МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

Методические рекомендации
по практическим занятиям
междисциплинарного курса: МДК.02.01 Программные и программно-аппаратные средства защиты информации

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника: Техник по защите информации

Нормативный срок обучения: 3 года 10 месяцев

Форма обучения: Очная

2021

Методические указания по практическим занятиям междисциплинарного курса: МДК.02.01 Программные и программно-аппаратные средства защиты информации разработаны на основе федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.15 Обеспечение информационной безопасности автоматизированных систем Утвержденным приказом Минобрнауки России от 09.12.2016г. №1553

дата утверждения и №)

Методические указания рассмотрены на заседании методического совета СПК и рекомендованы к использованию

«19» 02. 2020 года Протокол № __1__

Председатель методического совета СПК

Сергеева Светлана Ивановна _____

Методические указания утверждены на заседании педагогического совета СПК «28» 02. 2020 года Протокол № _6__

Председатель педагогического совета СПК

Облиенко Алексей Владимирович _____

Организация-разработчик: ФГБОУ ВО «ВГТУ»

Разработчики:

__ Демихова Ирина Владимировна_____

(Ф.И.О., ученая степень, звание, должность

_____

(Ф.И.О., ученая степень, звание, должность)

_____

(Ф.И.О., ученая степень, звание, должность)

_____

(Ф.И.О., ученая степень, звание, должность)

ПРАКТИЧЕСКАЯ РАБОТА № 1

Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.

Цель: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

Теоретические вопросы

1. Предмет и задачи программно-аппаратной защиты информации.
2. Основные понятия программно-аппаратной защиты информации.
3. Классификация методов и средств программно-аппаратной защиты информации.
4. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Приложение перечень основных нормативных документов, регламентирующих деятельность области защиты информации:

– Конституция Российской Федерации;

– Гражданский Кодекс Российской Федерации

– Уголовный Кодекс Российской Федерации

– Доктрина информационной безопасности Российской Федерации;

– Законы Российской Федерации:

• Федеральный закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»;

• Федеральный закон РФ от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

• Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

• Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

• Федеральный закон от 29.04.2004 № 98-ФЗ «О коммерческой тайне»;

– Указы Президента Российской Федерации:

• Указ Президента РФ от 30 ноября 1995 г. №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;

• Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;

– Постановления Правительства Российской Федерации:

• Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

• Постановление Правительства РФ от 03.02.2012 № 79 "О лицензировании деятельности по технической защите конфиденциальной информации";

– Документы ФСТЭК, ФСБ:

• Приказ от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не

составляющей государственную тайну, содержащейся в государственных информационных системах»;

• Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

• руководящие документы ФСТЭК по защите от НСД;

• руководящие документы ФСТЭК по защите от НДВ;

• Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.;

• Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);

• Приказ ФСБ РФ от 9 февраля 2005г. № 66 «Об утверждении, разработке, производстве, реализации и эксплуатации шифровальных и криптографических средств защиты (Положение ПКЗ-2005».

Задание 1. Определить нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 2. Изучить ФЗ «Об информации, информационных технологиях и о защите информации». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 3. Изучить приказ ФСТЭК России от 18 февраля 2013 г.; 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 4. Изучить типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством Центра ФСБ России 21.02.2008 №149/6/6-622. Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

ПРАКТИЧЕСКАЯ РАБОТА № 2
Обзор стандартов. Работа с содержанием стандартов

Цели: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

Теоретические вопросы

1. Предмет и задачи программно-аппаратной защиты информации.

2. Основные понятия программно-аппаратной защиты информации.

3. Классификация методов и средств программно-аппаратной защиты информации.

4. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 1. Выписать государственные стандарты в области информационной безопасности.

Задание 2. Выписать международные стандарты информационной безопасности.

Задание 3. Изучить ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

ПРАКТИЧЕСКАЯ РАБОТА № 3
Учет, обработка, хранение и передача информации в АИС

Цели: познакомиться со способами учета, обработки, хранения и передачи информации в АИС.

Теоретические вопросы

1. Технологии учета и хранения информации.
2. Технологический процесс обработки информации.
3. Способы обработки информации.
4. Режимы обработки информации на компьютере.
5. Технологии передачи и представления информации.

Задание 1. Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?

Задание 2. Изучить технологический процесс обработки информации. Перечислить и охарактеризовать технологические процессы процесса обработки информации. В чем заключается различие между централизованным и децентрализованным способами обработки информации? Какие режимы обработки информации вам известны?

Задание 3. Изучить технологии передачи и представления информации. Описать, как происходит передача данных.

Задание 4. Выполнить задания:

- набрать в одном из текстовых редакторов текст из 10 предложений на тему «Моя профессия»;
- вставить в набранный текст рисунок;
- сохранить текст на каких-либо носителях;
- создать свою электронную почту;
- отправить, набранную информацию по электронной почте;
- получить информацию по электронной почте;
- изменить полученный текст, введя диаграмму;
- сохранить текст.

Задание 5. Продумать и создать технологию учета и отработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудования «Сервис-ТЕХНО». Результат выполнения задания оформить в виде таблицы.

Задание 6. Используя технологии поиска информации, найдите разницу между терминами “хранение” и “сохранение данных”.

Задание 7. Используя средства Интернета, перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

ПРАКТИЧЕСКАЯ РАБОТА № 4
Ограничение доступа на вход в систему

Цель: ознакомиться с процедурами создания учётных записей пользователей и управления их правами.

Теоретические вопросы

1. Учётные записи пользователей.
2. Создание учётных записей пользователей.
3. Создание учётных записей пользователей для компьютеров, состоящих в рабочей группе.
4. Создание учётной записи при помощи оснастки «Локальные пользователи и группы».
5. Создание учётной записи при помощи командной строки.
6. Управление учётными записями при помощи диалога «Управление учётными записями пользователей».

Задание 1. Ознакомиться с технологиями создания и управления учетными записями пользователей. Примените к созданной учётной записи настройки, указанные в варианте.

Таблица 1 – Варианты заданий

Вариант / Параметр	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Пароль должен отвечать требованиям сложности	+	-	-	+	-	-	+	-	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на…	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через…	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

Задание 2. Создайте новую учетную запись пользователя с помощью командной строки.

Задание 3. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.

Задание 4. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

ПРАКТИЧЕСКАЯ РАБОТА № 5

Идентификация и аутентификация пользователей

Цель: ознакомиться с механизмами идентификации и аутентификации пользователей.

Теоретические вопросы

1. Понятия идентификации и аутентификации пользователей.
2. Механизмы аутентификации и идентификации пользователей.

Задание 1. Опишите параметры локальной политики безопасности операционной системы Windows:

– кто имеет доступ к компьютеру;

– какие ресурсы могут использовать пользователи на компьютере;

– включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задание 2. Опишите параметры и значения параметров Политики паролей. Заполните таблицу:

Параметр	Значение
Требовать повторяемости паролей	
Максимальный срок действия пароля	
Минимальный срок действия пароля.	
Минимальная длина пароля.	
Пароль должен отвечать требованиям сложности	
Хранить пароли всех пользователей в домене, используя обратимое шифрование.	

Задание 3. Опишите параметры и значения параметров Политики учетной записи. Заполните таблицу:

Параметр	Значение
Пороговое значение блокировки	
Блокировка учетной записи на	
Сброс счетчика блокировки через	

Задание 4. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения вашего задания.

Задание 5. После успешного выполнения предыдущего задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

Задание 6. Проведите эксперименты с другими параметрами Политики учетных записей.

ПРАКТИЧЕСКАЯ РАБОТА № 6

Разграничение доступа.

Цель: освоение навыков управления доступом пользователей.

Теоретические вопросы

1. Стандартные разрешения для файлов и папок.
2. Механизмы разграничения доступа.
3. Списки управления доступом ACL.
4. Реализация дискреционной модели доступа в ОС Windows.

Задание 1. Выполните задания.

- Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).
- Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.
- Выполните различные действия с папкой и файлами для обеих учетных записей и

установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

- Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.
- Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.
- Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.
- Составьте отчет о проведенных экспериментах.

Задание 2. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

ПРАКТИЧЕСКАЯ РАБОТА № 7
Регистрация событий (аудит)

Цель: ознакомиться с механизмами регистрации событий.

Теоретические вопросы

1. Понятия регистрации и аудита.
2. Средства регистрации и аудита.
3. События, фиксируемые в системном журнале.

Задание 1. Опишите параметры и значения параметров Политики аудита. Заполнить таблицу.

Параметр	Значение
Аудит событий Входа в систему	
Аудит управления Учетными записями	
Аудит доступа к службе каталогов	
Аудит входа в систему	
Аудит доступа к объектам	
Аудит изменения политики	
Аудит использования привилегий	
Аудит отслеживания процессов	
Аудит системных событий	

Задание 2. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале?

Задание 3. Включите аудит успеха и отказа всех параметров.

Задание 4. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись.

