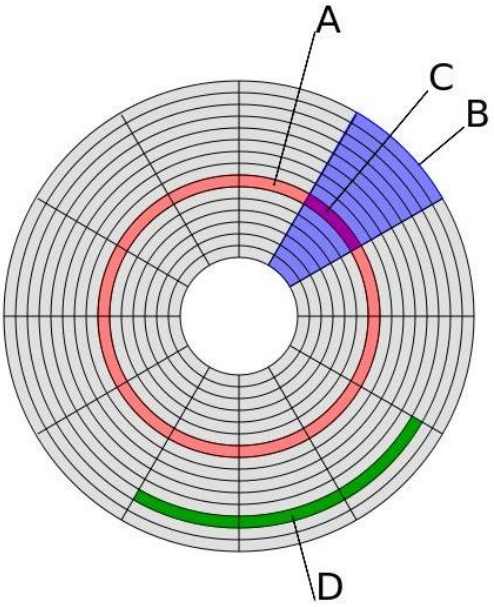

Рис. 1. Структура диска

Дайте ответы на следующие вопросы:

– Какая структура изображена на рисунке?
– Какие элементы отмечены буквами A, B, C, D?

Задание 2. Опишите процесс дефрагментации диска.

Задание 3. Откройте программу дефрагментации диска. Выпишите в отчет состояние разделов жесткого диска. Сделайте скриншот первого этапа работы программы и сохраните его в текстовом файле «Отчет_ПР13_Фамилия» в своей рабочей папке.

Задание 4. Выполните анализ фрагментации раздела D:. Запишите в отчет требуется ли дефрагментация этого раздела. Выведите отчет о фрагментации раздела. Сохраните отчет в своей рабочей папке с именем «Анализ_Том D_Фамилия.txt».

Задание 5. Сделайте скриншот оценки использования диска до дефрагментации и разместите его в документе «Отчет_ПР13_Фамилия».

Часть В

Задание 6. Запустите процесс дефрагментации раздела D: жесткого диска. Сделайте два скриншота процесса дефрагментации (в начале и в конце процесса). Сделайте скриншот конечного результата. Скриншоты поместите в документ «Отчет_ПР13_Фамилия».

Задание 7. Выведите отчет о дефрагментации и сохраните его в своей рабочей папке с именем «Дефрагментация_Том D_Фамилия.txt».

Часть С

Задание 8. Сделайте сравнительную таблицу основных параметров раздела D: до и после дефрагментации (используйте файлы «Анализ_Том D_Фамилия.txt» и «Дефрагментация_Том D_Фамилия.txt»)

Контрольные вопросы:

1. Что называется фрагментацией?
2. Что называется дефрагментацией?
3. Что представляет собой кластер?
4. Что представляет собой сектор?
5. В чем заключается разница между сектором и кластером?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 14
Кодирование текстовой информации

Цель: освоение приемов кодирования и декодирования текстовой информации.

Виды самостоятельной работы:

- кодирование информации с помощью кодировочных таблиц;
- декодирование информации с помощью кодировочных таблиц;
- кодирование информации с помощью алгоритма Хаффмана;
- декодирование информации с помощью алгоритма Хаффмана.

Краткая теоретическая справка

Информация, вводимая пользователем в компьютер, заменяется на специальные символы.

Набор условных обозначений (или сигналов) для записи (или передачи) некоторых заранее определенных понятий называется кодом.

Процесс представления информации (сообщения) в виде кода называется кодированием.

В более узком смысле под термином «кодирование» часто понимают переход от одной формы представления информации к другой, более удобной для хранения, передачи или обработки.

Все множество символов, используемых для кодирования, называется алфавитом кодирования.

Декодирование – процесс обратного преобразования кода к форме исходной символьной системы, т.е. получение исходного сообщения.

Человечество использует шифрование (кодировку) текста с того самого момента, когда появилась первая секретная информация. На различных этапах развития человеческой мысли использовались различные приемы кодировки текста. Например,

– криптография – это тайнопись, система изменения письма с целью сделать текст непонятным для непосвященных лиц;

– азбука Морзе или неравномерный телеграфный код, в котором каждая буква или знак представлены своей комбинацией коротких элементарных посылок электрического тока (точек) и элементарных посылок утроенной продолжительности (тире);

– сурдожесты – язык жестов, используемый людьми с нарушениями слуха.

Один из самых первых известных методов шифрования носит имя римского императора Юлия Цезаря (I век до н.э.). Этот метод основан на замене каждой буквы шифруемого текста, на другую, путем смещения в алфавите от исходной буквы на фиксированное количество символов, причем алфавит читается по кругу, то есть после буквы я рассматривается а.

А какими же правилами пользуется компьютер при кодировании информации? Каждый символ заменяется определенным числом.

Числа в компьютере представляются с помощью нулей и единиц, т.е. компьютеры обычно работают в двоичной системе счисления и, следовательно, используют принцип двоичного кодирования информации.

Принцип двоичного кодирования информации заключается в следующем:

1. Каждому символу ставится в соответствие его порядковый номер. Номер символов выражается числом десятичной системы счисления.

2. Порядковый номер символа преобразуется в двоичный код. Этот код и обрабатывается компьютером.

При выводе информации работает принцип декодирования информации.

Принцип декодирования информации заключается в следующем:

1. Двоичный код переводится в десятичную систему счисления. Десятичное число является порядковым номером символа.

2. По этому номеру определяется символ.

Для выполнения кодирования и декодирования текстовой информации в компьютере используются специальные кодовые таблицы.

Для разных типов ЭВМ используются различные таблицы кодировки.

В качестве международного стандарта принята кодовая таблица ASCII (American Standard Code for Information Interchange - Американский стандартный код для информационного обмена).

Эта таблица содержит столько символов, сколько можно ввести со стандартной клавиатуры.

Таблица ASCII состоит из двух частей. Сюда входят функциональные клавиши, буквы латинского алфавита, цифры, знаки препинания, скобки и некоторые другие символы. Им соответствуют порядковые номера от 0 до 127, т.е. всего 128 кодов. Именно эта часть таблицы и является международным стандартом и называется базовой.

Вторая часть таблицы называется национальной и содержит разные варианты кодировок. В русских национальных кодировках в этой части таблицы размещаются символы русского алфавита. В настоящее время существует пять кодовых таблиц для русских букв (Windows, MS-DOS, КОИ-8, Mac, ISO).

С конца 90-х годов проблема стандартизации символьного кодирования решается введением нового международного стандарта, который называется Unicode. Это 16-разрядная кодировка, т.е. в ней на каждый символ отводится 2 байта памяти. Конечно, при этом объем занимаемой памяти увеличивается в 2 раза. Но зато такая кодовая таблица допускает включение до 65536 символов. Полная таблица Unicode включает в себя все существующие алфавиты мира, а также множество математических, музыкальных, химических и прочих символов (рис. 1).

