**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Н.В. Калинина
17 марта 2022 г

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по междисциплинарному курсу

МДК.02.01. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

МДК.02.01. Защита информации в информационно телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты. Методические указания по выполнению практических работ.

Составил: Кривоносова Н.В. – Санкт-Петербург, 2022.

Методические указания содержат описания практических занятий, предусмотренных рабочей программой **МДК.02.01. Защита информации в информационно телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты**. Каждая работа рассчитана на 2 академических часа, общий объём составляет 30 часов. Методические указания предназначены для обучающихся очной формы обучения по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рассмотрено и одобрено предметной (цикловой) комиссией информационной безопасности телекоммуникационных систем Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля..

СОДЕРЖАНИЕ

Наименование работы

Практическая работа 1
ПАРАМЕТРЫ БЕЗОПАСНОСТИ. ПОЛИТИКА АУДИТА

1. Цель работы: Ознакомление с понятием параметров безопасности и политикой аудита в области информационной безопасности.

2. Задачи работы:

- Изучить основные понятия параметров безопасности и политики аудита.
- Ознакомиться с типичными параметрами безопасности и их значениями.
- Изучить требования, которые должны удовлетворяться при настройке параметров безопасности.
- Ознакомиться с принципами политики аудита и ее целями.
- Изучить типичные меры, которые применяются в рамках политики аудита для обеспечения безопасности.
- Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Составить описания аудитов:

Аудит событий входа в систему –

Аудит управления учетными записями –

Аудит доступа к службе каталогов –

Аудит события входа –

Аудит доступа к объектам –

Аудит изменения политики –

Аудит использования привилегий –

Аудит отслеживания процессов –

Аудит системных событий –

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;

3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Параметры безопасности - это настройки системы, которые обеспечивают безопасность ее функционирования и защиту информации. К ним относятся, например, параметры контроля доступа, пароли, шифрование данных и т.д. Настройка параметров безопасности должна удовлетворять требованиям безопасности системы и принимать во внимание ее специфические особенности.

Политика аудита - это набор правил и процедур, устанавливающих требования к регистрации и анализу событий в информационной системе. Цель политики аудита - обеспечить контроль за безопасностью системы, выявлять и предотвращать нарушения безопасности.

Практическая работа 2

АПМДЗ КРИПТОН: ИНИЦИАЛИЗАЦИЯ СИСТЕМНОГО АДМИНИСТРАТОРА, ИНИЦИАЛИЗАЦИЯ ПОЛЬЗОВАТЕЛЯ, ПРОВЕРКА ЦЕЛОСТНОСТИ СРЕДЫ

1. **Цель работы**: ознакомиться с процессом инициализации системного администратора и пользователя в системе АПМДЗ Криптон, а также с методами проверки целостности среды.

2. **Задачи работы:**
   - Изучить процесс инициализации системного администратора в системе АПМДЗ Криптон.
   - Ознакомиться с процедурой инициализации пользователя в системе АПМДЗ Криптон.
   - Изучить методы проверки целостности среды в системе АПМДЗ Криптон.
   - Освоить базовые навыки работы с системой АПМДЗ Криптон.

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

   Подготовить бланк отчета.

4. **Задание и порядок работы**
   - Запустить процесс инициализации системного администратора в системе АПМДЗ Криптон и создать учетную запись администратора.
   - Запустить процедуру инициализации пользователя в системе АПМДЗ Криптон и создать учетную запись пользователя.
   - Провести проверку целостности среды в системе АПМДЗ Криптон с помощью предоставленных инструментов и сравнить результаты с ожидаемыми.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Система АПМДЗ Криптон – это программно-аппаратный комплекс для обеспечения защиты информации в автоматизированных системах. Один из основных компонентов системы – это контроллер доступа к защищенным ресурсам. Процесс инициализации системного администратора и пользователя в системе АПМДЗ Криптон включает в себя создание учетных записей, установку прав доступа и прочие настройки, необходимые для работы в системе.