Задание 5. Удалите раннее созданную учетную запись и зафиксируйте все события системного журнала, связанные с этим действием.

ПРАКТИЧЕСКАЯ РАБОТА № 8
Контроль целостности данных

Цели: получить навыки обнаружения фактов изменения данных, контроля целостности данных с помощью механизма хэш-функций.

Теоретические вопросы

1. Хэш-функция.
2. Свойства хэш-функции.
3. Области использования хэш-функции.
4. Вычисление хэш-функции.

Хэш-функция H(x) – функция, которая преобразует (отображает) сообщение произвольной длины в число («свёртку») фиксированной длины. X – прообраз. H(x) – образ. Хэш-функция в общем случае – это функция, которая должна обладать следующими свойствами:

1. Хэш-функция может быть применена к аргументу любого размера.
2. Выходное значение хэш-функции имеет фиксированный размер (хэш-свёртка).
3. Хэш-функцию H(M) достаточно просто вычислить для любого M (простота вычисления образа).
4. Для любого y с вычислительной точки зрения невозможно найти x, такое что $H(x) = y$ (сложность вычисления прообраза).
5. Для любого фиксированного x с вычислительной точки зрения невозможно найти z, не равное x, такое, что $H(x) = H(z)$ (стойкость к коллизиям, вычислению второго прообраза).

Для криптографической хэш-функции (в отличие от хэш-функции общего назначения) сложно вычислить обратную и даже найти два сообщения с общей хэш-свёрткой. По четвёртому свойству $H(x)$ – односторонняя функция, поэтому $H(x)$ можно использовать в качестве контрольной суммы для проверки целостности. Области использования хэш-функции:

– защита паролей при их передаче и хранении;

– формирование контрольных кодов MDC (Manipulation Detection Code) - кода обнаружения манипуляций с данными;

– получение сжатого образа сообщения перед формированием электронной подписи;

– задачи поиска данных.

ГОСТ Р 34.11-2012 – криптографический стандарт вычисления хэш-функции. Размер блока входных данных: 512 бит. Размер хэша (хэш-свёртки): 512 бит. Стандарт ГОСТ Р 34.11-2012 определяет алгоритм и процедуру вычисления хэш-функции для последовательности символов.

Стандарт обязателен для применения в качестве алгоритма хэширования в государственных организациях РФ и ряде коммерческих организаций.

Для вскрытия паролей, преобразованных при помощи сложнообратимой хэш-функции, а также для атак на симметричные шифры на основе известного открытого текста используются радужные таблицы. Радужная таблица – специальный вариант таблиц поиска для обращения криптографических хэш-функций. Радужная таблица – готовая построенная цепочка возможных паролей. Однако таблицы могут взламывать только ту функцию, для которой создавались. Использование функции выведения ключа с применением соли делает эту атаку неосуществимой.

Для вычисления хэш-свёртки может быть использована любая программа. Кроме того, такой функционал есть в системе Windows через консоль. Для этого нужно использовать команду: «certutil –hashfail "Путь"», используется хэш-функция SHA-1.

Задание 1. Создать несколько файлов, заполнить их данными. Сделать копии файлов и произвести для некоторых из них «незаметные» для пользователей изменения в файлах. К таким изменениям можно отнести, к примеру:

- изменение кода цвета объектов, в частности текста;
- замена символов на похожие символы с другими кодами символов;
- вставка объектов со 100 %-ной прозрачностью, отсутствующими цветами заливками или совпадающими с цветом фона;
- изменение текста до минимального, установка цвета текста под цвет фона;
- вставка текста с атрибутами «скрытый текст», опция «Шрифт» => «Видоизменение»;
- изменение рисунка (областей с мало отличимой палитрой цветов);
- изменение метаданных файлов (к примеру, вкладка «Подробно» с полями «Авторы», «Организация» и пр.);
- прочее.

Задание 2. Используя программную реализацию механизма хэш-функций, проверить целостность и неизменность файлов. Предоставить снимки экрана, описание действий и результатов. Прокомментировать детально результаты работы: когда совпадают, когда расходятся и почему.

Задание 3. Современная диалектика оформлялась на основе обобщения огромного фактического материала. Причем она обобщает материалы не отдельной области знаний, а совокупность фактов бытия природы и всемирно-исторической практики и опирается на потенциал всего человеческого познания, на данные истории и достижения современного научно- технического прогресса. Согласны ли вы с такой оценкой диалектики? Если да, то покажите это на конкретном материале естественных и гуманитарных наук.

Задание 4. Изучить возможность атаки на хэш-функцию, продемонстрировать пример.

Задание 5. Продемонстрировать возможность тайной передачи данных (картинок, текста) в документах так, чтобы проверка контрольной суммы не обнаружила изменений.

ПРАКТИЧЕСКАЯ РАБОТА № 9
Уничтожение остаточной информации

Цель: ознакомиться с механизмами уничтожения остаточной информации.

Теоретические вопросы

1. Определение остаточной информации.
2. Причины возникновения остаточной информации.
3. Уничтожение информации как часть процесса обеспечения информационной безопасности.
4. Анализ современных методов и средств ликвидации информации с магнитных носителей.

Задание 1. Опишите причины возникновения остаточной информации.

Задание 2. Приведите примеры устройств уничтожения информации с магнитных носителей.

Задание 3. Изучите особенности современных методов ликвидации информации на магнитных носителях. Заполните таблицу.

Метод ликвидации информации	Принцип действия	Основные особенности

Задание 4. Изучите основные особенности современных устройств ликвидации магнитных записей. Заполните таблицу.

Тип устройства	Принцип действия	Основные особенности

Задание 5. Перечислите основные требования к современным устройствам уничтожения информации с магнитных носителей.

Задание 6. Охарактеризуйте программные методы уничтожения информации.

ПРАКТИЧЕСКАЯ РАБОТА № 10
Управление политикой безопасности. Шаблоны безопасности

Цель: ознакомиться с механизмами управления политикой безопасности.

Теоретические вопросы

1. Дискреционная политика безопасности.
2. Домены безопасности.
3. Матрица доступа.
4. Мандатная политика безопасности.

Задание 1. Исследуемая система состоит из множества субъектов и объектов.

Исходные данные

СУБЪЕКТЫ

1. Пользователь 1 (Администратор).
2. Пользователь 2.
3. Пользователь 3.
4. Текстовый редактор Word.

5. Редактор формул.

6. Модуль проверки правописания. ОБЪЕКТЫ

1. Документ пользователя 1.

2. Документ пользователя 2.

3. Документ пользователя 3.

4. Файл текстового редактора Word WINWORD.EXE.

5. Файл редактора формул EQUATION.DLL.

6. Файл модуля проверки правописания SPELL.DLL.

7. Файл-словарь DICTIONARY.DOC.

Политика безопасности системы устанавливает следующий порядок работы, при котором:

– пользователь 1 имеет возможность работы со своим документом с помощью программы WORD, может только просматривать документы пользователя 2 и 3, может проверять правописание в своем документе и вставлять в него формулы. Так же пользователь 1 может добавлять новые слова в словарь;

– пользователь 2 имеет возможность работать только со своим документом, может проверять правописание, но не может добавлять новые слова в словарь и не может вставлять в документ формулы;

– пользователь 3 имеет возможность работать со своим документов и документом пользователя 2, может проверять правописание в обоих документах, может добавлять в документы формулы, но не может добавлять новые слова в словарь.

Программа Word может быть запущена только пользователями системы и может вызывать редактор формул и модуль проверки правописания.

Только модуль проверки правописания может изменять файл-словарь DICTIONARY.DOC.

Необходимо:

– составить множество возможных прав доступа в системе. Для заданного множества субъектов и объектов построить матрицу доступов и заполнить ее в соответствии заданной политикой безопасности и с принципом минимизации привилегий;

– дополнить матрицу доступов временными доменами (например, добавить строку "Программа Word, запущенная от имени первого пользователя" или "Редактор формул, запущенный третьим пользователем из программы Word"). В матрице доступов должны быть представлены временные домены для всех возможных комбинаций взаимодействующих субъектов.

Задание 2. Заданы документы с различным уровнем секретности, заданы пользователи с различным уровнем доступа (список документов и пользователей и их уровни доступа/секретности составить самостоятельно. Не менее 5 пользователей и 5 документов).

1. Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

2. Для одного из пользователей составить список документов, доступных ему для работы при условии, что пользователь может понизить свой уровень доступа на один уровень.

3. Один из пользователей имеет возможность работать с несколькими документами. На основе этих документов он создает новый документ. Какой гриф секретности нужно присвоить этому документу?

4. Показать на примере одного из пользователей, что мандатная политика безопасности не

может быть нарушено программой типа "Троянский конь".

ПРАКТИЧЕСКАЯ РАБОТА № 11
Криптографическая защита. Обзор программ шифрования данных

Цель: ознакомиться с программами шифрования данных.