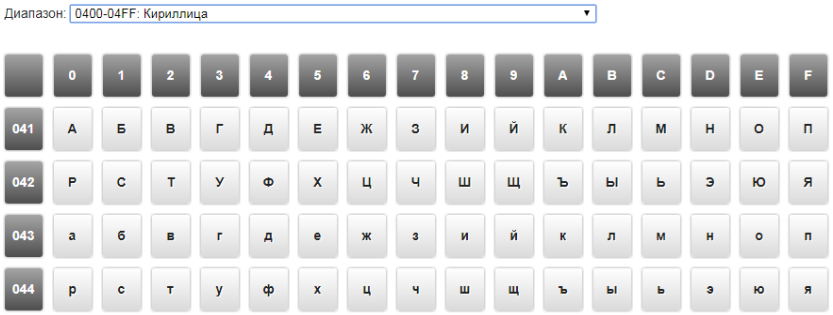

Рис. 1. Unicode.Таблица кодов русских букв

Сжатие текста. Алгоритм Хаффмана

При кодировании информации немало важным является занимаемый объем оперативной памяти. Поэтому необходимо познакомиться с таким понятием, как сжатие информации.

Сжатием информации называют такое преобразование, которое ведет к сокращению объема занимаемой памяти при сохранении закодированного содержания.

Одним из способов сжатия текстовой информации является алгоритм Хаффмана. Алгоритм был разработан в 1952 году американским ученым Дэвидом Хаффманом.

Идея алгоритма Хаффмана: по частоте вхождения символов в сообщение для них строятся коды переменной длины.

Символам с большей частотой присваиваются более короткие коды.

Наиболее частый символ сообщения кодируется наименьшим количеством битов, а наиболее редкий символ – наибольшим.

Дерево для алфавита английского языка с учётом частоты встречаемости его букв представлено на рисунке (рис. 2).

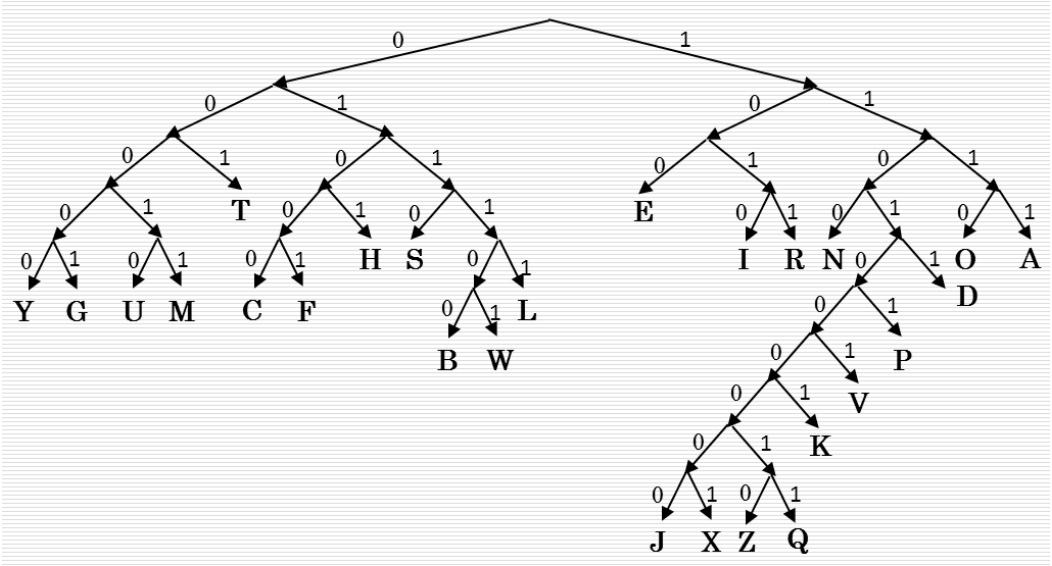

Рис. 2. Дерево Хаффмана

Рассмотрим пример. Необходимо закодировать слово «BIT». Находим нужные нам буквы и, двигаясь от корня дерева к буквам, определяем код каждой буквы: B – 011100, I – 1010, T – 001.

Теперь рассчитаем, какой объем памяти будет занимать информация при обычном кодировании (с помощью базовой таблицы ASCII) и при кодировании с помощью алгоритма Хаффмана.

Если пользоваться базовой таблицей кодирования, объем занимаемой оперативной памяти будет составлять 24 бита, т.к. каждая буква занимает 8 бит. При кодировании алгоритмом Хаффмана получаем 13 бит, что на 11 бит меньше, чем стандартное кодирование. Таким образом, использование алгоритма Хаффмана ведет к сжатию информации. Сжатие Хаффмана широко используется в программах архивации.

Аудиторная работа

1. Дайте характеристику понятий «Кодирование» и «Декодирование».

2. Рассчитать объем памяти, который будет занимать текстовое сообщение, содержащее 5 символов, после его кодирования с помощью таблицы ASCII.

3. Рассчитать объем памяти, который будет занимать текстовое сообщение, содержащее 5 символов, после его кодирования с помощью таблицы Unicode.

4. Закодировать слово «BYTE» с помощью алгоритма Хаффмана.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Опишите принцип кодирования информации.

Задание 2. Рассчитать какой объем памяти будет занимать текстовое сообщение, содержащее 15 символов, после его кодирования с помощью таблицы ASCII.

Задание 3. Закодировать слово «FILE» с помощью алгоритма Хаффмана.

Часть В

Задание 4. В последовательных ячейках оперативной памяти находится двоичный код слова: 01010000 01101000 01101001 01101100 01101001 01110000 01110011. Используется кодовая таблица ASCII (рис. 3). Какое слово отображается на экране?

0	☺ 1	☻ 2	♥ 3	♦ 4	♣ 5	♠ 6	• 7	◘ 8	○ 9	◙ 10	♂ 11	♀ 12	♪ 13	♫ 14	☼ 15
► 16	◄ 17	↕ 18	‼ 19	¶ 20	§ 21	▬ 22	↨ 23	↑ 24	↓ 25	→ 26	← 27	∟ 28	↔ 29	▲ 30	▼ 31
sp 32	! 33	" 34	# 35	$ 36	% 37	& 38	' 39	(40	) 41	* 42	+ 43	, 44	- 45	. 46	/ 47
0 48	1 49	2 50	3 51	4 52	5 53	6 54	7 55	8 56	9 57	: 58	; 59	< 60	= 61	> 62	? 63
@ 64	A 65	B 66	C 67	D 68	E 69	F 70	G 71	H 72	I 73	J 74	K 75	L 76	M 77	N 78	O 79
P 80	Q 81	R 82	S 83	T 84	U 85	V 86	W 87	X 88	Y 89	Z 90	[91	\ 92	] 93	^ 94	_ 95
` 96	a 97	b 98	c 99	d 100	e 101	f 102	g 103	h 104	i 105	j 106	k 107	l 108	m 109	n 110	o 111
p 112	q 113	r 114	s 115	t 116	u 117	v 118	w 119	x 120	y 121	z 122	{ 123	| 124	} 125	~ 126	⌂ 127

Рис. 3. Базовая таблица ASCII (коды символов 0 – 127)

Задание 5. Используя алгоритм сжатия Хаффмана, закодируйте слово «INTERNET». Определите, во сколько раз уменьшился объем в сравнении с однобайтовой кодировкой.

