**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.03.02. ФИЗИЧЕСКАЯ ЗАЩИТА ЛИНИЙ СВЯЗИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2022

МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей. Методические указания по выполнению практических работ.

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

Методические указания содержат описания практических занятий, предусмотренных рабочей программой **МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей**. Каждая работа рассчитана на 2 академических часа, общий объём составляет 54 часав. Нумерация рисунков, формул и таблиц в пределах одной работы. 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

МДК.03.02. Физическая защита линий связи ИТКС

Практическое занятие 1.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ СЗИ «СТРАЖ NT»

1. **Цель работы**: изучить возможности СЗИ "Страж NT" и способы его настройки для защиты информации.

2. **Задачи работы:**
   - Изучить теоретические основы работы СЗИ "Страж NT".
   - Ознакомиться с возможностями и настройками СЗИ "Страж NT".
   - Провести тестирование и оценку эффективности работы СЗИ "Страж NT".
   - Составить отчет о результатах тестирования.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Изучить возможности СЗИ "Страж NT"

5. **Порядок выполнения работы**
   - Установить и настроить СЗИ "Страж NT" на тестовом сервере.
   - Создать тестовые данные и попытаться получить к ним доступ, не используя авторизацию.
   - Проанализировать логи СЗИ "Страж NT" для выявления несанкционированного доступа и настроить его блокировку.
   - Повторно попытаться получить доступ к тестовым данным и проверить эффективность работы СЗИ "Страж NT".

6. **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;
7) ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что такое СЗИ "Страж NT" и для каких целей он используется?
2. Какие возможности предоставляет СЗИ "Страж NT" для защиты информации?
3. Какие особенности установки и настройки СЗИ "Страж NT"?
4. Каким образом СЗИ "Страж NT" обеспечивает защиту информации при передаче по сети?

Приложение 1

Краткие сведения из теории

СЗИ "Страж NT" - средство защиты информации на базе операционной системы Windows. Он обеспечивает контроль доступа к информации, аудит операций с ней, защиту от внешних угроз и защиту информации при передаче по сети.

Практическое занятие 2.
ИССЛЕДОВАНИЕ ПРОГРАММНОЙ СРЕДЫ «СТРАЖ NT»

1. **Цель работы**: ознакомление студентов с функциональными возможностями программной среды «Страж NT» и ее использованием в обеспечении безопасности информационных систем.

2. **Задачи работы:**
   - Изучить теоретические основы функционирования СЗИ «Страж NT».
   - Ознакомиться с основными функциональными возможностями программной среды «Страж NT».
   - Провести практическое исследование возможностей СЗИ «Страж NT» на примере моделирования атак на информационную систему.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание и порядок выполнения работы**
   - Установить программную среду «Страж NT» на локальный компьютер.
   - Создать тестовую информационную систему и настроить ее работу в программной среде «Страж NT».
   - Провести моделирование атак на созданную систему и оценить работу СЗИ «Страж NT».

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;
   7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое СЗИ «Страж NT» и каковы ее основные функциональные возможности?
2. Каковы задачи, которые может решать СЗИ «Страж NT»?
3. Как провести моделирование атак на информационную систему в программной среде «Страж NT»?

Приложение 1

Краткие сведения из теории

СЗИ «Страж NT» - комплекс программных и аппаратных средств, предназначенный для обеспечения безопасности информационных систем на базе операционной системы Windows NT и ее последующих версий. Программная среда «Страж NT» позволяет осуществлять контроль доступа к ресурсам информационной системы, защиту информации от несанкционированного доступа, контроль целостности и конфиденциальности информации, а также регистрацию и анализ событий в информационной системе

Практическое занятие 3.
УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ «СТРАЖ NT», УЧЕТ ПОЛЬЗОВАТЕЛЕЙ «СТРАЖ NT»

1. **Цель работы**: Изучить возможности управления пользователями и учета пользователей в системе защиты информации "Страж NT".

2. **Задачи работы:**
   - Ознакомиться с функциями управления пользователями в "Страж NT".
   - Изучить способы создания и настройки пользователей в системе.
   - Изучить функции учета пользователей и журналирования действий в системе.
   - Провести практические упражнения для закрепления полученных знаний.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**
   1. Создать нового пользователя в системе "Страж NT" с заданными правами доступа.
   2. Настроить ограничения доступа для созданного пользователя.
   3. Изучить журналы системы и найти записи о действиях созданного пользователя.
   4. Изменить права доступа созданного пользователя и проследить, как это отразится на доступности ресурсов.

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;
   7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое система защиты информации "Страж NT"?
2. Как создать нового пользователя в "Страж NT"?
3. Как настроить права доступа для пользователя в "Страж NT"?
4. Что такое учет пользователей в "Страж NT" и как он реализуется?

Приложение 1

Краткие сведения из теории

Система защиты информации "Страж NT" предоставляет возможность создания и настройки пользователей, управления их правами доступа к ресурсам, а также учета действий пользователей в системе.

Для создания нового пользователя необходимо указать логин и пароль, а также настроить права доступа к ресурсам системы.

Учет пользователей включает в себя ведение журналов действий, которые позволяют отследить все действия пользователя в системе.

Практическое занятие 4.
ИЗБИРАТЕЛЬНОЕ УПРАВЛЕНИЕ «СТРАЖ NT»

1. **Цель работы**: изучение принципов и возможностей избирательного управления в системе "Страж NT".