Теоретические вопросы

1. Понятия криптографии и криптоанализа.
2. Симметричные и асимметричные криптографические системы.
3. Криптостойкость шифра.
4. Алгоритмы шифрования.
5. Программы шифрования данных.
6. Требования к криптосистемам.

Задание 1. Разработать алгоритм шифрования данных.

Задание 2. Привести примеры программ шифрования данных.

Задание 3. Провести сравнительный анализ программ шифрования данных.

Задание 4. Описать возможности одной из программ шифрования данных.

ПРАКТИЧЕСКАЯ РАБОТА № 12
Управление политикой безопасности. Шаблоны безопасности

Цель: научиться работать с редактором шаблонов безопасности.

Теоретические вопросы

1. Понятие шаблона безопасности.
2. Редактор шаблона безопасности.
3. Управление шаблоном безопасности.

Задание 1. Загрузите редактор Шаблона безопасности. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?

Задание 2. Отредактируйте шаблон безопасности и сохраните его под новым именем.

Задание 3. Опишите разделы, включаемые в стандартный Шаблон безопасности.

Задание 4. Опишите, какие параметры политики безопасности можно настроить с помощью шаблонов безопасности?

ПРАКТИЧЕСКАЯ РАБОТА № 13
Распределение каналов в соответствии с источниками воздействия на информацию

Цель: ознакомиться с каналами несанкционированного получения информации.

Теоретические вопросы

1. Виды угроз безопасности информации.
2. Источники угроз безопасности информации.
3. Характер происхождения угроз безопасности информации.

4. Предпосылки появления угроз безопасности информации.

5. Пути получения конфиденциальной информации.

Задание 1. Заполнить таблицу:

Канал связи	Среда	Носитель сообщения	Процесс, используемый для передачи сообщения
Почта, курьеры			
Телефон, компьютерные сети			
Радио, телевидение			
Зрение			
Слух			
Обоняние, вкус			
Осязание			

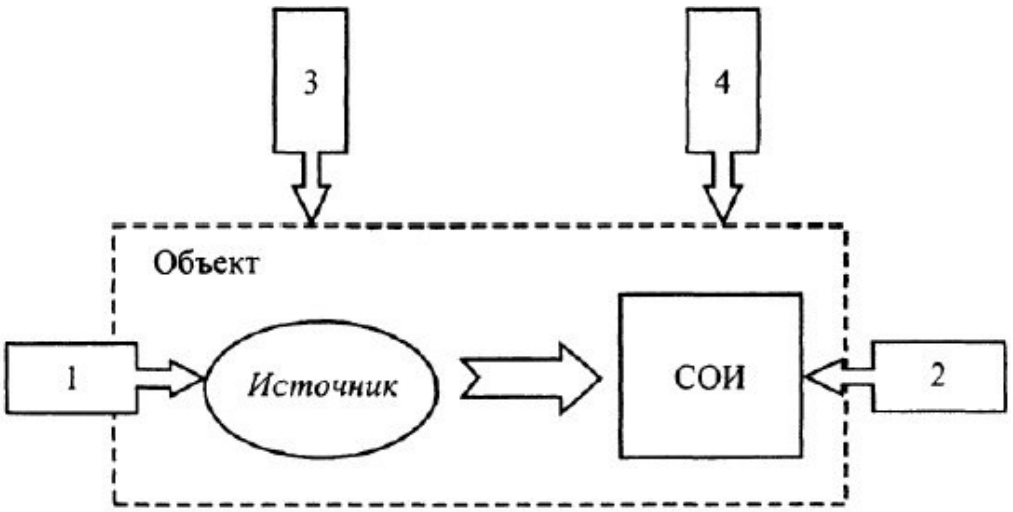
Задание 2. Приведите конкретные примеры каналов несанкционированного получения информации каждого класса. Классы каналов несанкционированного получения информации:

1) от источника информации при несанкционированном доступе (НСД) к нему;

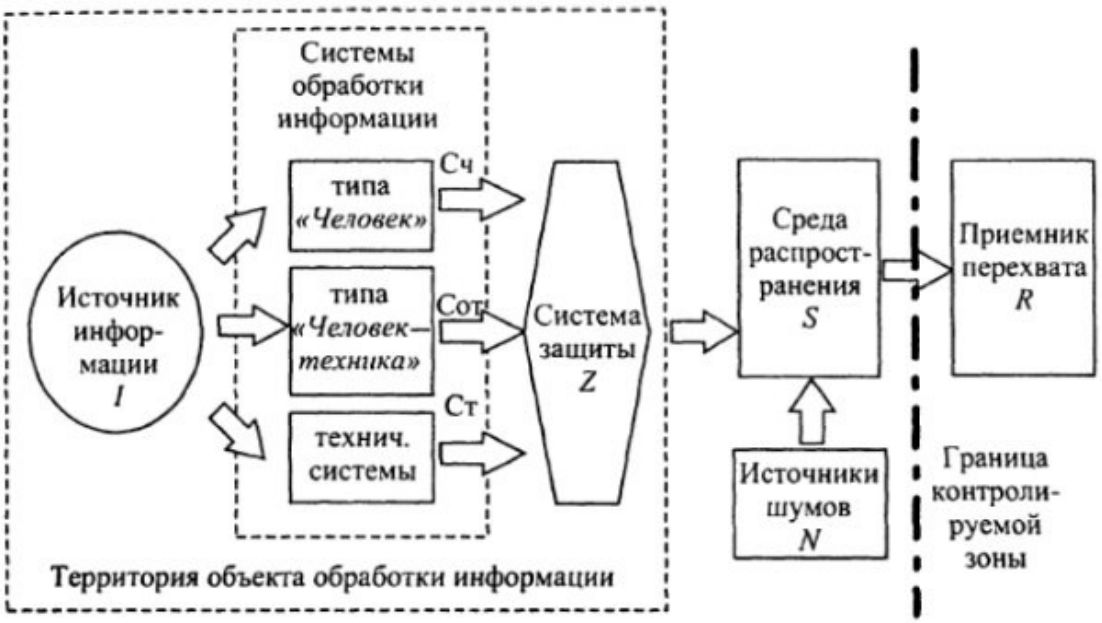
2) от средств обработки информации при НСД к ним;

3) от источника информации без НСД к нему;

4) от средств обработки информации без НСД к ним.



Задание 3. Поясните модель канала утечки информации.



Задание 4. Провести анализ защищенности заданного объекта защиты информации по следующим разделам:

- виды возможных угроз;
- характер происхождения угроз;
- классы каналов несанкционированного получения информации;
- источники появления угроз;
- причины нарушения целостности информации;
- потенциально возможные злоумышленные действия.

ПРАКТИЧЕСКАЯ РАБОТА № 14
Организация доступа к файлам

Цель: научиться назначать разрешения файлов и папок NTFS учетным записям и группам.

Теоретические вопросы

1. Разрешения файлов и папок NTFS.
2. Правила назначения разрешений.
3. Предотвращение наследования разрешений.

Задание 1. Заполните таблицы.

Разрешения папок NTFS

Разрешения папок NTFS	Позволяет:
Read (Чтение)	
Write (Запись)	
List Folder Contents (Список содержимого папки)	
Read & Execute (Чтение и выполнение)	
Modify (Изменить)	
Full Control (Полный доступ)	

Разрешения файлов NTFS

Разрешение файлов NTFS	Позволяет:
Read (Чтение)	
Write (Запись)	
Read & Execute (Чтение и выполнение)	
Modify (Изменить)	
Full Control (Полный доступ)	

Элементы вкладки Security (Безопасность)

Элемент	Описание
Name (Имя)	
Permissions (Разрешения)	
Add (добавить)	
Delete (Удалить)	
Advanced (Дополнительно)	

Задание 2. Планирование разрешений NTFS.

1. Спланируйте разрешения доступа к папкам и файлам. Затем реализуйте разрешения NTFS для файлов и папок вашего компьютера, а затем проверьте назначенные разрешения NTFS и убедитесь, что они работают должным образом.

Перед выполнением упражнений создайте следующие учетные записи и группы:

User8l (нет пароля) — член группы Managers; User82 (нет пароля) — член группы Accounting;

User83 (нет пароля) — член группы Managers и группы Accounting; User84 (нет пароля) — не является членом групп Accounting и– Managers. Создайте следующие папки:

C:\Public; C:\Public\Library; C:\Public\Manuals; C:\Public\Library\Misc.

Можно использовать и свою структуру объектов, имеющихся на вашем компьютере.

2. Спланируйте назначение разрешений NTFS для файлов и папок:

Имя папки	Группа	Разрешения
Public	Users Administrators	Read & Execute Full Control
Public\Library	Users Administrators Manager	Read & Execute Full Control Modify
Public\Library\Misc	Users Administrators User82	Read & Execute Full Control Modify
Public\Manuals	Users Administrators Accounting	Read & Execute Full Control Modify

Задание 3. Проверка разрешений NTFS.

1. Зарегистрируйтесь в системе под разными учетными записями и проверьте разрешения NTFS.