Часть С

Задание 6. Используя алгоритм сжатия Хаффмана, декодируйте слово 101110011111110111001011.

Задание 7. Автоматическое устройство осуществило перекодировку информационного сообщения длиной 48 символов, первоначально записанного в 7–битном коде ASCII, в 16–битную кодировку Unicode. На сколько байт увеличилось при этом информационное сообщение?

Вариант 2

Часть А

Задание 1. Опишите принцип декодирования информации.

Задание 2. Рассчитать объем памяти, который будет занимать текстовое сообщение, содержащее 15 символов, после его кодирования с помощью таблицы Unicode.

Задание 3. Закодировать слово «NEXT» с помощью алгоритма Хаффмана.

Часть В

Задание 4. В последовательных ячейках оперативной памяти находится двоичный код слова: 01001111 01010000 01000101 01010010 01000001 01010100 01001111 01010010. Используется кодовая таблица ASCII (рис. 3). Какое слово отображается на экране?

Задание 5. Используя алгоритм сжатия Хаффмана, закодируйте слово «INFORMATIKA». Определите, во сколько раз уменьшился объем в сравнении с однобайтовой кодировкой.

Часть С

Задание 6. Используя алгоритм сжатия Хаффмана, декодируйте слово 01100100011111100.

Задание 7. Автоматическое устройство осуществило перекодировку информационного сообщения длиной 54 символов, первоначально записанного в 7–битном коде ASCII, в 16–битную кодировку Unicode. На сколько байт увеличилось при этом информационное сообщение?

Контрольные вопросы:

1. Что называется кодом?
2. Что представляет собой криптография?
3. Опишите алгоритм Хаффмана.
4. Какие таблицы кодировки вы знаете?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 15
Шифрование информации симметричными методами

Цель: освоить технологию шифрования и дешифрования информации симметричными методами;

выполнить шифрование и дешифрование информации симметричными методами.

Средства обучения:

- методические рекомендации к практической работе № 15;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- шифрование и дешифрование информации методом Цезаря;
- шифрование и дешифрование информации методом Гронсфельда;
- шифрование и дешифрование информации методом Атбаш;
- шифрование и дешифрование информации методом цифрового шифра.

Краткая теоретическая справка

Шифр Цезаря

Шифр Цезаря — один из древнейших шифров. При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Естественным развитием шифра Цезаря стал шифр Виженера. С точки зрения современного криптоанализа, шифр Цезаря не имеет приемлемой стойкости.

Суть шифра состоит в замене каждой буквы на букву, отстоящую от нее в алфавите на 3 позиции вправо (возможен выбор любого ключа).

Подобные шифры, основанные на замене одних букв другими, называются подстановочными. Моноалфавитные шифры (к которым относится и шифр Цезаря) – это разновидность подстановочных шифров, в которой каждой букве нешифрованного текста всегда соответствует одна и та же буква в шифрованном тексте (рис. 1).

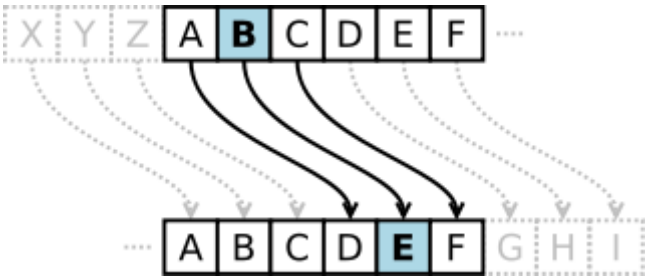

Рис. 1. Шифр Цезаря

Алфавит шифра представлен в таблице.

Алфавит шифра Цезаря

Буква	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**	**И**	**Й**
Номер	1	2	3	4	5	6	7	8	9	10	11
Буква	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**
Номер	12	13	14	15	16	17	18	19	20	21	22
Буква	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Ъ**	**Э**	**Ю**	**Я**
Номер	23	24	25	26	27	28	29	30	31	32	33

Пример:

Необходимо зашифровать сообщение по методу Цезаря.

Исходное сообщение: «Криптография».

Ключ – 3.

Решение:

Сообщение	**К**	**Р**	**И**	**П**	**Т**	**О**	**Г**	**Р**	**А**	**Ф**	**И**	**Я**
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 + 3	15	21	13	20	23	19	7	21	4	25	13	3
Шифр	**Н**	**У**	**Л**	**Т**	**Х**	**С**	**Ё**	**У**	**Г**	**Ч**	**Л**	**В**

Номер 1 – номер буквы согласно таблице.

Номер 1+3 – номер буквы согласно таблице + ключ (перемещаем букву на 3 позиции вперед).

Ответ: «Нултхсёугчлв».

Достоинством системы шифрования Цезаря является простота шифрования и расшифрования. К недостаткам системы Цезаря следует отнести следующие:

– подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста;

– сохраняется алфавитный порядок в последовательности заменяющих букв;

– шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте.

Однако, концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

Шифр Гронсфельда

Для шифрования здесь используется числовой ключ. Но каждая буква смещается не на постоянное число позиций, а на то число, которое соответствует ключу. Ключ соответственно состоит не из одной цифры, а из группы цифр.

Ключ не обязательно должен быть таким же длинным как шифруемое сообщение. Если ключ короче сообщения, то его просто повторяют по циклу. Так, например, если в тексте 10 символов, а длина ключа 5 символов, то для шифрования ключ будет использоваться 2 раза.

Пример:

Исходный текст: «шифр гронсфельда»

Ключ 15382

Решение представлено в таблице. Зашифрованный текст: «щнчш есуръцёрялв»

Исходный текст	Ш	И	Ф	Р		Г	Р	О	Н	С	Ф	Е	Л	Ь	Д	А
Ключ	1	5	3	8		2	1	5	3	8	2	1	5	3	8	2
Зашифрованный текст	Щ	Н	Ч	Ш		Е	С	У	Р	Ъ	Ц	Ё	Р	Я	Л	В

Шифр Атбаш

Еще один шифр простой (моноалфавитной) замены.

Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее.

Этот шифр использовался для еврейского алфавита и отсюда получил свое название.

Первая буква – алеф, заменяется на тау (последнюю), вторая буква – бет, заменяется на шин (предпоследнюю). Из этих букв и сформировалось название.

Шифр Атбаш для русского алфавита.

А Б В Г Д Е Ё 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 Ё Е Д Г В Б А.

Пример:

Исходное слово: замена.

Зашифрованное слово: чятъся.

Цифровые шифры

Алфавит разбивается на группы с равным числом букв, затем каждой группе присваивается свой номер. Так формируется первая цифра для шифровки символа. Вторая цифра – это порядковый номер буквы в группе. Распределение букв по группам представлено в таблице:

АБВГ	ДЕЖЗ	ИЙКЛ	МНОП	РСТУ	ФХЦЧ	ШЩЪЫ	ЬЭЮЯ
1	2	3	4	5	6	7	8

Таблица не обязательно должна выглядеть таким образом. Количество групп может быть другим. Также буквы из алфавита могут идти в таблице не по порядку.

Пример:

Зашифруем таким способом слово «цифра».

Зашифрованный текст: 63 31 61 51 11.

Аудиторная работа

1. Опишите технологию шифрования информации методом Цезаря.
2. Зашифровать слово «Студент» по методу Цезаря (ключ – 5).
3. Опишите технологию шифрования информации методом Гронсфельда.
4. Зашифровать слово «Знания» по методу Гронсфельда (ключ – 257).
5. Опишите технологию шифрования информации методом Атбаш.
6. Зашифровать слово «Отлично» по методу Атбаш.
7. Опишите технологию шифрования информации методом цифровых шифров.
8. Зашифровать слово «Технология» методу цифровых шифров.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Выполните шифрование пословицы «Где слова редки, там они вес имеют» методом Цезаря (ключ – 9).

Задание 2. Выполните декодирование сообщения «Уч ирем чурпш серу, кцрн шс цркф» методом Цезаря (ключ – 5).

Задание 3. Зашифруйте слово «Технология» по методу Гронсфельда (ключ – 3142).

Часть В

Задание 4. Расшифруйте слово «Ктчптоещйб» методом Гронсфельда (ключ – 25312).

Задание 5. Выполните шифрование сообщения «Защита информации» методом Атбаш.

Задание 6. Расшифруйте сообщение «Цтлспуяицсттяа юъчсряотсонг», зашифрованное методом Атбаш.

Часть С

Задание 7. Выполните шифрование сообщения «От глаз толку мало, если ум слеп» методом цифровых шифров.

Задание 8. Выполните дешифрование сообщения «11 42 53 31 13 31 51 54 52 42 11 84 24 11 72 31 53 11» методом цифровых шифров.

Вариант 2

Часть А

Задание 1. Выполните шифрование пословицы «Хорошее воспитание - лучшее наследство» методом Цезаря (ключ – 7).

Задание 2. Выполните декодирование сообщения «Хйфч нсшфчх сховые, цйнч нофч щйрьховые» методом Цезаря (ключ – 9).

Задание 3. Зашифруйте слово «Программа» по методу Гронсфельда (ключ – 4635).

Часть В

Задание 4. Расшифруйте слово «Хйцпфоудке» методом Гронсфельда (ключ – 35126).

Задание 5. Выполните шифрование сообщения «Методы шифрования» методом Атбаш.

Задание 6. Расшифруйте сообщение «Чяёцня цтлспуяицц», зашифрованное методом Атбаш.

Часть С

Задание 7. Выполните шифрование сообщения «Мало диплом иметь, надо дело разуметь» методом цифровых шифров.

Задание 8. Выполните дешифрование сообщения «44 51 43 14 51 11 41 41 42 43 22 43 12 22 52 44 22 64 22 42 31 22» методом цифровых шифров.

Контрольные вопросы:

1. Дайте понятие криптографии.
2. Какие методы шифрования называются симметричными?
3. Что такое ключ?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 16

Шифрование информации асимметричными методами

Цель: освоить технологию шифрования и дешифрования информации асимметричными методами;

научиться создавать открытые и закрытые ключи программными средствами;

научиться выполнять шифрование и дешифрование информации программными средствами.

Средства обучения:

- методические рекомендации к практической работе № 16;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- шифрование информации с помощью алгоритма RSA;
- создание открытого ключа в;
- создание закрытого ключа;
- шифрование и дешифрование информации программными средствами.

Краткая теоретическая справка

В ассиметричном шифровании используется 2 ключа – открытый и закрытый (тайный). Открытый ключ для шифрования, закрытый – для дешифрования.

Наиболее распространенные алгоритмы асимметричного шифрования:

- Rivest–Shamir–Adleman (RSA);
- Elliptic curve cryptosystem (ECC);
- Diffie–Hellman (DH);
- El Gamal.

Плюсы ассиметричных алгоритмов:

- можно свободно делиться открытым ключом и любой может отправить тебе тайное сообщение.

Минусы:

- скорость шифрования/дешифрования.

Алгоритм RSA

Алгоритм RSA был разработан в 1977 году Роном Ривестом, Ади Шамиром и Леном Адлеманом и опубликован в 1978 году. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом.

Алгоритм RSA состоит из трёх этапов:

1. Вычисление ключей. Важным моментом в этом криптоалгоритме является создание пары ключей: открытого и закрытого. Для алгоритма RSA этап создания ключей состоит из следующих операций:

   a) Выбираются два простых различных числа p и q. Вычисляется их произведение $n=p*q$, называемое модулем.

   b) Вычисляется функция Эйлера $\varphi(n)=(p-1)*(q-1)$.

   c) Выбирается произвольное число $e(e<n)$ такое, что $1<e<\varphi(n)$ и не имеет с числом $\varphi(n)$ других общих делителей, кроме 1 (т.е. оно является взаимно простым с ним).

   d) Вычисляется d (алгоритмом Евклида) таким образом, что ($e*d-1$) делилось на $\varphi(n)$.

   e) Два числа (e, n) публикуются как открытый ключ.

   f) Число d хранится в секрете. Пара (d, n) есть закрытый ключ, который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

2. Шифрование с помощью этих ключей производится следующим образом:

a) Отправитель разбивает своё сообщение M на блоки m_i. Значение $m_i<n$, поэтому длина блока открытого текста m_i в битах не больше $k=[log_2 n]$ бит, где квадратные скобки обозначают взятие целой части от дробного числа. Например, если $n=21$, то максимальная длина блока открытого текста $k=[log_2 21]=[4{,}39\ldots]$ = 4бита.

b) Подобный блок может быть интерпретирован как число из диапазона $(0;2^k-1)$. Для каждого такого числа m_i вычисляется выражение (c_i – зашифрованное сообщение):

$$c_i = (m_i)^e \bmod n.$$

В качестве размера блока зашифрованного текста следует брать $k_e=\lceil log_2 n \rceil$ бит, где операция $\lceil\ \rceil$ – это округление вверх до ближайшего целого. Необходимо добавлять нулевые биты слева в двоичное представление блока c_i до размера k_e бит.