Практическая работа 3
АППАРАТНЫЕ СРЕДСТВА ШИФРОВАНИЯ КРИПТОН: НАСТРОЙКА, ЭКСПЛУАТАЦИЯ

1. **Цель работы**: ознакомиться с аппаратными средствами шифрования Криптон, научить их настраивать и эксплуатировать данные устройства для обеспечения безопасности информации.
2. **Задачи работы:**
   - изучение теоретических основ работы аппаратных средств шифрования Криптон;
   - ознакомление с принципами настройки и эксплуатации аппаратных средств шифрования Криптон;
   - проведение практических занятий по настройке и эксплуатации аппаратных средств шифрования Криптон.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:
- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:
- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета
4. **Задание и порядок выполнения работы**
   - Подготовить рабочую станцию для работы с аппаратными средствами шифрования Криптон.
   - Настроить аппаратное средство шифрования Криптон для работы на данной рабочей станции.
   - Зашифровать файл с помощью аппаратного средства шифрования Криптон.
5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Система АПМДЗ Криптон – это программно-аппаратный комплекс для обеспечения защиты информации в автоматизированных системах. Один из основных компонентов системы – это контроллер доступа к защищенным ресурсам. Процесс инициализации системного администратора и пользователя в системе АПМДЗ Криптон включает в себя создание учетных записей, установку прав доступа и прочие настройки, необходимые для работы в системе.

Практическая работа 4
ПРОГРАММНЫЕ СРЕДСТВА ШИФРОВАНИЯ. ЗАЩИЩЕННЫЕ КОНТЕЙНЕРЫ.

1. **Цель работы**: ознакомить студентов с понятием программных средств шифрования и их применением, а также пониманием концепции защищенных контейнеров.
2. **Задачи работы:**
   - Изучить основы программных средств шифрования.
   - Ознакомиться с понятием защищенных контейнеров и их применением.
   - Научиться создавать и использовать защищенные контейнеры.

Студент должен:
Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Создайте защищенный контейнер с помощью программы VeraCrypt и зашифруйте в него текстовый документ с секретной информацией. Затем расшифруйте документ и убедитесь в его целостности.
5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Программные средства шифрования - это программы, которые позволяют зашифровывать информацию для защиты ее от несанкционированного доступа. Применение программных средств шифрования позволяет повысить уровень безопасности данных, которые передаются по сети или хранятся на компьютере.

Защищенный контейнер - это файл, который создается с помощью специальной программы, такой как VeraCrypt, и который может содержать зашифрованные файлы и папки. При использовании защищенного контейнера требуется вводить пароль для доступа к его содержимому. Контейнер можно перемещать по сети или хранить на флеш-накопителе, при этом содержимое будет защищено от несанкционированного доступа.

Практическая работа 5
ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ТИПОВЫМИ СРЕДСТВАМИ

1. **Цель работы**: ознакомиться с типовыми средствами восстановления информации и научить их применять эти средства для восстановления утерянной информации.

2. **Задачи работы:**
   - изучить основные методы восстановления информации с помощью типовых средств;
   - ознакомиться с характеристиками типовых средств восстановления информации;
   - освоить процесс восстановления информации с помощью типовых средств;
   - научиться анализировать результаты восстановления информации и делать выводы о его качестве.

Студент должен:
Иметь практический опыт:
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;

Уметь:
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Восстановить удаленный файл с помощью программы Recuva. Сначала удалить файл из корзины или удалить его перманентно с помощью Shift+Delete. Затем запустить программу Recuva и восстановить удаленный файл.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Восстановление информации является важным процессом в области информационной безопасности. Это процесс восстановления данных после их потери или повреждения.

Основные методы восстановления информации включают использование резервных копий, восстановление файлов из удаленных областей диска и использование специальных программных средств, таких как средства для восстановления файлов и программ для восстановления данных.