2. Проверьте разрешения доступа к папке Misc для пользователя User81.

3. Проверьте разрешения доступа к папке Misc для пользователя User82.

4. Зарегистрируйтесь в системе как User82 и откройте папку Public\Library\Misc. Попробуйте создать файл в папке Misc. Удалось ли это? Почему?

5 Проверьте разрешения доступа к папке Manuals для пользователя Administrator. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

6. Проверьте разрешения доступа к папке Manuals для пользователя User81. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

7. Проверьте разрешении доступа к папке Manuals для пользователя User82. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

ПРАКТИЧЕСКАЯ РАБОТА № 15
Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД

Цель: ознакомиться с современными программными и программно-аппаратными средствами защиты от НСД.

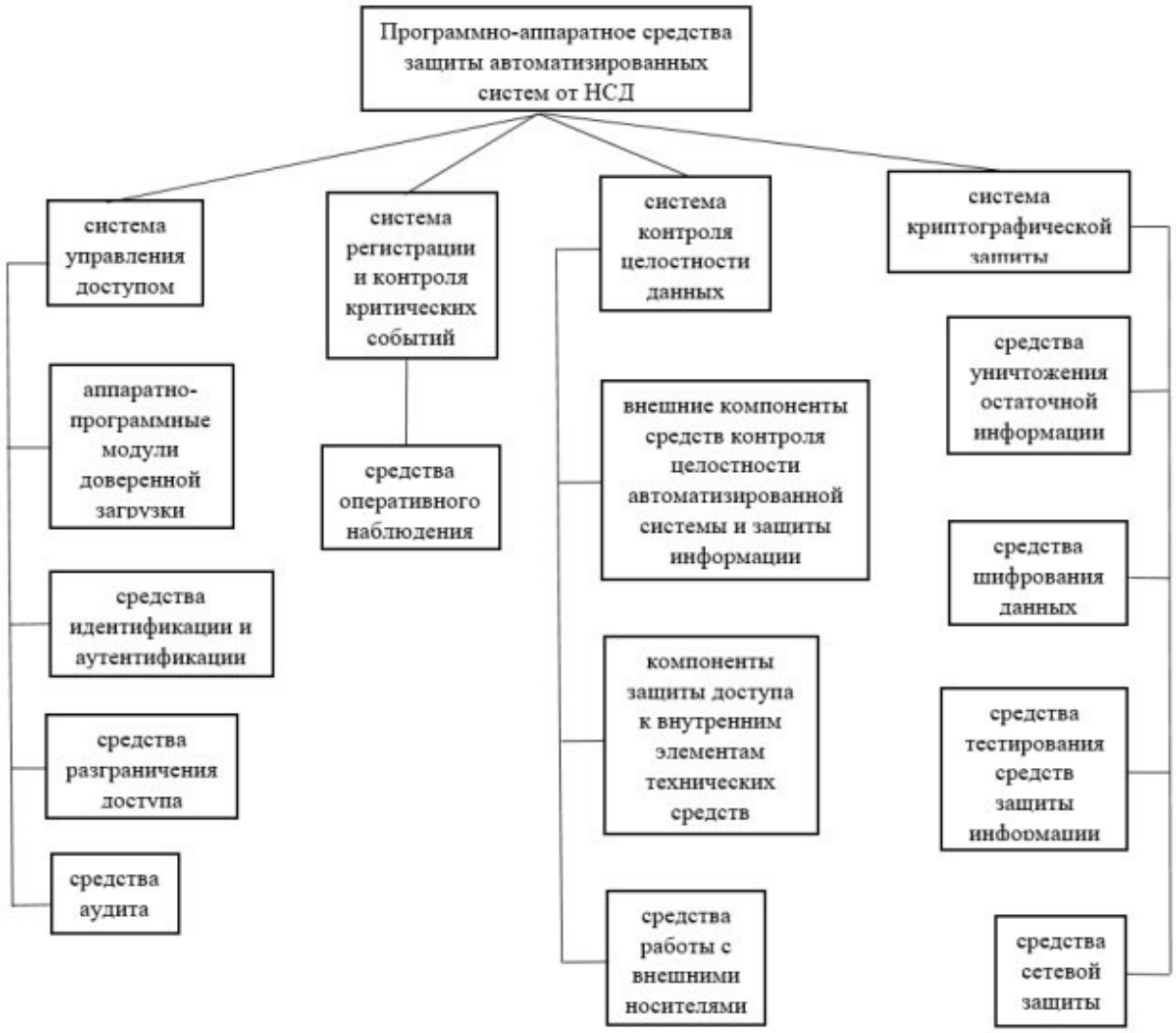
Теоретические вопросы

1. Понятие несанкционированного доступа (НСД).

2. Пути НСД к информации.

3. Способы защиты от НСД к информации.

Задание 1. Охарактеризуйте программно-аппаратные средства защиты автоматизированных систем от НСД.



Задание 2. В качестве примеров отдельных программ, повышающих защищенность от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др. Опишите одно из программных средств, повышающих защищенность от НСД.

Задание 3. В качестве примеров отечественных аппаратно-программных средств защиты можно привести системы «Аккорд-4», «DALLAS LOCK 3.1», «Редут», «ДИЗ-1».Опишите одно из программно-аппаратных средств защиты информации от НСД.

Задание 4. Приведите примеры современных систем защиты ПК от несанкционированного доступа к информации.

ПРАКТИЧЕСКАЯ РАБОТА № 16

Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО

Цель: ознакомиться с реестром Windows.

Теоретические вопросы

1. Основные принципы работы с системным реестром.

2. Расположение системного реестра.

3. Редактирование системного реестра.

4. Структура системного реестра.

5. Копирование и восстановление реестра.

Задание 1. Опишите разделы реестра Windows. Заполните таблицы.

HKEY_CURRENT_USER	
HKEY_USERS	
HKEY_LOCAL_MACHINE;	
HKEY_CLASSES_ROOT	
HKEY_CURRENT_CONFIG	

Состав основного раздела Hkey_Local_Machine

Раздел	**Назначение**
Config	
Enum	
Hardware	
Network	
Security	
Software	
System	

Задание 2. В каких разделах реестра хранится информация о выбранной политике безопасности.

Задание 3. Опишите возможности программы REGEDIT.EXE.

Задание 4. Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

ПРАКТИЧЕСКАЯ РАБОТА № 17

Защита информации от несанкционированного копирования с использованием специализированных программных средств

Цель: ознакомиться с механизмами защиты информации от несанкционированного копирования с использованием специализированных программных средств.

Теоретические вопросы

1. Понятие системы защиты от несанкционированного использования и копирования.
2. Понятие надежности системы защиты от несанкционированного копирования.
3. Принципы создания и использования систем защиты от копирования.
4. Основные требования, предъявляемые к системе защиты от копирования.
5. Основные компоненты системы защиты программных продуктов от несанкционированного копирования.
6. Методы, затрудняющие считывание скопированной информации.
7. Методы, препятствующие использованию скопированной информации.
8. Основные функции средств защиты от копирования.

Задание 1. Охарактеризуйте компоненты системы защиты от несанкционированного копирования.

Задание 2. Системы защиты от несанкционированного копирования можно классифицировать по способу внедрения защитного механизма:

- встроенная внедряется при создании программного продукта;
- пристыковочная подключается к уже готовому программному продукту. Приведите достоинства и недостатки этих способов внедрения защитного механизма.

Задание 3. Опишите основные требования, предъявляемые к системе защиты от копирования.

Задание 4. Угроза несанкционированного копирования информации блокируется методами, которые могут быть распределены по двум группам:

• методы, затрудняющие считывание скопированной информации;

• методы, препятствующие использованию информации.

Приведите примеры методов каждой группы. Сделайте сравнительный анализ основных методов защиты от копирования.

Задание 5. Отобразите схематично общий алгоритм механизма защиты от несанкционированного использования программ в «чужой» среде размещения.

ПРАКТИЧЕСКАЯ РАБОТА № 18

Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)

Цель: ознакомиться с защитными механизмами в приложения.

Теоретические вопросы

1. Средства защиты документов MS Word.
2. Средства защиты документов MS Excel.
3. Средства защиты документов MS PowerPoint.

Задание 1. Создайте шаблон делового письма, содержащий текст шапки и подписи стандартного письма организации, с защищенными от изменения реквизитами. Средняя часть письма (содержание письма) доступно для изменения.

При этом в защищенных шапке и подпись письма следует предусмотреть возможность изменения следующих данных:

– исходящий номер и дата создания письма могут быть изменены (набраны) с клавиатуры;

– фамилия исполнителя может быть выбрана из списка. Открытие файла письма должно быть защищено паролем.