3. Дешифрование производится следующим образом:

4. Чтобы получить открытый текст, надо каждый блок зашифрованного текста длиной k_e бит дешифровать отдельно:

$$m_i=(c_i)^d \bmod n.$$

Пример:

Выбрать два простых числа $p=7$, $q=17$.

Вычислить $n=p*q=7*17=119$.

Вычислить $\varphi(n)=(p-1)*(q-1)=96$.

Выбрать e так, чтобы e было взаимно простым с $\varphi(n)$ и меньше, чем $\varphi(n)$: $e=5$.

Определить d так, чтобы $d*e \equiv 1 \bmod 96$ и $d<96$: $d=77$, т.к. $77*5=385=4*96+1$.

Результирующие ключи: открытый ключ (5, 119) и закрытый ключ (77,119).

Пусть, например, требуется зашифровать сообщение $M=19$:

$$C=19^5=66 \pmod{119}.$$

Для дешифрования вычисляется $66^{77} \pmod{119}=19$.

Программа Gpg4usb

Алгоритм RSA лежит в основе многих программ, используемых для шифрования данных. Программа Gpg4usb является наиболее удобной и простой в использовании.

Данная программа использует PGP шифрование.

Для выполнения процедуры шифрования необходимо создать два ключа: открытый (для шифрования) и закрытый (для дешифрования). Для этого выполняется следующая последовательность действий:

1. В разделе «Менеджер ключей» выбираем в верхней панели кнопку «Ключ», затем команду «Генерировать ключ». На экране появится диалоговое окно «Генерировать ключ» (рис. 1)

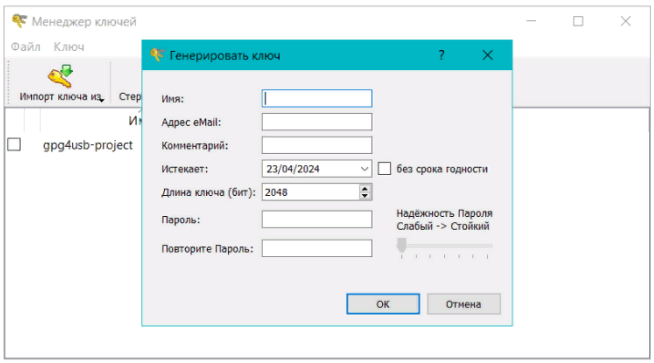

Рис. 1. Диалоговое окно «Генерировать ключ»

2. Пустые поля необходимо заполнить. Пароль нужно запомнить или записать, т.к. он понадобится в последующем для дешифрования сообщения.

Теперь ключ создан, можно приступать непосредственно к шифрованию.

На главном экране присутствует текстовое поле, которое используется для создания сообщений. В правой боковой панели помечается флажком свой ключ. Вводится сообщение в поле и кнопка «Зашифровать» (рис. 2).

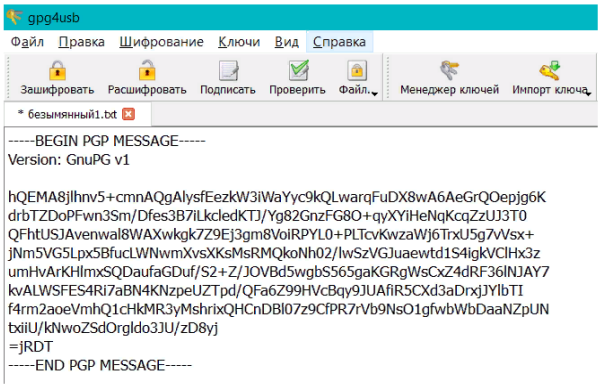

Рис. 2. Диалоговое окно программы. Зашифрованное сообщение

Процесс дешифровки происходит аналогично, вместо кнопки «Зашифровать» используется кнопка «Расшифровать».

Теперь необходимо передать сообщение и ключ. Для этого в окне, где создавались ключи для шифрования, помечается флажком нужный ключ и в верхней панели выбирается команда «Экспорт в файл» (рис. 3). Теперь ключ можно передавать кому угодно, чтобы получать зашифрованные сообщения.

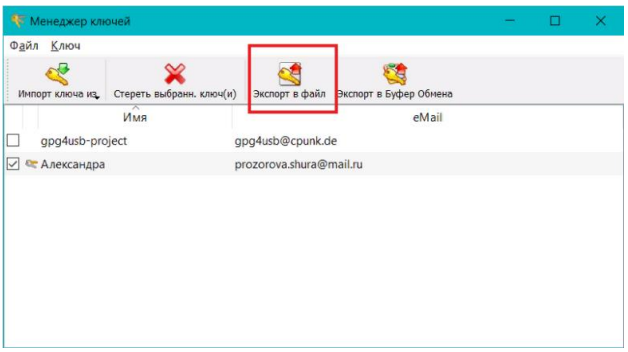

Рис. 3. Диалоговое окно «Экспорт ключей»

Чтобы получить закрытый ключ (для работы с другого компьютера, т.к. ключи хранятся локально), в главном окне программы в правой боковой панели вызывается контекстное меню для нужного ключа и выбирается пункт «Показать свойства ключа». А в открывшемся окне выбирается «Экспортировать Секретный ключ» (рис. 4).

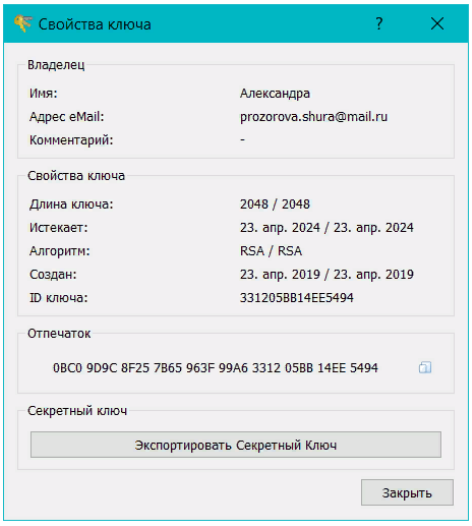

Рис. 4. Диалоговое окно «Свойства ключа»

Таким образом, были созданы открытый и закрытый ключи шифрования.