Существуют также типовые средства для восстановления информации, такие как программы для восстановления удаленных файлов, программы для восстановления поврежденных дисков, программы для восстановления данных с поврежденных CD и DVD дисков, а также программы для восстановления данных с цифровых устройств хранения информации.

При восстановлении данных необходимо учитывать параметры безопасности, такие как доступность восстановления только авторизованным пользователям и защита от несанкционированного доступа к восстановленным данным.

Практическая работа 6
ПРОГРАММЫ НАДЕЖНОГО УДАЛЕНИЯ ИНФОРМАЦИИ

1. **Цель работы**: ознакомиться с программами надежного удаления информации и их применением для защиты конфиденциальных данных.

2. **Задачи работы:**
   - изучить принципы работы программ надежного удаления информации;
   - ознакомиться с основными функциями программ надежного удаления информации;
   - научиться использовать программы надежного удаления информации для удаления конфиденциальных данных.

Студент должен:
Иметь практический опыт:
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание**
   Выбрать программный продукт и подготовить доклад:
   - Wipe
   - BCWipe
   - Uninstall Tool
   - Kryptelite
   - Wise Disk Cleaner
   - Total Uninstall
   - Hardwipe

- Eraser
- The Mop

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Программы надежного удаления информации предназначены для безвозвратного удаления данных с жестких дисков, USB-накопителей, SD-карт и других носителей информации. Такие программы позволяют уничтожить данные таким образом, чтобы их восстановление стало невозможным даже специальными методами восстановления данных.

Существует несколько методов надежного удаления информации, которые используются в программных средствах, включая перезапись, уничтожение, криптографическое удаление и др.

Практическая работа 7
АРХИВИРОВАНИЕ ИНФОРМАЦИИ

1. **Цель работы**: ознакомление с принципами архивирования информации, понимание различных форматов архивов, а также навыки создания и извлечения архивов.
2. **Задачи работы:**
   - Изучение принципов архивирования информации
   - Ознакомление с форматами архивов, такими как ZIP, RAR, 7Z и другими
   - Создание архива с помощью программного обеспечения, такого как WinZip, WinRAR или 7-Zip
   - Извлечение файлов из архива и восстановление их в исходное состояние
   - Понимание принципов сжатия и эффективного использования места на диске

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание**

   1. На компьютере в личной папке создать папку с именем «Архивация».
   2. В нее скопировать следующие типы файлов: графический (bmp и jpg), текстовый, звуковой, презентация, табличный,
   3. Заархивировать каждый файл и всю папку, используя программу архиватор 7-zip.
   4. Посмотреть, как измениться размер файла по отношению к размеру архива.
   5. Результаты занести в таблицу и посчитать коэффициент сжатия:

Имя файла	***Тип файла***	***Размер файла***	***Размер архива***	***Коэффициент сжатия***

   6. Сделайте аналогичные действия с другой программой архиватором - ZIP
   7. Сделать вывод по работе. В выводе указать, какие файлы следует сжимать и почему.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Архивирование информации - это процесс упаковки одного или нескольких файлов в один файл, который может быть легко передан или сохранен на диске. Архивы могут использоваться для сжатия файлов и экономии места на диске, а также для упрощения передачи больших объемов данных.

Форматы архивов могут быть открытыми или закрытыми. Открытые форматы, такие как ZIP, могут быть использованы многими программами, в то время как закрытые форматы, такие как RAR, могут быть использованы только с программным обеспечением, которое поддерживает этот формат.

Существуют различные программы для создания и извлечения архивов, такие как WinZip, WinRAR и 7-Zip. Они обычно предоставляют простой и удобный интерфейс для создания, открытия и управления архивами.

Практическая работа 8
ПРОГРАММНЫЕ СРЕДСТВА РЕЗЕРВНОГО КОПИРОВАНИЯ. НАСТРОЙКА RAID-МАССИВОВ

1. **Цель работы**: ознакомиться с принципами и методами создания резервных копий данных, а также настройкой RAID-массивов.