Задание 2. В приложении MS Word создайте короткий опросник (анкету) с защищенным от изменения текстом вопросов для получения от пользователей различных данных. Сформулировать вопросы так, чтобы требовались:

a) ответы в произвольной форме, подразумевающие ввод текста, (например, ФИО, какие-либо комментарии или пожелания, номер учебной группы, дата заполнения),

b) выбор даты (дата дня рождения, начала сессии, рекомендуемая дата мероприятия или посещения и т.п.),

c) выбор единственного варианта ответа из списка и с помощью переключателей (например, пол, возрастная группа, форма обучения, специальность),

d) выбор нескольких вариантов с помощью флажков (например, знания, предпочтения, сферы интересов, участие в мероприятиях и т.п.)

Задание 3. Создайте новую книгу для проведения простых вычислений (например, вычисление суммы, разности, произведения и т.п.) над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем.

Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных.

Установите защиту: ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты.

При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

Задание 4. Создать книгу «Организация», содержащую три листа: «Справочники», «Ведомость», «Отчет». На лист «Справочники» поместить две таблицы следующего вида.
Данные о подразделениях

Код подразделения	Наименование	Руководитель

Данные о сотрудниках

Фамилия	Дата поступления	Разряд	Подразделение

Задать ограничения на ввод данных в столбец «Код подразделения» таблицы «Данные о подразделениях»: 1, 2 или 3.

Заполнить таблицу «Данные о подразделениях»: коды и наименования подразделений не повторяются.

Задать ограничения на ввод данных в столбец «Подразделение» таблицы «Данные о сотрудниках»: код подразделения должен выбираться из списка, определенного в столбце «Код подразделения» таблицы «Данные о подразделениях». Задать ограничения на ввод данных в столбец «Разряд» – целое число от 10 до 17.

Заполнить данными таблицу «Данные о сотрудниках»:

– фамилии сотрудников не повторяются;

– разряды и подразделения могут повторяться.

На лист «Ведомость» поместить таблицу следующего вида. Сводная ведомость

Фамилия	Код подразделения	Стаж, в годах	Оклад	Премия	Начислено

В таблице «Сводная ведомость» в столбец «Фамилия» поместить значения из одноименного столбца таблицы «Данные о сотрудниках». Остальные столбцы таблицы должны заполняться автоматически на основе справочников с помощью стандартных функций MS Excel (функции

ВПР, СЕГОДНЯ, ДОЛЯГОДА, ЕСЛИ).

Стаж вычисляется как разница между текущей датой и датой поступления на работу в организацию. Для вычисления текущей даты используется функция СЕГОДНЯ, для вычисления временного промежутка в годах – функция ДОЛЯГОДА.

Оклад рассчитывается как сумма базовой ставки для 10 разряда и надбавки за каждый следующий разряд. Размер базовой ставки и надбавки следует выбрать самостоятельно.

Премия начисляется в размере 50 % от оклада тем сотрудникам, которые проработали в организации больше 7 лет. Если стаж сотрудника меньше 7 лет, премия не начисляется (принимается равной нулю).

Значения столбца «Начислено» рассчитываются как сумма оклада и премиальных. На лист «Отчет» поместить таблицу следующего вида.

Сводные данные по подразделениям

Подразделение	
Наименование	
Руководитель	
Общая численность сотрудников	
Сумма премий	
Всего начислено	

В ячейке, расположенной правее слова «Подразделение», задать ограничения на ввод данных – может быть 1, 2 или 3. В ячейке, расположенной правее слова «Группа», выбирается код подразделения, а ниже выдается наименование, фамилия этого подразделения, и итоговые данные по численности и суммам начислений для сотрудников выбранного подразделения. Наименование подразделения и фамилия руководителя должны вычисляться автоматически с помощью стандартной функции ВПР. Итоговые значения должны вычисляться автоматически с помощью стандартных функций MS Excel (функции СЧЕТЕСЛИ, СУММЕСЛИ).

Установить защиту книги «Организация»:

1) придумать три различных пароля: пароль нижнего уровня (пароль1) позволяет открывать книгу «Организация» и просматривать данные листа «Отчет», кроме данных о начислениях; пароль среднего уровня (пароль2) позволяет просматривать данные с других листов книги, кроме данных о начислениях; пароль верхнего уровня (пароль3) позволяет просматривать и изменять все данные книги. Придуманные пароли следует записать, во избежание их утраты;

2) ограничить доступ к книге «Организация», установив пароль для открытия (пароль1);

3) на листе «Ведомость» скрыть столбцы с данными о начислениях («Оклад», «Премия», «Начислено»). Защитить листы «Справочники» и «Ведомость» с паролем3;

4) скрыть листы «Справочники» и «Ведомость», затем защитить структуру книги «Организация» с паролем2;

5) на листе «Отчет» оставить незащищенной ячейку для ввода кода подразделения, а в

ячейках, содержащих итоги, скрыть формулы. На листе «Отчет» скрыть строки, содержащие данные о суммах премий и общих начислений. Установить защиту листа «Отчет» с паролем3. Проверить, что можно просматривать итоги для разных подразделений.

Задание 5. Создать документ в приложении PowerPoint. Используя свойства и возможности приложения PowerPoint, защитить созданный файл паролем.

ПРАКТИЧЕСКАЯ РАБОТА № 19

Применение средства восстановления остаточной информации на примере Foremost или аналога

Цель: ознакомиться со средствами восстановления остаточной информации.

Теоретические вопросы

1. Программы восстановления данных.
2. Принцип действия программ восстановления данных.
3. Проблема остаточной информации.
4. Атака типа «сборка мусора». Способы защиты.

Задание 1. Приведите примеры программ восстановления данных. Опишите их возможности.

Составьте сравнительную характеристику.

Задание 2. Опишите возможности программы восстановления данных Foremost. Как Foremost

восстанавливает файлы? Опишите параметры запуска программы Foremost.

Задание 3. Создайте произвольный каталог и запишите туда данные каталога другого каталога. Удалите созданный каталог. С помощью Foremost восстановите данные.

ПРАКТИЧЕСКАЯ РАБОТА № 20

Применение специализированного программно средства для восстановления удаленных файлов

Цель: ознакомиться со средствами восстановления удаленных файлов.

Теоретические вопросы

1. Стандартная процедура удаления фалов в ОС Windows.
2. Стандартная процедура восстановления файлов в ОС Windows.
3. Программы восстановления удаленных файлов.

Задание 1. Опишите назначение и возможности программы Easy Recovery Pro.

Задание 2. Создайте на рабочем столе файл. Удалите его в Корзину. Восстановите файл из Корзины.

Задание 3. Создайте текстовый файл на диске D: с именем Proba.txt, введите свою фамилию, закройте и сохраните файл. Удалите созданный файл. Очистите Корзину. Восстановите файл с помощью программы Easy Recovery Pro.

Задание 4. Создайте на диске D:\ папку с именем Директория. Перепишите в созданную папку с диска C:\ файл Proba.txt. Удалите папку Директория. Очистите Корзину. Восстановите папку с помощью Easy Recovery Pro.

ПРАКТИЧЕСКАЯ РАБОТА № 21
Применение программ для безвозвратного удаления данных

Цель: ознакомиться с программами безвозвратного удаления файлов.

Теоретические вопросы

1. Необходимость безвозвратного удаления данных.
2. Алгоритмы удаления данных.
3. Методы гарантированного уничтожения данных с электронных носителей.

Задание 1. Опишите программные механизмы удаления данных. Достоинства и недостатки. На чем основаны программные методы гарантированного удаления информации?

Задание 2. Опишите механические механизмы удаления данных. Как работают аппаратные средства гарантированного удаления информации?

Задание 3. Сравните программные и аппаратные средства гарантированного удаления информации.

Задание 4. Проконтролируйте удаление файла с помощью стандартного метода удаления. Реализовать восстановление файла, после удаления стандартными средствами ОС.

Задание 5. Изучите методы уничтожения данных с электронных носителей путем многократной перезаписи.

Задание 6. В состав программ PGP и BestCrypt входят утилиты для безвозвратного удаления данных. В PGPtools – это Wipe (удаление файлов) и Freespace Wipe (очистка диска). В BestCrypt – Wipe drive free space (очистка диска). Изучите возможности этих утилит.

Задание 7. Создайте на диске D:\ папку с именем Директория. Перепишите в созданную папку с диска C:\ файл Proba.txt. Удалите файл с помощью утилиты Wipe.

ПРАКТИЧЕСКАЯ РАБОТА № 22
Применение программ для шифрования данных на съемных носителях

Цель: ознакомиться с программами шифрования данных.

Теоретические вопросы

1. Назначение шифрования информации.
2. Шифрование и дешифрование файлов и папок.
3. Атрибуты шифрования папки.
4. Архивация зашифрованных файлов.
5. Программы шифрования данных на съемных носителях.

Задание 1. Создайте на диске C:\Темп папку и скопируйте в нее любой файл. Зашифруйте

файл вместе с папкой таким образом, чтобы все помещаемые в папку файлы тоже шифровались (если шифрование не удалось – дальнейшие действия с папкой делайте, как с зашифрованной). Создайте на рабочем столе папку с вашей фамилией и добавьте в неё резервную копию зашифрованной вами папки (сохраняя шифрование).