2. **Задачи работы:**
   - изучение основных понятий и терминов, связанных с избирательным управлением;
   - ознакомление с функциональностью модуля избирательного управления в "Страж NT";
   - научиться создавать избирательные правила и проводить избирательный отбор.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Создать избирательное правило в "Страж NT" для отбора пользователей, у которых истекает срок действия учетной записи в течение ближайших 7 дней

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;
   7) ответы на контрольные вопросы.

6. **Контрольные вопросы к защите**
   1. Что такое избирательное управление в информационной системе?
   2. Какие функции выполняет модуль избирательного управления в "Страж NT"?
   3. Как создать избирательное правило в "Страж NT"?
   4. Какие критерии можно использовать для проведения избирательного отбора

в "Страж NT"?

5. Какие преимущества может дать использование избирательного управления в информационной системе?

Приложение 1

Краткие сведения из теории

Избирательное управление - это процесс управления доступом пользователей к ресурсам информационной системы на основе определенных правил и условий. В "Страж NT" модуль избирательного управления позволяет создавать избирательные правила и проводить избирательный отбор пользователей на основе различных критериев

Практическое занятие 5.
СОРТИРОВКА И ПОИСК С «СТРАЖ NT»

1. **Цель работы**: изучение принципов и возможностей сортировки и поиска данных в системе "Страж NT".

2. **Задачи работы:**
   - изучение основных методов сортировки и поиска данных;
   - ознакомление с функциональностью модуля сортировки и поиска в "Страж NT";
   - научиться выполнять сортировку и поиск данных в "Страж NT".

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

выполнить сортировку списка пользователей по фамилии в алфавитном порядке.

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;
   7) ответы на контрольные вопросы.

6. **Контрольные вопросы к защите**
   1. Какие алгоритмы сортировки поддерживаются в программной среде "Страж NT"?
   2. Какой алгоритм сортировки следует выбрать для сортировки большого массива данных?
   3. Как осуществляется поиск в программной среде "Страж NT"?
   4. Какой алгоритм поиска следует выбрать для поиска элемента в большом массиве данных?

Приложение 1

Краткие сведения из теории

Сортировка и поиск данных - это основные методы работы с большими объемами информации. В "Страж NT" модуль сортировки и поиска позволяет выполнять сортировку и поиск данных в различных таблицах системы.

Практическое занятие 6.
РЕДАКТИРОВАНИЕ ПОЛЬЗОВАТЕЛЕЙ «СТРАЖ NT»

1. **Цель работы**: ознакомление студентов с возможностями редактирования пользователей в программном обеспечении "Страж NT" для управления доступом к информационным ресурсам.

2. **Задачи работы:**
   - Изучить функции редактирования пользователей в "Страж NT".
   - Освоить порядок создания новых пользователей и изменения параметров уже существующих пользователей.
   - Понять принцип работы системы прав доступа "Страж NT"

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание и порядок выполнения работы**
   - Запустите программу "Страж NT".
   - Создайте нового пользователя с помощью функции "Добавить пользователя".
   - Измените параметры уже существующего пользователя с помощью функции "Редактировать пользователя".
   - Протестируйте доступ пользователя к определенным информационным ресурсам.

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;
   7) ответы на контрольные вопросы.

6. **Контрольные вопросы к защите**

1. Что такое "Страж NT"?
2. Какие функции предоставляет программа "Страж NT" для управления пользователями?
3. Какие параметры можно изменить при редактировании пользователя?
4. Зачем необходимо использовать систему прав доступа при работе с конфиденциальной информацией?

Приложение 1

Краткие сведения из теории

"Страж NT" - программа для управления доступом к информационным ресурсам, используемая в операционных системах Windows NT и Windows 2000. Пользователи могут создаваться, удаляться, блокироваться и редактироваться с помощью данной программы. Каждому пользователю назначаются определенные права доступа к файлам и папкам, что позволяет ограничить доступ к конфиденциальной информации.

Практическое занятие 7.
ИЗМЕНЕНИЕ НАСТРОЕК «СТРАЖ NT»

1. **Цель работы**: изучить возможности изменения настроек программной среды "Страж NT".
2. **Задачи работы:**
   - ознакомиться с возможными настройками "Страж NT";
   - понять, как изменять настройки в программе;
   - изучить влияние изменений на работу программы.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми 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. Запустить программу "Страж NT".
2. Выбрать раздел "Настройки" в главном меню.
3. Изучить доступные настройки, их назначение и значения по умолчанию.
4. Изменить одну или несколько настроек и сохранить изменения.
5. Проверить работу программы с новыми настройками.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что позволяет изменять настройки в программе "Страж NT"?
2. Какие параметры программы могут быть изменены с помощью настроек?

3. Кто имеет доступ к изменению настроек "Страж NT"?

Приложение 1

Краткие сведения из теории

"Страж NT" позволяет изменять настройки программы для оптимизации ее работы в соответствии с требованиями пользователя. Настройки могут касаться безопасности, функциональности, внешнего вида и других параметров программы. Некоторые настройки доступны только для администратора системы.

Практическое занятие 8.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ «СИГУРД М19»

1. **Цель работы**: ознакомиться с функциональными возможностями системы безопасности "Сигурд М19" и показать, как ее можно использовать для защиты информации.