Аудиторная работа

1. Дайте понятия асимметричных методов шифрования.
2. Опишите алгоритм RSA.
3. Рассчитать открытый e и закрытый d ключи, пользуясь алгоритмом RSA для чисел p и q: p=29, q=7.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Загрузите операционную систему под своей административной учетной записью. Установите программу «Gpg4usb».

Сделайте скриншот главного окна программы и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Задание 2. Создайте открытый и закрытый ключи для шифрования и дешифрования информации. Сделайте скриншот, отображающий созданные ключи и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Задание 3. Выполните шифрование вашей фамилии и отправьте сообщение другу так, чтобы он смог его прочесть. Сделайте скриншот зашифрованного сообщения и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Часть B

Задание 4. Найти алгоритмом Евклида элемент *d* такой, что e*d≡1(mod n), если: *e*=15, *n*=82.

Задание 5. Выполните шифрование предложенного текста и отправьте сообщение другу. Сделайте скриншот зашифрованного сообщения и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Часть C

Задание 6. Выполните дешифрование полученного сообщения. Сделайте скриншот расшифрованного сообщения и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Задание 7. Используя значения *p* и *q*, построить ключевую пару (*e*, *d*) для алгоритма RSA, если *p*=11, *q*=23.

Вариант 2

Часть A

Задание 1. Загрузите операционную систему под своей административной учетной записью. Установите программу «Gpg4usb». Сделайте скриншот главного окна программы и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Задание 2. Создайте открытый и закрытый ключи для шифрования и дешифрования информации. Сделайте скриншот, отображающий созданные ключи и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Задание 3. Выполните шифрование вашей фамилии и отправьте сообщение другу так, чтобы он смог его прочесть. Сделайте скриншот зашифрованного сообщения и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Часть B

Задание 4. Найти алгоритмом Евклида элемент *d* такой, что e*d≡1(mod n), если: *e*=29, *n*=86.

Задание 5. Выполните шифрование предложенного текста и отправьте сообщение другу. Сделайте скриншот зашифрованного сообщения и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Часть C

Задание 6. Выполните дешифрование полученного сообщения. Сделайте скриншот расшифрованного сообщения и сохраните его в текстовом документе «Отчет_ПР16_Фамилия» в своей рабочей папке.

Задание 7. Используя значения *p* и *q*, построить ключевую пару (*e*, *d*) для алгоритма RSA, если *p*=19, *q*=11.

Контрольные вопросы:

1. В чём заключаются достоинства и недостатки асимметричных алгоритмов?
2. Что представляет собой открытый ключ?
3. Что представляет собой закрытый ключ?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 17
Установка и настройка параметров антивирусного программного обеспечения

Цель: выполнить установку антивирусного программного обеспечения и настройку параметров работы.

Средства обучения:

- методические рекомендации к практической работе № 17;
- персональные компьютеры;
- проектор.

Виды самостоятельной работы:

- анализ компьютерных вирусов;
- установка антивирусного программного обеспечения;
- настройка параметров антивирусного программного обеспечения;

Краткая теоретическая справка

Вирусы

Компьютерный вирус - это целенаправленно созданная программа, автоматически прописывающая себя к другим программным продуктам, изменяющая или уничтожающая их. Такая программа обладает способностью самовоспроизведения, распространения, внедрения в другие программы.

Вредоносные программы можно разделить на три класса: черви, вирусы и троянские программы**.**

Черви – это класс вредоносных программ, использующих для распространения сетевые ресурсы. «Черви» проникают в компьютер, вычисляют сетевые адреса других ПК и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов.

Вирусы – это программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов.

Троянская программа – программы, которые выполняют на пораженных ПК несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводя систему к зависанию, воруют конфиденциальную информацию и т.д.

В зависимости от среды обитания вирусы можно разделить на:

– *сетевые вирусы* распространяются по различным компьютерным сетям;

– *файловые вирусы* внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширение COM и EXE;

– *загрузочные вирусы* внедряются в загрузочный сектор диска или сектор, содержащий программу загрузки системы диска;

– *файлово-загрузочные* вирусы заражают файлы и загрузочные сектора дисков.

По способу заражения вирусы разделяются на резидентные и нерезидентные.

Резидентные вирусы при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения и внедряется в них.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

Признаки заражения компьютера вирусами:

– вывод на экран непредусмотренных сообщений или изображений;

– подача непредусмотренных сигналов;

– неожиданное открытие и закрытие CD-ROM-устройства;

– произвольный, без вашего участия, запуск на компьютере каких-либо программ;

– вывод на экран предупреждения о попытке какой-либо из программ вашего компьютера выйти в Интернет.

Антивирусная программа

Антивирусная программа – это программа, которая предотвращает заражение ПК компьютерными вирусами и позволяет устранить последствия заражения.

Различают следующие виды антивирусных программ:

– программы-детекторы;

– программы-доктора (фаги);

– программы-ревизоры;

– программы-фильтры;

– программы-вакцины или иммунизаторы.

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких

антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ (*AVSP).*

Программы-доктора или *фаги*, а также *программы-вакцины* не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. Наиболее известные из них: Norton AntiVirus, Doctor Web, антивирус Касперский.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора.

К числу программ-ревизоров относится программа «Adinf»*.*

Программы-фильтры или *«сторожа»* представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM, EXE;
- изменение атрибутов файла;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие (*программа Vsafe).*

Вакцины или *иммунизаторы* – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. В настоящее время программы-вакцины имеют ограниченное применение.

Основные меры по защите от вирусов:

– оснастите свой компьютер одной из современных антивирусных программ;

– постоянно обновляйте антивирусные базы;

– делайте архивные копии ценной для Вас информации (гибкие диски, CD).

Аудиторная работа

1. Проанализируйте классификацию вирусов по среде обитания.
2. Дайте характеристику классификации вирусов по способу заражения.
3. Перечислите признаки заражения компьютера вирусами.
4. Проведите анализ видов антивирусных программ.
5. Опишите технологию установки антивирусного программного обеспечения.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Подумайте в чем сходство и различие биологического и компьютерного вируса. Заполните таблицу:

Сходства	Различия
1. 2. 3.	1. 2. 3.

Задание 2. Перечислите профилактические меры, предохраняющие от потери или повреждения информации (8 – 10 пунктов).

Часть В

Задание 3. Заполните схему классификации вирусов (рис. 1).

Рис. 1. Схема «Классификация вирусов»

Задание 4. С помощью панели управления убедитесь, что антивирусное программное обеспечение на вашем компьютере не установлено. Сделайте скриншот списка программ, доказывающий, что

антивирусная программа не установлена. Сохраните скриншот в своей рабочей папке в текстовом файле «Отчет_ПР17_Фамилия».

Часть С

Задание 5. Установите со съемного носителя антивирусную программу. Скриншоты этапов установки сохраните в файле «Отчет_ПР17_Фамилия».