Задание 2. Программа VeraCrypt позволяет создавать виртуальный зашифрованный диск, представляющий собой файл, который можно смонтировать в локальный диск. Программа NeoCrypt позволяет шифровать содержимое файла без изменения его расширения.

Опишите возможности этих программ.

Задание 3. Опишите технологию шифрования дисков BitLocker. Примените технологию BitLocker To Go к Flash – диску с пошаговым описанием всех действий. Дайте сравнительную характеристику шифрования жесткого и съемного дисков.

ПРАКТИЧЕСКАЯ РАБОТА № 23

Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений

Цели: ознакомиться с инструментальными средствами обнаружения вторжений.

Теоретические вопросы

1. Понятие атаки.
2. Моделирование проведения атаки.
3. Методы обнаружения вторжений.
4. Инструментальные средства обнаружения вторжений.
5. Средства предотвращения вторжений.
6. Активные и пассивные системы обнаружения вторжений.
7. Стандарты в области систем обнаружения вторжений

Задание 1. Выделяют следующие методы обнаружения вторжений:

– сигнатурный анализ:

– использование статистики Байеса;

– продукционные (экспертные) системы;

– анализ перехода системы из состояния в состояние и сети Петри;

– статистический анализ:

– относительная частота последовательностей;

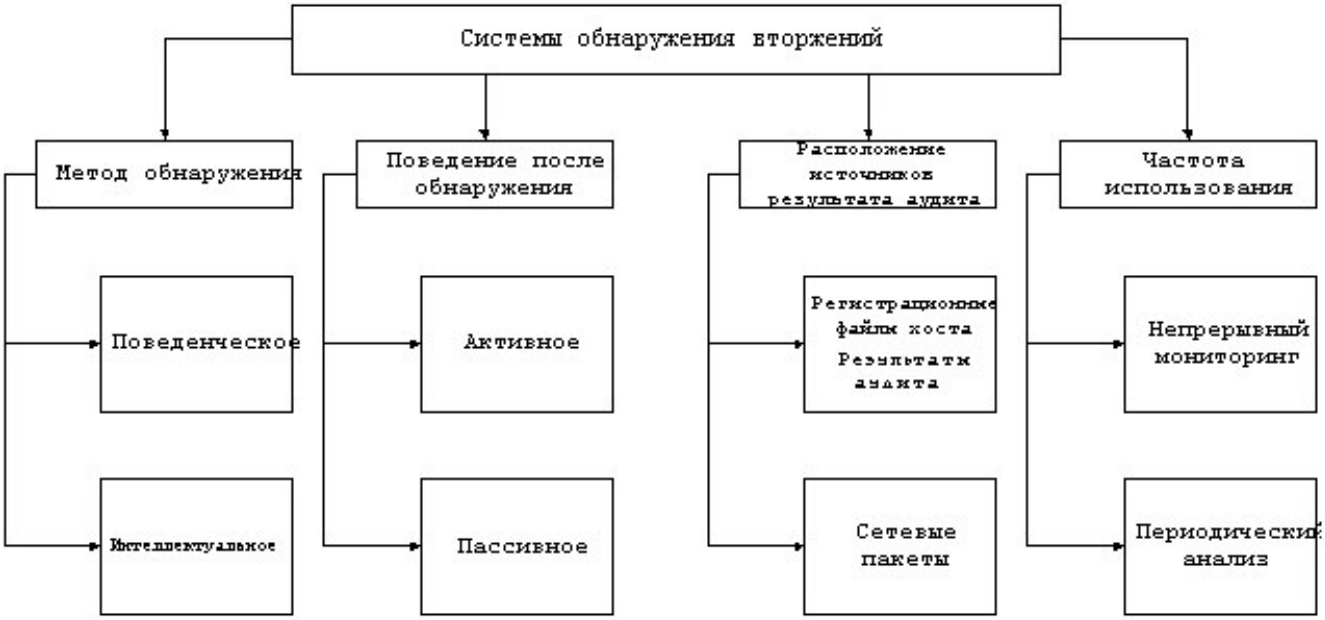
– модель среднего значения и среднеквадратичного отклонения;

– операционная модель;

– модель временных серий.

Опишите один из методов обнаружения вторжений.

Задание 2. Поясните классификацию систем обнаружения вторжений.



Задание 3. Охарактеризуйте основные элементы локальной архитектуры систем обнаружения вторжений.

Задание 4. Приведите примеры систем обнаружения вторжений. Охарактеризуйте одну из систем обнаружения вторжений.

Задание 5. Изучите систему обнаружения вторжений Snort.

ПРАКТИЧЕСКАЯ РАБОТА № 24
Развертывание VPN

Цель: изучить технологии VPN.

Теоретические вопросы

1. Понятие VPN.
2. Уровни реализации, структура, классификация VPN.
3. Построение безопасных сетей на основе VPN
4. Настройка VPN-сервера.
5. Настройка VPN-клиента.

Задание 1. Опишите этапы создания VPN сервера в Windows.

Задание 2. Опишите этапы создания VPN клиента в Windows.

Задание 3. Опишите технологии тестирования виртуальных сетей.

Задание 4. Представьте проект виртуальной сети для заданной организации.

ПРАКТИЧЕСКАЯ РАБОТА № 25
Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.

Цель: изучение архитектур межсетевых экранов.

Теоретические вопросы

1. Понятие межсетевого экрана.
2. Назначение межсетевых экранов.
3. Основные типы межсетевых экранов.
4. Симметричные и несимметричные межсетевые экраны.
5. Пакетные фильтры.
6. Фильтрация служб с протокол зависимыми модулями и поиск ключевых слов в теле пакетов на сетевом уровне.
7. Proxy сервера прикладного уровня.
8. Однохостовые межсетевые экраны. Достоинства и недостатки.
9. Мультихостовые межсетевые экраны. Достоинства и недостатки.

Задание 1. Изучить основные типы архитектур мультихостовых Firewall: Dual Homed Host, Bastion Host, Perimetr, Demilitarized Zone.

Задание 2. Сравнить основные типы архитектур мультихостовых Firewall: Dual Homed Host, Bastion Host, Perimetr, Demilitarized Zone. Результаты представить с помощью таблицы.

ПРАКТИЧЕСКАЯ РАБОТА № 26
Изучение различных способов закрытия "опасных" портов

Цель: изучение различных способов закрытия "опасных" портов.

Теоретические вопросы

1. Понятие и функции порта.
2. Понятие «опасного» порта.

3. Уязвимые порты Windows.

4. Способы закрытия «опасных» портов.

Задание 1. Многочисленные исследования и опросы специалистов показывают, что до 80 % вредоносных атак и взломов происходили при помощи четырех основных портов, использующихся для быстрого обмена файлами между разными версиями Windows:

– TCP порт 139;

– TCP порт 135;

– TCP порт 445;

– UDP порт 137.

Пишите назначение приведенных портов.

Задание 2. С помощью командной строки закрыть порты 135-139 и 445.

Задание 3. Опишите назначение и возможности программы Windows Doors Cleaner.

ПРАКТИЧЕСКАЯ РАБОТА № 27
Изучение механизмов защиты СУБД MS Access

Цель изучение механизмов защиты СУБД MS Access.

Теоретические вопросы

1. Физическая и логическая целостность базы данных.
2. Защита базы данных на уровне пароля, на уровне пользователя.
3. Типы разрешений на доступ к базе данных.
4. Встроенные учетные записи MS Access.
5. Порядок изменения пароля пользователя или группы.
6. Объекты базы данных MS Access и права доступа к объектам. Понятие владельца объекта.
7. Алгоритм защиты базы данных MS Access.

Задание 1. Создать новую базу данных и создать в ней следующие объекты:

- таблицу Заказы;
- запрос Сведения о заказах;
- форму Заказы клиентов.

Заполнить таблицу несколькими записями.

Задание 2. Защитите созданную базу данных паролем. Каким образом обеспечивается целостность данных?

Задание 3. Защитите созданную базу данных с помощью Мастера. MS Access предоставляет средства распределенного доступа к базе данных. С одним файлом могут одновременно работать большое количество пользователей, обладающих разными правами: одни могут только просматривать таблицы, другие – только вносить новые данные, и лишь администраторы базы обладают полным доступом. Разделите доступ для двух пользователей – один сможет только просматривать данные (читать), другой будет обладать полным доступом.

Опишите этапы защиты базы данных с помощью Мастера.

Задание 4. Создайте резервную копию базы данных.

ПРАКТИЧЕСКАЯ РАБОТА № 28

Изучение штатных средств защиты СУБД MSSQL Server

Цель: изучение механизмов защиты СУБД MS SQL Server.

Теоретические вопросы

1. Уровни безопасности MS SQL Server.
2. Модель безопасности MS SQL Server.
3. Тип подключения к MS SQL Server.
4. Типы ролей в MS SQL Server.
5. Стандартные роли уровня базы данных.
6. Предоставление и отмена привилегий.