2. **Задачи работы:**
   - Изучение принципов резервного копирования данных и его типов.
   - Изучение принципов работы и настройки RAID-массивов.
   - Ознакомление с программными средствами резервного копирования данных и настройки RAID-массивов.
   - Практическое освоение навыков настройки программных средств резервного копирования и RAID-массивов.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   1. Настройка программного средства резервного копирования данных на компьютере.
   2. Создание полной и дифференциальной резервных копий важных данных.
   3. Восстановление данных из резервных копий.
   4. Настройка RAID-массива на компьютере.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Резервное копирование данных – это процесс создания копии важных данных, которые могут быть использованы для восстановления информации в случае ее потери или повреждения. Существует несколько типов резервного копирования, таких как полное, дифференциальное, инкрементное и т.д.

RAID-массив (от англ. Redundant Array of Independent Disks) – это группа жестких дисков, объединенных в единую систему для повышения производительности и/или надежности. RAID-массивы могут быть настроены на различные уровни, такие как RAID 0, 1, 5, 6, 10 и т.д.

Практическая работа 9
ИНСАЙДЕРСКАЯ ИНФОРМАЦИЯ. ПРОГРАММЫ СБОРА ИНФОРМАЦИИ О ПК

1. **Цель работы**: ознакомиться с понятием "инсайдерская информация", программами сбора информации о ПК и методами защиты от утечки данных.

2. **Задачи работы:**
   - Изучить основные понятия в области защиты информации, связанные с инсайдерской информацией.
   - Ознакомиться с основными программами сбора информации о ПК, их функциональностью и возможностями.
   - Провести анализ утечек информации и выявить возможные причины их возникновения.
   - Разработать рекомендации по защите от утечки данных и предотвращению инцидентов с использованием программных средств.

Студент должен:
Иметь практический опыт:
- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   С помощью программы сбора информации о ПК, например, Speccy, собрать информацию о технических характеристиках компьютера, установленных приложениях, активных процессах и сетевых подключениях. Оценить уровень конфиденциальности полученной информации и разработать рекомендации по ее защите.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Инсайдерская информация - это информация, полученная от внутреннего источника, который имеет законный доступ к ней, но нарушает правила ее использования. Информация может быть украдена, продана или использована для личных целей. В большинстве случаев это происходит непреднамеренно, из-за незнания сотрудниками правил обращения с конфиденциальной информацией. Однако, утечка данных может нанести серьезный ущерб бизнесу или организации. Для защиты от утечки инсайдерской информации используются различные методы, включая обучение персонала, ограничение прав доступа, мониторинг действий сотрудников и использование специальных программных средств.

Практическая работа 10
НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА

1. **Цель работы**: ознакомиться с базовыми понятиями и принципами работы межсетевых экранов, а также приобретение практических навыков настройки межсетевого экрана.

2. **Задачи работы:**
   - Изучить основные понятия и принципы работы межсетевых экранов.
   - Ознакомиться с видами межсетевых экранов и их особенностями.
   - Изучить основные функции и возможности межсетевых экранов.
   - Научиться настраивать межсетевой экран на примере конкретного программного обеспечения.
   - Ознакомиться с принципами работы правил фильтрации трафика на межсетевом экране.
   - Научиться создавать правила фильтрации трафика на межсетевом экране на примере конкретного программного обеспечения.

Студент должен:
Иметь практический опыт:
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   настроить межсетевой экран на своем компьютере с помощью выбранного программного обеспечения, создать несколько правил фильтрации трафика для разных типов сетевых соединений.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;

3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Межсетевой экран (firewall) – это программное или аппаратное средство, которое применяется для защиты компьютеров и сетей от несанкционированного доступа и вредоносного программного обеспечения. Основная функция межсетевого экрана заключается в контроле и фильтрации сетевого трафика между различными сетями.