2. **Задачи работы:**
   - Изучить основные характеристики и возможности системы "Сигурд М19".
   - Ознакомиться с процедурой установки и настройки системы.
   - Освоить основные функции системы: мониторинг, аудит, защита данных, управление доступом и т.д.
   - Провести практические упражнения по настройке системы и ее основным функциям.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Настроить систему мониторинга событий на компьютере с помощью "Сигурд М19" и настроить уведомления о подозрительной активности. Затем провести тестирование системы, попробовав провести несколько запрещенных действий 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;
   7) ответы на контрольные вопросы.

6. **Контрольные вопросы к защите**
   1. Что такое "Сигурд М19"?

2. Какие функции обеспечивает "Сигурд М19"?
3. Каковы основные характеристики системы "Сигурд М19"?
4. Какие ресурсы могут быть защищены с помощью "Сигурд М19"?
5. Какие настройки доступны в системе "Сигурд М19" для контроля доступа пользователей?

Приложение 1

Краткие сведения из теории

"Сигурд М19" - это система безопасности, которая обеспечивает защиту информации на уровне операционной системы. Она предназначена для защиты от утечки информации, контроля доступа к ресурсам и аудита действий пользователей. Система может быть настроена для автоматической блокировки доступа к ресурсам в случае нарушения политики безопасности.

Практическое занятие 9.
ПОДГОТОВКА К РАБОТЕ «СИГУРД М19»

1. **Цель работы**: ознакомление с подготовкой к работе с программным комплексом "Сигурд М19".

2. **Задачи работы:**
   - изучение основных этапов подготовки к работе с "Сигурд М19";
   - ознакомление с возможностями программного комплекса;
   - практическое освоение процесса подготовки к работе с "Сигурд М19".

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Провести установку и настройку "Сигурд М19" на компьютере.

5. **Порядок выполнения работы**
   - Загрузить установочный файл "Сигурд М19" с официального сайта разработчика или с диска, если он был предоставлен.
   - Запустить установочный файл и следовать инструкциям мастера установки. Обычно требуется принять лицензионное соглашение, выбрать место установки и настройки по умолчанию.
   - После завершения установки запустить "Сигурд М19".
   - Открыть настройки программы и ввести информацию о своей организации, включая название, адрес и телефон.
   - Настроить параметры безопасности, включая установку пароля для доступа к программе и настройку прав доступа пользователей.
   - Добавить пользователей и настроить их права доступа.
   - Заполнить справочники и настроить систему учета и отчетности.
   - Проверить работоспособность программы и правильность настроек..

6. **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;
7) ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что такое "Сигурд М19"?
2. Какие возможности предоставляет "Сигурд М19"?
3. Какие основные этапы подготовки к работе с "Сигурд М19" можно выделить?
4. Какое практическое задание может быть выполнено студентами для овладения процессом подготовки к работе с "Сигурд М19"?

Приложение 1

Краткие сведения из теории

"Сигурд М19" – это программный комплекс для обработки, анализа и хранения информации, разработанный для обеспечения безопасности информации в организациях различного уровня. Он предоставляет возможности по защите информации, контролю доступа, мониторингу сетевых ресурсов и системного администрирования.

Практическое занятие 10.
ПОИСК СИГНАЛОВ ПЭМИН «СИГУРД М19»

1. **Цель работы**: изучить принципы поиска сигналов ПЭМИН с помощью программного комплекса «СИГУРД М19».
2. **Задачи работы:**
   - Ознакомиться с принципами работы программного комплекса «СИГУРД М19».
   - Изучить методы поиска сигналов ПЭМИН.
   - Практически освоить работу с программным комплексом «СИГУРД М19».
   - Проанализировать полученные результаты и сделать выводы.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми 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. Запустить программный комплекс «СИГУРД М19».
2. Настроить параметры поиска сигналов ПЭМИН.
3. Выполнить поиск сигналов на заданной области.
4. Проанализировать полученные результаты поиска и определить наиболее вероятные места нахождения сигналов.
5. Сделать выводы по результатам проведенного поиска.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое ПЭМИН?
2. Как работает программный комплекс «СИГУРД М19»?
3. Какие методы используются для поиска сигналов ПЭМИН?
4. Какие параметры можно настроить в программном комплексе «СИГУРД М19»?
5. Какие места наиболее вероятны для нахождения сигналов ПЭМИН?

Приложение 1

Краткие сведения из теории

Программный комплекс «СИГУРД М19» предназначен для поиска сигналов ПЭМИН (переносное электронное средство малой мощности) и позволяет определить их местоположение с высокой точностью. Программа работает на основе измерения интенсивности поля, возникающего при работе этих устройств, и анализа полученных данных.

Практическое занятие 11.
АНАЛИЗ СИГНАЛОВ «СИГУРД М19»

1. **Цель работы**: ознакомиться с возможностями анализа сигналов с помощью программы "Сигурд М19" и научить применять различные методы анализа.

2. **Задачи работы:**
   - Ознакомиться с основными методами анализа сигналов: Фурье-анализ, вейвлет-анализ, спектральный анализ.
   - Научиться работать с программой "Сигурд М19" и применять различные методы анализа на практике.
   - Провести анализ сигналов различных типов и сравнить результаты различных методов анализа.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Проанализировать сигналы различных типов (например, звуковые, электрические) с помощью программы "Сигурд М19" и применить различные методы анализа(проанализировать гармонические сигналы разной частоты и амплитуды, шумы различной природы)

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;
   7) ответы на контрольные вопросы.