Задание 1. Создать базу данных для работы компьютерных курсов (рисунок 1). Заполнить таблицу несколькими записями.

Задание 2. Установите права на доступ к объектам базы данных.

Задание 3. Каким образом обеспечивается целостность данных?

Задание 4. Изучите операторы GRANT и REVOKE, используемые для предоставления и отмены привилегий соответственно.

Задание 5. Создайте резервную копию базы данных.

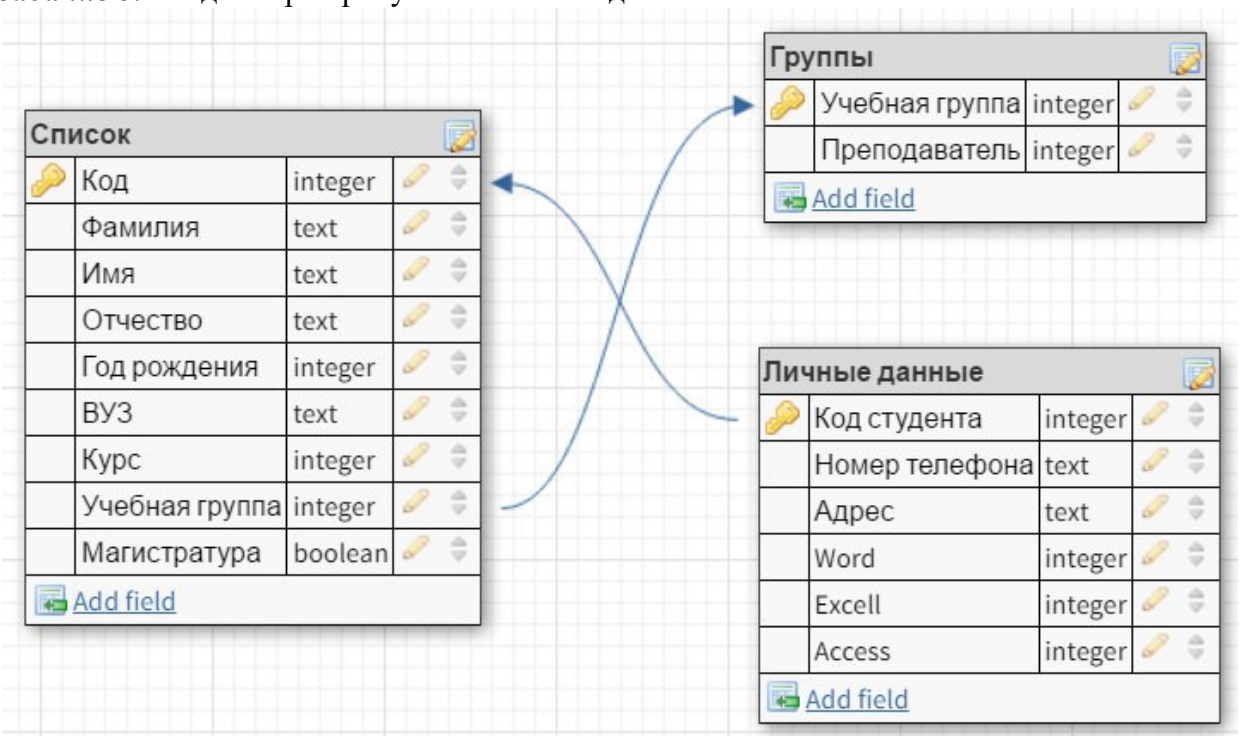


Рисунок 1

ПРАКТИЧЕСКАЯ РАБОТА № 29

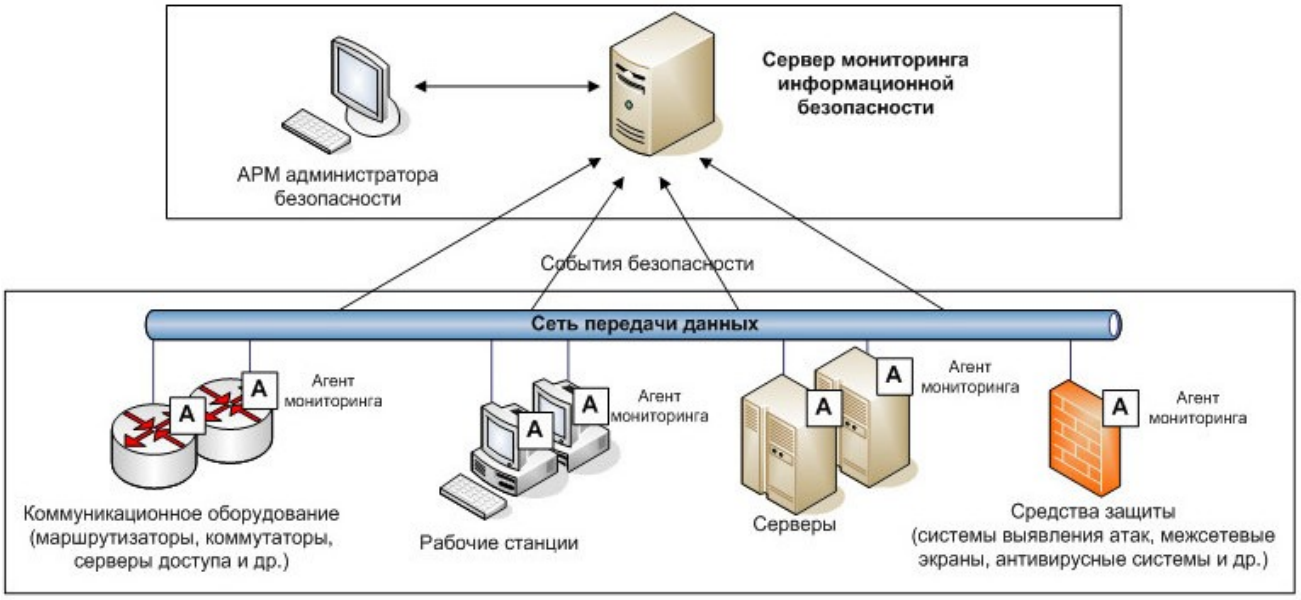
Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов

Цель: изучение сетевых мониторов.

Теоретические вопросы

1. Понятие системы мониторинга информационной безопасности.
2. Компоненты системы мониторинга информационной безопасности.
3. Структура системы мониторинга информационной безопасности.
4. Роли в составе системы мониторинга информационной безопасности.
5. Основные этапы создания системы мониторинга информационной безопасности.

Задание 1. Поясните структуру системы мониторинга информационной безопасности.



Задание 2. Изучите назначение и основные возможности сетевых мониторов (RealSecure, SNORT, NFR или другие аналоги).

Задание 3. Проведите сравнительный анализ распространенных сетевых мониторов. Результаты оформите с помощью таблицы.

ПРАКТИЧЕСКАЯ РАБОТА № 30

Проведение аудита ЛВС сетевым сканером

Цель: знакомство с сетевыми сканерами безопасности.

Теоретические вопросы

1. Аудит сети.
2. Цели проведения аудита сети.
3. Этапы проведения аудита сети.
4. Сканеры безопасности.
5. Принцип работы сканера безопасности.
6. Классы сканеров безопасности.

Задание 1. Приведите примеры сканеров безопасности сетевых сервисов и протоколов.

Задание 2. Опишите возможности сетевого сканера безопасности Shadow Security Scanner или аналога. Основные команды.

Задание 3. Перечислите и охарактеризуйте стандартные правила, определяющие параметры сессии сканирования. На базе одного из них создайте собственное правило.

Задание 4. Проведите сканирование указанных преподавателем компьютеров в учебной лаборатории. При сканировании надо учитывать, что часть имеющихся уязвимостей может быть закрыта путем использования встроенного межсетевого экрана (брандмауэра Windows), появившегося в ОС семейства Windows, начиная Windows XP. Чтобы получить более полную информацию об исследуемых узлах, лучше провести одно сканирование при включенном, другое – при отключенном межсетевом экране (изменение настройки доступно через Панель управления –> Брандмауэр Windows). Аналогичная ситуация возникает и при использовании других межсетевых экранов. Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров.

ПРАКТИЧЕСКАЯ РАБОТА № 31

Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.

Цель: знакомство с программными и программно-аппаратными средствами защиты информации в информационных системах.

Теоретические вопросы

1. Задачи системы информационной безопасности.
2. Внешняя и внутренняя безопасность ИС.
3. Меры обеспечения безопасности информационных систем.
4. Основные принципы построения систем защиты ИС.

Задание 1. Приведите примеры законодательных мер защиты информации в ИС.

Задание 2. Приведите примеры административных мер защиты информации в ИС.

Задание 3. Приведите примеры процедурных мер защиты информации в ИС.

Задание 4. Приведите примеры программно-технических мер защиты информации в ИС.