Задание 6. Проверьте готовность программы к работе.

Вариант 2

Часть А

Задание 1. Перечислите объекты компьютерной системы, заражение которых приведет к незначительным и необратимым последствиям. Заполните таблицу:

Незначительные разрушительные последствия	Необратимые разрушительные последствия
1. 2. 3.	1. 2. 3.

Задание 2. Перечислите внешние признаки проявления деятельности вирусов.

Часть В

Задание 3. Заполните таблицу «Классификация вирусов»

Классификация вирусов

Группа вирусов	Вредоносное действие вирусов
по масштабу вредных воздействий	
По среде обитания	

Задание 4. С помощью панели управления убедитесь, что антивирусное программное обеспечение на вашем компьютере не установлено. Сделайте скриншот списка программ, доказывающий, что антивирусная программа не установлена. Сохраните скриншот в своей рабочей папке в текстовом файле «Отчет_ПР17_Фамилия».

Часть С

Задание 5. Установите со съемного носителя антивирусную программу. Скриншоты этапов установки сохраните в файле «Отчет_ПР17_Фамилия».

Задание 6. Проверьте готовность программы к работе.

Контрольные вопросы:

1. Что называется вирусом?
2. Какие основные три класса вредоносных программ можно выделить?
3. Перечислите основные методы борьбы с вирусами.

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

Практическая работа № 18
Установка и настройка параметров антивирусного программного обеспечения

Цель: выполнить настройку параметров работы антивирусного программного обеспечения;

выполнить проверку, лечение и удаление зараженных объектов информационной системы, используя установленное антивирусное программное обеспечение.

Средства обучения:

– методические рекомендации к практической работе № 18;

– персональные компьютеры;

– проектор.

Виды самостоятельной работы:

– анализ антивирусного программного обеспечения;

– настройка антивирусного программного обеспечения;

– проверка информационной системы на наличие зараженных объектов;

– лечение зараженных объектов;

– удаление зараженных объектов.

Краткая теоретическая справка

Антивирусные программы - это программы, основной задачей которых является защита именно от вирусов, или точнее, от вредоносных программ.

Методы и принципы защиты теоретически не имеют особого значения, главное чтобы они были направлены на борьбу с вредоносными программами. Но на практике дело обстоит несколько иначе: практически любая антивирусная программа объединяет в разных пропорциях все технологии и методы защиты от вирусов, созданные к сегодняшнему дню. Из всех методов антивирусной защиты можно выделить две основные группы:

– Сигнатурные методы - точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.

– Эвристические методы - приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Сигнатурный анализ

Слово «Сигнатура» в данном случае является калькой на английское «signature», означающее «подпись» или же в переносном смысле «характерная черта, нечто идентифицирующее». Сигнатурный анализ заключается в выявлении характерных идентифицирующих черт каждого вируса и поиска вирусов путем сравнения файлов с выявленными чертами. Сигнатурой вируса будет считаться совокупность черт, позволяющих однозначно идентифицировать наличие вируса в файле (включая случаи, когда файл целиком является вирусом). Все вместе сигнатуры известных вирусов составляют антивирусную базу. Задачу выделения сигнатур, как

правило, решают люди - эксперты в области компьютерной вирусологии, способные выделить код вируса из кода программы и сформулировать его характерные черты в форме, наиболее удобной для поиска.

Эвристический анализ

Слово «эвристика» происходит от греческого глагола «находить». Суть эвристических методов состоит в том, что решение проблемы основывается на некоторых правдоподобных предположениях, а не на строгих выводах из имеющихся фактов и предпосылок. Эвристический анализ основывается на (весьма правдоподобном) предположении, что новые вирусы часто оказываются похожи на какие-либо из уже известных. Постфактум такое предположение оправдывается наличием в антивирусных базах сигнатур для определения не одного, а сразу нескольких вирусов. Основанный на таком предположении эвристический метод заключается в поиске файлов, которые не полностью, но очень близко соответствуют сигнатурам известных вирусов. Положительным эффектом от использования этого метода является возможность обнаружить новые вирусы еще до того, как для них будут выделены сигнатуры.

Карантин

Среди вспомогательных средств во многих антивирусах есть специальные технологии, которые защищают от возможной потери данных в результате действий антивируса. Например, легко представить ситуацию, при которой файл детектируется как возможно зараженный эвристическим анализатором и удаляется согласно настройкам антивируса. Однако эвристический анализатор никогда не дает стопроцентной гарантии того, что файл действительно заражен, а значит с определенной вероятностью антивирус мог удалить незараженный файл. Или же антивирус обнаруживает важный документ зараженный вирусом и пытается согласно настройкам выполнить лечение, но по каким-то причинам происходит сбой и вместе с вылеченным вирусом теряется важная информация. Разумеется, от таких случаев желательно застраховаться. Проще всего это сделать, если перед лечением или удалением файлов сохранить их резервные копии, тогда если окажется, что файл был удален ошибочно или была потеряна важная информация, всегда можно будет выполнить восстановление из резервной копии.

Тестирование работы антивируса

После того как антивирус установлен и настроен, каждый пользователь хочет убедиться, что он все сделал правильно и антивирусная защита работает. Значит нужен такой способ тестирования антивирусов,

который был бы безопасным, но давал четкий ответ на вопрос, корректно ли работает антивирус. Понимая важность проблемы, организация EICAR при участии антивирусных компаний создала специальный тестовый файл, который был назван по имени организации – eicar.com.com. Это исполняемый файл в COM-формате, который не выполняет никаких вредоносных действий, а просто выводит на экран строку "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!".

Тестирование антивируса при помощи eicar.com тоже не идеально. Eicar.com в первую очередь позволяет протестировать, как антивирус справляется с файловыми вирусами и близкими по структуре вредоносными программами – большинством троянов, некоторыми червями.

Режимы работы антивирусов

Надежность антивирусной защиты обеспечивается не только способностью отражать любые вирусные атаки. Другое не менее важное свойство защиты - ее непрерывность. Это означает, что антивирус должен начинать работу по возможности до того, как вирусы смогут заразить только что включенный компьютер и выключаться только после завершения работы всех программ. Однако с другой стороны, пользователь должен иметь возможность в любой момент запросить максимум ресурсов компьютера для решения своей, прикладной задачи и антивирусная защита не должна ему помешать это сделать. Оптимальный выход в этой ситуации - это введение двух различных режимов работы антивирусных средств: один с небольшой функциональностью, но работающий постоянно, и второй - тщательная и более ресурсоемкая проверка на наличие вирусов по запросу пользователя. Такое разделение принято в большинстве современных антивирусов.