6. **Контрольные вопросы к защите**

1. Что такое Фурье-анализ?
2. Как работает вейвлет-анализ?
3. Что такое спектральный анализ?
4. Какие методы анализа сигналов доступны в программе "Сигурд М19"?
5. Как можно использовать программу "Сигурд М19" для анализа звуковых сигналов?

Приложение 1

Краткие сведения из теории

Программа "Сигурд М19" предназначена для анализа сигналов и имеет множество инструментов для работы с сигналами, включая Фурье-анализ, вейвлет-анализ, спектральный анализ и другие методы. Фурье-анализ позволяет представить сигнал в виде суммы гармонических функций различных частот и амплитуд. Вейвлет-анализ позволяет анализировать сигналы с различными частотами и различными временными интервалами. Спектральный анализ позволяет определить спектральную плотность мощности сигнала.

Практическое занятие 12.
ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОЗДАНИЯ СКУД ОБЪЕКТА ИНФОРМАТИЗАЦИИ НА ОСНОВЕ НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ

1. **Цель работы**: иметь представление о необходимости создания системы контроля и управления доступом (СКУД) на объектах информатизации на основе нормативных и методических документов.

2. **Задачи работы:**

- Ознакомиться с основными понятиями и принципами работы систем контроля и управления доступом;
- Рассмотреть основные нормативные и методические документы, регулирующие создание СКУД;
- Объяснить необходимость создания СКУД на объектах информатизации;
- Предоставить пример успешной реализации СКУД на объектах информатизации

Студент должен:

Иметь практический опыт:

- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:

- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи 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 план создания СКУД на объекте информатизации на основе номативных и методических документов.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое СКУД и какие принципы ее работы?
2. Какие нормативные документы регулируют создание СКУД

Приложение 1

Краткие сведения из теории

Система контроля и управления доступом (СКУД) – это комплекс программных и аппаратных средств, предназначенный для организации контроля доступа на объектах информатизации. Основными принципами работы СКУД являются: идентификация, аутентификация и авторизация.

Идентификация – это определение личности пользователя.

Аутентификация – это проверка подлинности личности пользователя.

Авторизация – это определение прав доступа пользователя.

Нормативные и методические документы, регулирующие создание СКУД:

1. ФЗ от 27 июля 2006г. N 152-ФЗ «О персональных данных»;
2. ГОСТ Р ИСО/МЭК 27001-2013 «Информационная технология. Методы обеспечения информационной безопасности. Системы менеджмента информационной безопасности. Требования»;
3. Приказ Федеральной службы безопасности РФ от 19.06.2019 N 295 «Об утверждении Порядка создания, организации работы и обеспечения безопасности систем контроля и управления доступом на объектах информатизации, объектах технического и информационного обеспечения государственной важности, а также правил установки и эксплуатации систем контроля и управления доступом на указанных объектах».

Практическое занятие 13.
МОДЕЛИ НАРУШИТЕЛЕЙ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

1. **Цель работы**: изучить модели нарушителей физической безопасности объекта информатизации, чтобы иметь представление о возможных угрозах и рисках для безопасности информации и объекта

2. **Задачи работы:**
   - изучить основные модели нарушителей физической безопасности (внутренние, внешние, организованные, непрофессиональные и т.д.);
   - описать каждую модель нарушителя и привести примеры реальных ситуаций;
   - оценить уровень рисков для безопасности информации и объекта при использовании каждой модели нарушителя;
   - предложить меры по защите объекта информатизации от каждой модели нарушителя.

Студент должен:
Иметь практический опыт:
- установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. Задание

Создать презентацию на тему "Модели нарушителей физической безопасности объекта информатизации". В презентации необходимо описать каждую модель нарушителя, привести примеры реальных ситуаций, оценить уровень рисков для безопасности информации и объекта при использовании каждой модели нарушителя, а также предложить меры по защите объекта информатизации от каждой модели нарушителя.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое модели нарушителей физической безопасности объекта информатизации?
2. Какие основные модели нарушителей вы знаете?
3. Что такое внутренние нарушители и каковы риски их деятельности?

Приложение 1

Краткие сведения из теории

Модели нарушителей физической безопасности объекта информатизации включают в себя различные типы нарушителей, которые могут причинить ущерб безопасности информации и объекта. Основные модели нарушителей:

- внутренние нарушители, которые имеют доступ к объекту информатизации и нарушают безопасность изнутри;
- внешние нарушители, которые пытаются получить доступ к объекту информатизации извне;
- организованные нарушители, которые действуют в организованных группах и планируют нарушения;
- непрофессиональные нарушители, которые не имеют специальных навыков и оборудования для нарушения безопасности.

Практическое занятие 14.
РАЗРАБОТКА ТОПОЛОГИИ МНОГОЗОНАЛЬНОЙ И МНОГОРУБЕЖНОЙ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТА

1. **Цель работы**: Ознакомление студентов с процессом разработки топологии многозональной и многорубежной системы физической защиты объекта информатизации

2. **Задачи работы:**
   - Ознакомить студентов с понятием многозональной и многорубежной системы физической защиты.
   - Рассмотреть основные принципы разработки топологии системы физической защиты объекта информатизации.
   - Изучить методы выбора оборудования для системы физической защиты.
   - Провести практическое задание по разработке топологии многозональной и многорубежной системы физической защиты.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. Задание

Разработать топологию многозональной и многорубежной системы физической защиты объекта информатизации. Определить количество зон и рубежей, расположение оборудования и соединений между ними. Выбрать оборудование для системы физической защиты и описать его основные характеристики.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое многозональная система физической защиты?
2. Какие принципы разработки топологии системы физической защиты существуют?