Задание 5. Разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты:

1. Общие положения.

1.2. Цели системы информационной безопасности.

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности.

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности Предприятия.

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия.

4.1. Организационное обеспечение информационной безопасности:

- задачи организационного обеспечения информационной безопасности;
- подразделения, занятые в обеспечении информационной безопасности;
- взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия:

- общие положения;
- защита информационных ресурсов от несанкционированного доступа;
- средства комплексной защиты от потенциальных угроз;
- обеспечение качества в системе безопасности;
- принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия:

- правовое обеспечение юридических отношений с работниками Предприятия;
- правовое обеспечение юридических отношений с партнерами Предприятия;
- правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

Вариант – номер по списку в журнале

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда

17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Железнодорожная касса

ПРАКТИЧЕСКАЯ РАБОТА № 32

Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов

Цель: знакомство с приложением SecretNetStudio.

Теоретические вопросы

1. Назначение SecretNetStudio.
2. Возможности SecretNetStudio.
3. Режимы управления SecretNetStudio.

Задание 1. Изучите учебную версию приложения SecretNetStudio.

Задание 2. Опишите возможности приложения SecretNetStudio. Какие задачи информационной безопасности решаются с помощью этого продукта?

Задание 3. Опишите уровни защиты информации с помощью приложения SecretNetStudio.

Задание 4. Опишите варианты настройки приложения SecretNetStudio.

ПРАКТИЧЕСКАЯ РАБОТА № 33

Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов

Цель: знакомство с приложением MaxPatrol 8.

Теоретические вопросы

1. Назначение MaxPatrol 8.
2. Возможности MaxPatrol 8.
3. Сценарии внедрения MaxPatrol 8.

Задание 1. Изучите приложениея MaxPatrol 8.

Задание 2. Опишите возможности приложения MaxPatrol 8. Какие задачи информационной безопасности решаются с помощью этого продукта?

Задание 3. Опишите варианты настройки приложения MaxPatrol 8.

ПРАКТИЧЕСКАЯ РАБОТА № 34

Изучение типовых решений для построения VPN на примере VipNet или других аналогов

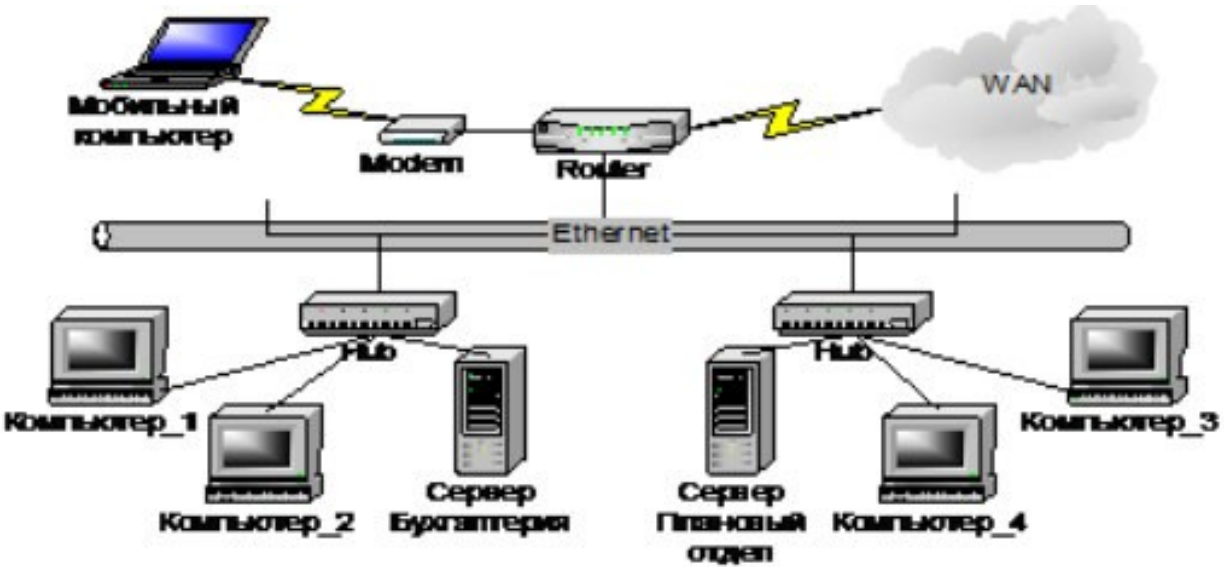
Цель: исследование защищенной сети передачи данных на базе технологии ViPNet Custom.

Теоретические вопросы

1. Технология ViPNet.
2. Состав программно-аппаратного комплекса ViPNet.
3. Сеть ViPNet с точки зрения маршрутизации сообщений.
4. Особенности структуры сети ViPNet.

Задание 1. Опишите назначение компонентов ViPNet [Администратор], ViPNet [Координатор], ViPNet [Клиент].

Задание 2. Сформировать защищенную сеть, исходя из нижеперечисленных условий и приведенной схемы реальной сети



Условия построения защищенной сети

1. В защищенную сеть включаются следующие СУ: Сервер Бухгалтерия, Компьютер_1, Компьютер_2, Сервер Плановый отдел, Компьютер_3, Компьютер_4, Мобильный компьютер.
2. Компьютер_1, Компьютер_2 и Мобильный компьютер на транспортном уровне в качестве сервера должны использовать Сервер Бухгалтерия.
3. Компьютер_3, Компьютер_4 на транспортном уровне в качестве сервера должны использовать Сервер Плановый отдел.
4. Бухгалтерия и Плановый отдел на транспортном уровне должны иметь связь.
5. На Компьютере_1 постоянно работает один человек (абонент Петров).
6. На Компьютере_2 могут работать два человека (абоненты Сидоров и Васечкин), они не должны иметь доступ к информации друг друга на транспортном уровне.
7. На Компьютере_3, Компьютере_4 и Мобильном компьютере постоянно работают по одному человеку (абоненты Лялин, Свиридова и Кузовкин, соответственно).
8. На каждом сервере регистрируется по абоненту: Администратор Сервера Бухгалтерия и

Администратор Сервера Планового отдела.

9. В защищенной сети все видят всех за исключением Васечкина, который не должен иметь связи с Петровым.

10. Дополнительно требуется, чтобы Кузовкин имел возможность получить доступ к Компьютеру_4 и защищенной информации Свиридовой.

11. Администратором защищенной сети будет Лялин.

ПРАКТИЧЕСКАЯ РАБОТА № 35

Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов

Цель: изучение способов защиты информации от вирусов на примере программы Антивирус Касперского.

Теоретические вопросы

1. Возможности корпоративных решений KasperskyLab.
2. Автоматическая настройка программ в процессе установки.
3. Автоматическое обновление баз. Настройка обновлений.
4. Способы настройки системы.
5. Настройка проактивной защиты.
6. Уровни безопасности Файлового антивируса.

Задание 1. Настройте обновление сигнатур антивирусной программы и обновите их.

Задание 2. Изучите настройки Файлового, Почтового и Веб-антивируса.

Задание 3. Проверьте любой внешний носитель информации на вирусы.

Задание 4. Подготовьте доклад и презентацию на тему: «Общие сведения и особенности работы антивирусной программы [Название антивирусной программы]». Название антивирусной программы выбрать согласно своему варианту из вариантов заданий к работе.

Объем доклада 4–5страницы. Слайдов в презентации не менее пяти, по времени 7–10минут.

Варианты заданий

Вариант	Название антивирусной программы
1	AVG
2	Dr.Web
3	Avira
4	Panda AntiVirus
5	McAfee VirusScan
6	Eset Nod32

7	Microsoft Security Essentials
8	Norton AntiVirus
9	Антивирус Касперского
10	Avast!

ПРАКТИЧЕСКАЯ РАБОТА № 36

Изучение функционала и областей применения DLP систем на примере InfoWatch TrafficMonitor или других аналогов

Цель: изучение функционала и областей применения DLP систем на примере InfoWatch Traffic Monitor или других аналогов.

Теоретические вопросы

1. Назначение InfoWatch Traffic Monitor.
2. Возможности InfoWatch Traffic Monitor.
3. Архитектура системы InfoWatch Traffic Monitor.
4. Общие принципы анализа данных.
5. Мониторинг и обработка данных.

Задание 1. Опишите основные функции InfoWatch Traffic Monitor.

Задание 2. Опишите компоненты системы InfoWatch Traffic Monitor

Компонент	**Назначение**
Traffic Monitor Server включает в себя отдельные подсистемы для контроля различных видов трафика а также подсистемы анализа: Decision and Analysis Engine (DAE) (интегрирована с подсистемами контроля), Content Analysis Server (CAS)	
Sniffer	
Management Console	
CreateSchemaWizard	

Задание 4. Опишите варианты настройки приложения InfoWatch Traffic Monitor.

ЛИТЕРАТУРА

Основная учебная литература:

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/476997

Дополнительная учебная литература:

Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2021. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475704