Проверка в режиме реального времени

Проверка в режиме реального времени, или постоянная проверка, обеспечивает непрерывность работы антивирусной защиты. Это реализуется с помощью обязательной проверки всех действий, совершаемых другими программами и самим пользователем, на предмет вредоносности, вне зависимости от их исходного расположения - будь это свой жесткий диск, внешние носители информации, другие сетевые ресурсы или собственная оперативная память.

Проверка по требованию

Для такого режима обычно предполагается, что пользователь лично укажет какие файлы, каталоги или области диска необходимо проверить и

время, когда нужно произвести такую проверку - в виде расписания или разового запуска вручную.

Антивирусные комплексы

Антивирусный комплекс - набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем.

В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз. Всякая локальная сеть, как правило, содержит компьютеры двух типов - рабочие станции, за которыми непосредственно сидят люди, и сетевые серверы, используемые для служебных целей. В соответствии с характером выполняемых функций сервера делятся на:

– *сетевые*, которые обеспечивают централизованное хранилище информации: файловые сервера, сервера приложений и другие;

– *почтовые*, на которых работает программа, служащая для передачи электронных сообщений от одного компьютера к другому;

– *шлюзы*, отвечающие за передачу информации из одной сети в другую. Например, шлюз необходим для соединения локальной сети с Интернет.

Рабочие станции - это компьютеры локальной сети, за которыми непосредственно работают пользователи. Главной задачей комплекса для защиты рабочих станций является обеспечение безопасной работы на рассматриваемом компьютере. Для этого необходима проверка в режиме реального времени, проверка по требованию и проверка локальной электронной почты.

Сетевые сервера - это компьютеры, специально выделенные для хранения или обработки информации. Они обычно не используются для непосредственной работы за ними и поэтому в отличие от рабочих станций проверка электронной почты на наличие вирусов тут не нужна. Следовательно, антивирусный комплекс для файловых серверов должен производить проверку в режиме реального времени и проверку по требованию.

Аудиторная работа

1. Дайте характеристику методов антивирусной защиты.
2. Проведите анализ режимов работ антивирусного программного обеспечения.
3. Дайте характеристику антивирусных комплексов.

Самостоятельная работа

Вариант 1

Часть А

Задание 1. Перечислите критерии качества антивирусных программ (4+).

Задание 2. Загрузите установленную вами программу и выполните проверку съемного носителя. Сделайте скриншоты, подтверждающие, выполненную вами работу (установка параметров работы антивирусной программы и результаты работы) и сохраните их в текстовом документе «Отчет_ПР18_Фамилия» в своей рабочей папке.

Часть В

Задание 3. Заполните таблицу «Классификация антивирусных программ».

Наименование	Назначение	Метод обнаружения вирусов	Достоинства	Недостатки

Часть С

Задание 4. Загрузите установленную вами программу и выполните проверку дисков C: и D:. Выполните лечение или удаление вирусов, обнаруженных программой. Сделайте скриншоты, подтверждающие, выполненную вами работу (установка параметров работы антивирусной программы и результаты работы) и сохраните их в текстовом документе «Отчет_ПР18_Фамилия» в своей рабочей папке.

Задание 5. В отчете заполните следующую таблицу:

Название антивирусной программы	
Проверяемый логический или физический диск (диски)	
Всего проверено файлов	
Число зараженных файлов	
Число подозрительных файлов	
Число потенциально опасных, но разрешенных к использованию файлов	
Число вылеченных файлов	

Вариант 2

Часть А

Задание 1. Перечислим наиболее распространенные антивирусные программные комплексы (3+).

Задание 2. Загрузите установленную вами программу и выполните проверку съемного носителя. Сделайте скриншоты, подтверждающие, выполненную вами работу (установка параметров работы антивирусной программы и результаты работы) и сохраните их в текстовом документе «Отчет_ПР18_Фамилия» в своей рабочей папке.

Часть В

Задание 3. Заполните таблицу «Классификация антивирусных программ»

Наименование	Назначение	Метод обнаружения вирусов	Достоинства	Недостатки

Часть С

Задание 4. Загрузите установленную вами программу и выполните проверку дисков C: и D:. Выполните лечение или удаление вирусов, обнаруженных программой. Сделайте скриншоты, подтверждающие, выполненную вами работу (установка параметров работы антивирусной программы и результаты работы) и сохраните их в текстовом документе «Отчет_ПР18_Фамилия» в своей рабочей папке.

Задание 5. В отчете заполните следующую таблицу:

Название антивирусной программы	
Проверяемый логический или физический диск (диски)	
Всего проверено файлов	
Число зараженных файлов	
Число подозрительных файлов	
Число потенциально опасных, но разрешенных к использованию файлов	
Число вылеченных файлов	

Контрольные вопросы:

1. Что представляют собой антивирусные программы?
2. Что представляет собой карантин?
3. Для чего проводится тестирование антивируса?
4. Что представляют собой антивирусные комплексы?

Критерии оценки:

Отметка *«отлично»* ставится, если правильно выполнены задания аудиторной работы, частей А, В, С самостоятельной работы.

Отметка *«хорошо»* ставится, если правильно выполнены задания аудиторной работы, частей А, В самостоятельной работы.

Отметка *«удовлетворительно»* ставится, если правильно выполнены задания аудиторной работы, части А самостоятельной работы.

Отметка *«неудовлетворительно»* ставится, если с ошибками выполнены задания аудиторной работы, части А самостоятельной работы.

Требования к отчету:

После выполнения работы студент обязан продемонстрировать преподавателю отчёт о выполненной работе, содержащий:

- порядковый номер и наименование практической работы;
- цель практической работы;
- ход выполнения работы, включающий в себя выполненные задания аудиторной и самостоятельной работ;
- ответы на контрольные вопросы;
- вывод о выполненном задании.

СПИСОК ЛИТЕРАТУРЫ

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2018. –416 с.

2. Шаньгин В.Ф. Информационная безопасность. – М.: ДМК Пресс, 2017. – 702 с.

3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. защита информации техническими средствами: учебное пособие. – СПб: НИУ ИТМО, 2016. –416 с.

4. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебник для среднего профессионального образования. – М.: ФОРУМ: ИНФРА – М, 2015. –368 с.

5. Максимов Н.В., Партыка Т.Л., Попов И.И. Архитектура ЭВМ и вычислительных систем: Учебник. – М.: ФОРУМ: ИНФРА – М, 2016. –512 с.

6. Исаев А.Б. Современные технические методы и средства защиты информации: Учеб. пособие. – М.: РУДН, 2015. –253 с.

Интернет-ресурсы:

1. Методы и средства защиты информации [Электронный ресурс] URL: http://www.melnikoff.com/yuriv/posobie.htm.

2. Методы защиты информации [Электронный ресурс] URL: http://wiki.kiit-tsu.ru/index.php.