Приложение 1

Краткие сведения из теории

Многозональная система физической защиты — это система, состоящая из нескольких зон физической защиты, каждая из которых выполняет свои задачи по обеспечению безопасности объекта. Каждая зона имеет свой уровень доступа и свои методы защиты.

Многорубежная система физической защиты — это система, состоящая из нескольких рубежей физической защиты, которые выполняют функцию контроля доступа к объекту информатизации. Каждый рубеж имеет свой уровень доступа и свои методы защиты.

Топология системы физической защиты определяет структуру системы, расположение оборудования и соединений между ними. Основными принципами разработки топологии системы физической защиты являются принципы минимизации зон и рубежей, принцип открытости системы, принцип сокрытия информации об устройстве системы.

Практическое занятие 15.
РАЗРАБОТКА СТРУКТУРНОЙ И ФУНКЦИОНАЛЬНОЙ СХЕМ СКУД

1. **Цель работы**: ознакомиться с процессом разработки структурной и функциональной схем системы контроля и управления доступом (СКУД) и обеспечить понимание необходимости их разработки.
2. **Задачи работы:**
   - Изучить принципы и функции СКУД.
   - Ознакомиться с требованиями, предъявляемыми к структурной и функциональной схемам СКУД.
   - Разработать структурную схему СКУД, определив ее основные компоненты и связи между ними.
   - Разработать функциональную схему СКУД, определив основные функции и процессы, выполняемые компонентами структурной схемы.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- использовать средства физической защиты линий связи ИТКС;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

3. Подготовка к работе

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

Подготовить бланк отчета.

4. Задание

Разработать структурную и функциональную схемы СКУД для офисного здания. Структурная схема должна включать следующие компоненты: контроллер доступа, считыватель карт, электромагнитный замок, датчик двери, мониторинг состояния системы. Функциональная схема должна описывать процессы: аутентификация пользователя, проверка доступа, управление дверным замком, мониторинг состояния 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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое СКУД и какие функции она выполняет?
2. Какие компоненты входят в состав СКУД?
3. Что такое структурная схема СКУД и за что она отвечает?
4. Что такое функциональная схема СКУД и за что она отвечает?

Приложение 1

Краткие сведения из теории

Система контроля и управления доступом (СКУД) предназначена для обеспечения безопасности объектов путем контроля доступа к ним. Она состоит из компонентов, таких как контроллеры доступа, считыватели карт, замки, датчики дверей и многие другие. Структурная схема СКУД описывает взаимодействие компонентов системы, а функциональная схема определяет основные процессы, выполняемые компонентами.

Практическое занятие 16.
РАЗРАБОТКА ОСНОВНЫХ ОРГАНИЗАЦИОННЫХ ДОКУМЕНТОВ СЛУЖБЫ РЕЖИМА ПРЕДПРИЯТИЯ

1. **Цель работы**: ознакомиться с процессом разработки организационных документов службы режима предприятия и их значением для обеспечения безопасности.
2. **Задачи работы:**
   - Изучить основные организационные документы, необходимые для работы службы режима предприятия.
   - Освоить методику разработки организационных документов.
   - Составить перечень необходимых документов для конкретного предприятия.
   - Разработать основные организационные документы для службы режима предприятия.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. Подготовка к работе

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

Подготовить бланк отчета.

4. Задание

Разработать проект организационных документов для службы режима предприятия, включающий:
- Инструкцию по режиму и допуску на предприятие;
- Положение о службе режима предприятия;

- Правила внутреннего трудового распорядка;
- Положение о порядке оформления пропусков.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Какие организационные документы необходимы для работы службы режима предприятия?
2. Какие правила и положения регламентируют порядок доступа на объекты предприятия?
3. Какие функции выполняет служба режима предприятия?
4. Какие основные документы должны быть разработаны для службы режима предприятия?

Приложение 1

Краткие сведения из теории

Организационные документы службы режима предприятия являются необходимым инструментом для обеспечения безопасности на предприятии. Они включают инструкции, правила и положения, регламентирующие порядок доступа на объекты предприятия, охрану имущества, режим труда и отдыха работников и т.д.

Практическое занятие 17.
РАЗРАБОТКА МЕТОДИК КОНТРОЛЯ ЭФФЕКТИВНОСТИ СКУД

1. **Цель работы**: ознакомиться с методиками контроля эффективности системы контроля и управления доступом (СКУД) на объекте информатизации.
2. **Задачи работы:**
   - Изучить принципы работы СКУД и основные параметры эффективности системы.
   - Разработать методики контроля эффективности СКУД на объекте информатизации.
   - Провести анализ полученных результатов контроля эффективности СКУД и предложить меры по их улучшению

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Создать план контроля эффективности СКУД на конкретном объекте информатизации, определить критерии оценки и разработать методики измерения этих критериев. Провести тестирование СКУД на основе разработанных методик и проанализировать полученные результаты.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое СКУД и для чего она предназначена?
2. Какие параметры эффективности СКУД являются ключевыми?
3. Что включает в себя методика контроля эффективности СКУД?