Существуют разные типы межсетевых экранов: сетевые, периметровые, хост-ориентированные и другие. Каждый тип межсетевого экрана имеет свои особенности и предназначен для определенных задач.

Настройка межсетевого экрана включает в себя создание правил фильтрации трафика для разных типов сетевых соединений, определение доступности сетевых сервисов, создание и настройку виртуальных частных сетей (VPN) и другие функции. Одним из ключевых принципов работы межсетевого экрана является использование правил фильтрации трафика, которые определяют, какие типы трафика разрешены и какие запрещены.

Практическая работа 11
НАСТРОЙКА ИНТЕРФЕЙСОВ ВИРТУАЛЬНЫХ МАШИН

1. **Цель работы**: ознакомиться с процессом настройки интерфейсов виртуальных машин и научить их работать с такими интерфейсами.

2. **Задачи работы:**
   - Изучить основные принципы виртуализации и работу виртуальных машин.
   - Ознакомиться с типами сетевых интерфейсов виртуальных машин и их назначением.
   - Научиться настраивать интерфейсы виртуальных машин на примере популярных виртуальных сред (например, VirtualBox).
   - Продемонстрировать практическое применение настроенных интерфейсов виртуальных машин.

Студент должен:
Иметь практический опыт:
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   1. Запустите виртуальную машину (например, VirtualBox).
   2. Выберите в настройках виртуальной машины тип интерфейса и настройте его (например, выберите NAT, чтобы виртуальная машина могла получать доступ к интернету).
   3. Подключите виртуальную машину к сети и проверьте, что интерфейс работает корректно.

4. Настройте другие типы интерфейсов (например, Bridged или Host-only) и проведите аналогичную проверку их работы.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Виртуализация - это технология, которая позволяет запускать несколько операционных систем на одном физическом компьютере. Виртуальная машина - это программа, которая эмулирует работу физического компьютера и позволяет запускать на нем гостевую операционную систему.

Существует несколько типов сетевых интерфейсов виртуальных машин:

- NAT - позволяет виртуальной машине получать доступ к интернету, но не позволяет внешним компьютерам получать доступ к виртуальной машине.
- Bridged - позволяет виртуальной машине работать в сети так же, как и физический компьютер, т.е. получать свой IP-адрес и быть доступной из внешней сети.
- Host-only - позволяет виртуальной машине работать только в локальной сети, недоступной извне.

Практическая работа 12
КОНФИГУРАЦИЯ ПРАВИЛА ДЛЯ СОВ

1. **Цель работы**: знакомство студентов с настройкой правил для современных систем безопасности, а именно с фильтрацией сетевого трафика на уровне ядра операционной системы Linux.

2. **Задачи работы:**
   - Изучить теоретические основы работы сетевых фильтров на уровне ядра операционной системы Linux.
   - Ознакомиться с инструментами настройки правил для современных систем безопасности, таких как iptables.
   - Научиться создавать правила для фильтрации сетевого трафика на уровне ядра операционной системы Linux.
   - Протестировать созданные правила на практике.

Студент должен:
Иметь практический опыт:
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. **Подготовка к работе**
   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1
   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   Настроить правила для фильтрации сетевого трафика на уровне ядра операционной системы Linux с помощью iptables. Необходимо создать правила, позволяющие разрешать или запрещать доступ к определенным портам и протоколам.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;

4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Linux содержит встроенные сетевые фильтры, которые позволяют выполнять различные операции с сетевым трафиком на уровне ядра операционной системы. Наиболее распространенным инструментом для настройки правил безопасности в Linux является iptables.

Iptables – это утилита командной строки для настройки сетевых правил в Linux. Она позволяет создавать правила, которые определяют, какие типы трафика разрешены, а какие запрещены. В iptables правила обрабатываются последовательно сверху вниз, поэтому порядок правил имеет большое значение.