Приложение 1

Краткие сведения из теории

Система контроля и управления доступом (СКУД) предназначена для ограничения доступа к объектам информации на основе установленных правил и политик безопасности. Ключевыми параметрами эффективности СКУД являются:

- точность определения легитимности пользователей;
- скорость обработки запросов на доступ;
- отказоустойчивость и надежность системы

Практическое занятие 18.
РАССМОТРЕНИЕ ПРИНЦИПОВ УСТРОЙСТВА, РАБОТЫ И ПРИМЕНЕНИЯ СРЕДСТВ ВИДЕОНАБЛЮДЕНИЯ

1. **Цель работы**: изучение принципов работы и применения средств видеонаблюдения в системах безопасности.

2. **Задачи работы:**
   - Рассмотреть принципы устройства средств видеонаблюдения.
   - Определить основные принципы работы средств видеонаблюдения.
   - Изучить области применения средств видеонаблюдения.
   - Рассмотреть вопросы применения средств видеонаблюдения в системах безопасности

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Изучить устройство и принцип работы конкретного устройства видеонаблюдения, провести его настройку и подключение, а также проанализировать снятые видеоматериалы.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое средства видеонаблюдения?
2. Какие области применения средств видеонаблюдения вы знаете?
3. Что такое аналоговые и цифровые средства видеонаблюдения?
4. Какие задачи может решать средство видеонаблюдения в системах безопасности?

Приложение 1

Краткие сведения из теории

Средства видеонаблюдения – это комплекс устройств, предназначенных для наблюдения за происходящими процессами, с помощью зафиксированных видеоматериалов. Они используются в различных областях, таких как техническое наблюдение, безопасность, мониторинг и контроль. Они могут быть как аналоговыми, так и цифровыми.

Средства видеонаблюдения могут использоваться для:

- Охраны и безопасности на территории предприятий, учреждений и в общественных местах.
- Видеонаблюдения на производстве и технического контроля.
- Видеонаблюдения в медицине и науке.
- Для контроля транспортных потоков.

Практическое занятие 19.
РАССМОТРЕНИЕ ПРИНЦИПОВ УСТРОЙСТВА, РАБОТЫ И ПРИМЕНЕНИЯ СРЕДСТВ КОНТРОЛЯ ДОСТУПА

1. **Цель работы**: изучение принципов устройства, работы и применения средств контроля доступа для обеспечения безопасности объекта информатизации.

2. **Задачи работы:**
   - Изучение основных принципов устройства средств контроля доступа.
   - Рассмотрение различных типов средств контроля доступа и их применения.
   - Изучение основных этапов проектирования системы контроля доступа.
   - Практическое задание на выбор оптимальной системы контроля доступа для объекта информатизации.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

выбрать объект информатизации (например, офисное здание) и разработать концепцию системы контроля доступа для данного объекта, учитывая его особенности, требования безопасности и бюджетные ограничения. Предложить несколько вариантов систем контроля доступа, сравнить их по параметрам, таким

как надежность, удобство использования, цена и др. Выбрать оптимальный вариант и представить его в виде презентации.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое средства контроля доступа?
2. Какие технологии могут использоваться в системах контроля доступа?
3. Какие уровни доступа могут быть включены в систему контроля доступа?
4. Как выбрать оптимальную систему контроля доступа для объекта информатизации?

Приложение 1

Краткие сведения из теории

Средства контроля доступа предназначены для ограничения доступа к объекту информатизации для неавторизованных лиц. Они могут включать в себя различные технологии, такие как считыватели карт, биометрические сенсоры (сканеры отпечатков пальцев, распознавание лица и т.д.), PIN-коды и т.д. Система контроля доступа может быть оснащена различными уровнями доступа в зависимости от должности и роли сотрудника в организации

Практическое занятие 20.
РАССМОТРЕНИЕ ПРИНЦИПОВ УСТРОЙСТВА, РАБОТЫ И ПРИМЕНЕНИЯ СИСТЕМЫ СБОРА И ОБРАБОТКИ ИНФОРМАЦИИ

1. **Цель работы**: изучение принципов устройства, работы и применения системы сбора и обработки информации для обеспечения безопасности объектов.

2. **Задачи работы:**
   - Изучить теоретические основы системы сбора и обработки информации.
   - Ознакомиться с принципами устройства и работы системы.
   - Изучить примеры применения системы в реальных объектах.
   - Освоить базовые навыки работы с системой сбора и обработки информации.

Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Создание диаграммы блоков системы сбора и обработки информации с описанием работы каждого блока.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое система сбора и обработки информации?
2. Какие блоки входят в систему сбора и обработки информации?
3. Какие задачи решает система сбора и обработки информации?
4. В каких сферах можно применять систему сбора и обработки информации?

Приложение 1

Краткие сведения из теории

Система сбора и обработки информации - это комплекс технических средств, предназначенный для контроля и обеспечения безопасности объектов. Она состоит из различных блоков, таких как датчики, анализаторы, контроллеры, архиваторы, и т.д. Они работают совместно для сбора, обработки, анализа и хранения информации о происходящих событиях на объекте.

Практическое занятие 21.
СРАВНЕНИЕ ОТЕЧЕСТВЕННЫХ ССОИ

1. **Цель работы**: ознакомление с отечественными системами средств обеспечения информационной безопасности (ССОИ) и их сравнительный анализ

2. **Задачи работы:**
   - Изучить основные характеристики отечественных ССОИ.
   - Сравнить функциональность и особенности работы различных систем.
   - Определить преимущества и недостатки каждой системы.
   - Сформулировать рекомендации по выбору наиболее подходящей ССОИ для конкретных задач.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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**

провести сравнительный анализ двух отечественных ССОИ на основе их технических характеристик, функциональности, стоимости и отзывов пользователей.

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;
    7) ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
    1. Что такое отечественные ССОИ?
    2. Какие типы отечественных ССОИ существуют?
    3. Какие задачи решает система обнаружения и предотвращения вторжений?
    4. Для чего используется система контроля доступа?
    5. Что такое система мониторинга и аудита?

Приложение 1

Краткие сведения из теории

Отечественные ССОИ предназначены для защиты информации от несанкционированного доступа, внешних и внутренних угроз, а также обеспечения конфиденциальности, целостности и доступности информации. Существует несколько различных типов отечественных ССОИ, включая системы антивирусной защиты, системы обнаружения и предотвращения вторжений, системы защиты периметра, системы контроля доступа, системы шифрования, системы мониторинга и аудита и т.д.

Практическое занятие 22.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ РАДИОЛОКАТОРА NR-900EMS

1. **Цель работы**: ознакомиться с возможностями и особенностями радиолокатора NR-900EMS.
2. **Задачи работы:**
   - Ознакомиться с теоретическими основами работы радиолокатора.
   - Изучить технические характеристики радиолокатора NR-900EMS.
   - Определить возможности радиолокатора в различных условиях эксплуатации.
   - Определить особенности использования радиолокатора в различных целях.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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. Изучение технических характеристик радиолокатора NR-900EMS.
2. Сравнение радиолокатора NR-900EMS с другими радиолокаторами.

3. Разработка сценариев использования радиолокатора в различных условиях.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое радиолокатор?
2. Каковы технические характеристики радиолокатора NR-900EMS?
3. Для каких целей можно использовать радиолокатор NR-900EMS?
4. Что можно обнаружить с помощью радиолокатора NR-900EMS?
5. Каковы особенности работы радиолокатора NR-900EMS в различных условиях?

Приложение 1

Краткие сведения из теории

Радиолокатор NR-900EMS – это радиолокационная станция с дальностью обнаружения до 500 км и высотой обнаружения до 50 км. Радиолокатор обладает высокой точностью и надежностью в работе. Он может использоваться для обнаружения и отслеживания различных объектов, включая самолеты, корабли, машины, здания и другие объекты.

Практическое занятие 23.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРИБОРА ST 033P ПИРАНЬЯ

1. **Цель работы**: ознакомить студентов с принципами работы и возможностями прибора ST 033P "Пиранья".

2. **Задачи работы:**
   - Рассмотреть принцип работы прибора ST 033P "Пиранья".
   - Изучить основные параметры и характеристики прибора.
   - Изучить области применения прибора.
   - Освоить методы работы с прибором и интерпретации результатов.

Студент должен:

Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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**

Провести измерения с помощью прибора ST 033P "Пиранья" и проанализировать результаты измерений.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Как работает прибор ST 033P "Пиранья"?
2. Какие параметры и характеристики прибора необходимо учитывать при работе с ним?
3. В каких областях применяется прибор ST 033P "Пиранья"?
4. Какие преимущества имеет прибор ST 033P "Пиранья" по сравнению с другими методами измерения уровня жидкости?

Приложение 1

Краткие сведения из теории

ST 033P "Пиранья" - это прибор, основанный на микроволновой технике и используется для измерения уровня жидкости в емкостях различной формы и материала. Принцип работы прибора заключается в замере изменения амплитуды отраженного от поверхности жидкости микроволнового сигнала. Прибор обладает высокой точностью и надежностью в измерениях.

Практическое занятие 24.
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ АНАЛИЗАТОРА СПЕКТРА OSCOR GREEN

1. **Цель работы**: изучение принципов работы и возможностей анализатора спектра OSCOR GREEN.

2. **Задачи работы:**
   - Изучение основных принципов работы анализатора спектра OSCOR GREEN.
   - Изучение возможностей прибора в обнаружении и анализе радиоэлектронных сигналов.
   - Ознакомление с функциональными возможностями и настройками прибора.
   - Практическое использование прибора для анализа радиоэлектронных сигналов.

Студент должен:
Иметь практический опыт:
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
- организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых 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**

Провести анализ радиочастотного спектра в заданной области частот с помощью анализатора спектра OSCOR GREEN.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Для чего используется анализатор спектра OSCOR GREEN?
2. Какой диапазон частот охватывает прибор?
3. Какие функциональные возможности имеет анализатор спектра OSCOR GREEN?
4. Какие характеристики радиосигналов можно определить с помощью прибора?
5. Какие преимущества имеет анализатор спектра OSCOR GREEN перед другими анализаторами спектра?

Приложение 1

Краткие сведения из теории

Анализатор спектра OSCOR GREEN предназначен для обнаружения и анализа радиоэлектронных сигналов в широком диапазоне частот от 10 кГц до 24 ГГц. Он имеет высокую чувствительность, быстродействие и точность измерения. С помощью прибора можно исследовать частотный спектр радиосигналов, определить их мощность и амплитуду, а также выявить наличие помех и перегрузок.