Для создания правил iptables необходимо определить следующие параметры:

- Тип трафика (TCP, UDP, ICMP и т.д.)
- Исходный IP-адрес и порт
- Назначение IP-адрес и порт

Практическая работа 13
РАЗВЕРТЫВАНИЕ ОТКРЫТЫХ СПИСКОВ ПРАВИЛ

1. **Цель работы**: ознакомиться студентов с процессом развертывания открытых списков правил для обеспечения безопасности в компьютерных сетях.
2. **Задачи работы:**
   - Изучить теоретические основы открытых списков правил.
   - Ознакомиться с основными инструментами для развертывания открытых списков правил.
   - Провести практическое задание по настройке открытых списков правил.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**

   Настройка OPA для контроля доступа к веб-приложению. Студентам нужно настроить OPA на основе правил, которые будут контролировать доступ к веб-приложению. Затем они должны проверить, что приложение работает корректно при заданных правилах.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;

Приложение 1

Краткие сведения из теории

Открытые списки правил (англ. Open Policy Agent, OPA) – это инструмент для автоматизации принятия решений на основе политик безопасности. Они могут использоваться для контроля доступа к ресурсам, настройки сетевых правил и других задач, связанных с безопасностью. OPA поддерживает язык регулярных выражений и позволяет создавать более сложные правила. Он может быть использован в различных средах, включая Kubernetes и другие контейнерные платформы, а также в других сетевых приложениях.

Практическая работа 14
ПОДКЛЮЧЕНИЕ СРЕДСТВА МОНИТОРИНГА

1. **Цель работы**: ознакомиться с процессом подключения средств мониторинга к компьютеру и настройки соответствующих параметров.
2. **Задачи работы:**
   - Узнать о средствах мониторинга и их назначении.
   - Ознакомиться с процессом подключения средств мониторинга к компьютеру и необходимые для этого шаги.
   - Рассмотреть на примере, как настраивать параметры средств мониторинга.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание и порядок выполнения работы**
   - Подключить средство мониторинга (например, датчик температуры или монитор системы).
   - Установить драйверы и программное обеспечение для средства мониторинга.
   - Настроить параметры средства мониторинга и проверить его работу.
5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;

3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Средства мониторинга позволяют отслеживать работу компьютера и собирать информацию о его состоянии. Для этого обычно используются специальные программы или устройства.

Перед подключением средства мониторинга к компьютеру необходимо убедиться, что устройство или программа совместимы с операционной системой компьютера и подключены все необходимые кабели и провода. Затем нужно установить соответствующие драйверы и настроить параметры средства мониторинга.

Практическая работа 15
ВКЛЮЧЕНИЕ РЕЖИМА БЛОКИРОВКИ

1. **Цель работы**: ознакомление с функционалом и настройками режима блокировки и защиты компьютера.
2. **Задачи работы:**
   - Изучение принципов работы режима блокировки компьютера.
   - Ознакомление с настройками режима блокировки и методами его включения.
   - Определение практических применений режима блокировки компьютера.

Студент должен:

Иметь практический опыт:

- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

   Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1

   Подготовить бланк отчета

4. **Задание и порядок работы**

   Включите режим блокировки на своем компьютере. Попробуйте разблокировать компьютер различными способами (ввод пароля, отпечатка пальца и т.д.). Проверьте, какие настройки режима блокировки доступны в настройках вашей операционной системы.

5. **Содержание отчета**

   1. название и цель работы;

2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

Приложение 1

Краткие сведения из теории

Режим блокировки компьютера - это функция, которая временно заблокирует доступ к компьютеру, когда пользователь уходит от него на некоторое время. Режим блокировки помогает защитить данные на компьютере от несанкционированного доступа, например, когда пользователь оставляет свой компьютер в общественном месте. Режим блокировки может быть включен автоматически при определенных условиях, например, когда пользователь уходит от компьютера на определенный период времени или когда экран компьютера закрывается.