Практическое занятие 25.
ПРОВЕДЕНИЕ АНАЛИЗА ЗАЩИЩАЕМОЙ В КАБИНЕТЕ РУКОВОДИТЕЛЯ ИНФОРМАЦИИ

1. **Цель работы**: научиться проводить анализ уровня защищенности кабинета руководителя информации и выявлять потенциальные уязвимости

2. **Задачи работы:**
   - Изучение основных принципов защиты информации.
   - Осмотр кабинета руководителя информации и оценка уровня его защищенности.
   - Определение потенциальных уязвимостей и рекомендации по их устранению.
   - Разработка плана улучшения уровня защищенности кабинета руководителя информации.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- применять нормативные правовые акты и нормативные методические документы в области защиты информации.

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
- принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

ПК:
- ПК 3.2Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
- ПК 3.3Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. Задание

Провести анализ защищенности кабинета руководителя информации в учебных или реальных условиях.

5. Порядок выполнения работы

При этом нужно обратить внимание на следующие аспекты:

- Физическая защита кабинета: наличие замков, противопожарных систем, охраны и т.д.
- Логическая защита: наличие паролей, протоколов безопасности, механизмов аутентификации и т.д.
- Техническая защита: наличие антивирусных программ, брандмауэров, систем мониторинга и т.д.

6. 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;
    7) ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что такое защита информации и какие цели она преследует?
2. Какие аспекты защиты информации вы можете выделить?
3. Какие меры защиты могут быть применены в кабинете руководителя информации?
4. Какие потенциальные уязвимости могут быть выявлены в кабинете руководителя информации?

Приложение 1

Краткие сведения из теории

Защита информации — это комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности информации. Кабинет руководителя информации содержит важную и часто конфиденциальную информацию, поэтому его защита является особенно важной.

Практическое занятие 26.
МОДЕЛИРОВАНИЕ УГРОЗ ВОЗДЕЙСТВИЯ НА ИСТОЧНИКИ ИНФОРМАЦИИ

1. Цель работы: ознакомление с основами моделирования угроз воздействия на источники информации и умение проводить анализ уязвимостей.

2. Задачи работы:

- изучение основных методов моделирования угроз;
- ознакомление с понятием уязвимости информационных систем;
- проведение анализа уязвимостей источника информации;
- определение возможных угроз и мер по их предотвращению.

Студент должен:

Иметь практический опыт:

- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:

- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;

Знать:

- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:

- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. Подготовка к работе

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

Подготовить бланк отчета.

4. Задание

1. Выбрать информационную систему, которую необходимо защитить.

2. Описать уязвимости данной системы.
3. Разработать сценарий угрозы воздействия на данную систему.
4. Предложить меры по предотвращению угрозы.

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;
7) ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое моделирование угроз?
2. Что такое уязвимость информационной системы?
3. Какие методы можно использовать для предотвращения угрозы воздействия на источники информации?

Приложение 1

Краткие сведения из теории

Моделирование угроз – это процесс создания упрощенной модели, которая отражает потенциальные угрозы информационной системе. Она позволяет определить, какие именно угрозы могут быть опасны для системы, а также какими методами их можно предотвратить или минимизировать.

Уязвимость информационной системы – это слабое место в ее защите, которое может использоваться злоумышленником для получения доступа к конфиденциальной информации или нарушения функционирования системы.

Практическое занятие 27.
РАЗРАБОТКА И ОСУЩЕСТВЛЕНИЕ МЕР ПО ПРЕДОТВРАЩЕНИЮ ПРОНИКНОВЕНИЯ ЗЛОУМЫШЛЕННИКА К ИСТОЧНИКАМ ИНФОРМАЦИИ

1. **Цель работы**: ознакомиться с основными методами разработки и реализации мер по предотвращению проникновения злоумышленника к источникам информации.

2. **Задачи работы:**
   - Изучить основные способы проникновения злоумышленников к источникам информации.
   - Разработать меры по защите информации от нежелательного доступа.
   - Осуществить контроль и анализ эффективности мер защиты информации.

Студент должен:
Иметь практический опыт:
- защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
- проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Уметь:
- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;

Знать:
- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
- основные типы технических средств защиты информации от утечки по техническим каналам;
- порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
- содержание и организацию работ по физической защите линий связи ИТКС;
- принципы действия и основные характеристики технических средств физической защиты;
- законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

ПК:
- ПК 3.1Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно телекоммуникационных системах и сетях
- ПК 3.4Проводить отдельные работы по физической защите линий связи информационно телекоммуникационных систем и сетей

3. **Подготовка к работе**

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

Подготовить бланк отчета.

4. **Задание**

Разработать план мер по защите информации от нежелательного доступа для вымышленной компании, работающей в сфере банковского дела. В плане должны быть учтены все возможные угрозы и методы их предотвращения.

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;
    7) ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
    1. Что такое социальная инженерия?
    2. Какие средства защиты информации могут быть использованы для предотвращения проникновения злоумышленника к источникам информации?
    3. Что такое ролевая модель доступа к информации?
    4. Что такое мониторинг событий и зачем он необходим при защите информации?

Приложение 1

Краткие сведения из теории

Проникновение злоумышленника к источникам информации может происходить через различные каналы связи, уязвимости программного и аппаратного обеспечения, а также при помощи социальной инженерии. Для предотвращения таких атак могут быть использованы следующие меры:

- ограничение доступа к информации на основе ролевой модели;
- использование средств криптографической защиты данных;
- мониторинг событий, связанных с доступом к информации;
- усиление защиты сети и периметра системы;
- обучение сотрудников правилам безопасности информации и методам защиты от социальной инженерии.