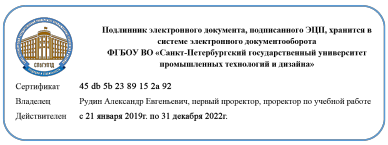
Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ И ДИЗАЙНА»**

УТВЕРЖДАЮ
Первый проректор, проректор по учебной работе

_____ А.Е. Рудин

«30» июня 2020 г.




# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

| Б1.Б.25 | Безопасность корпоративных компьютерных сетей |
|---|---|
| *(Индекс дисциплины)* | *(Наименование дисциплины)* |

Кафедра: 20 Интеллектуальных систем и защиты информации
*Код* *Наименование кафедры*

Направление подготовки: 10.03.01 Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем (в коммерческих структурах)

Уровень образования: **бакалавриат**

**План учебного процесса**

| Составляющие учебного процесса | | Очное обучение | Очно-заочное обучение | Заочное обучение |
|---|---|---|---|---|
| Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы) | Всего | 180 | | |
| | Аудиторные занятия | 68 | | |
| | Лекции | 34 | | |
| | Лабораторные занятия | 17 | | |
| | Практические занятия | 17 | | |
| | Самостоятельная работа | 76 | | |
| | Промежуточная аттестация | 36 | | |
| Формы контроля по семестрам (номер семестра) | Экзамен | 7 | | |
| | Зачет | | | |
| | Контрольная работа | | | |
| | Курсовой проект (работа) | | | |
| **Общая трудоемкость дисциплины** (зачетные единицы) | | 5 | | |

| Форма обучения: | Распределение зачетных единиц трудоемкости по семестрам | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Очная | | | | | | | 5 | | | | | |
| Очно-заочная | | | | | | | | | | | | |
| Заочная | | | | | | | | | | | | |

Санкт-Петербург
2020

Программа государственной итоговой аттестации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по соответствующему направлению подготовки

и на основании учебного плана № 1/1/704

# 1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

### 1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1: Базовая [X] Обязательная [X] Дополнительно является факультативом [ ]
Вариативная [ ] По выбору [ ]

### 1.2. Цель дисциплины

Сформировать компетенции обучающегося в области безопасности корпоративных компьютерных сетей.

### 1.3. Задачи дисциплины

- Рассмотреть теоретические аспекты в области построения и функционирования безопасности сетей корпоративного типа;
- Раскрыть принципы современных систем безопасности корпоративных сетей;
- Продемонстрировать особенности современных принципов построения систем безопасности корпоративных компьютерных сетей.

### 1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

| Код компетенции | Формулировка компетенции | Этап формирования |
|---|---|---|
| ОПК-7 | Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты | Второй |
| **Планируемые результаты обучения**<br>Знать:<br>1) Элементы корпоративной модели информации<br>Уметь:<br>1) анализировать и оценивать угрозы информационной безопасности объектов в корпоративных компьютерных сетях<br>Владеть:<br>1) современными техническими средствами и информационными технологиями | | |
| ПК-3 | Способность администрировать подсистемы информационной безопасности объекта защиты | Второй |
| **Планируемые результаты обучения**<br>Знать:<br>1) Модели IEEE<br>Уметь:<br>1) Настраивать параметры современных программно-аппаратных межсетевых экранов<br>Владеть:<br>1) Навыками установки межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети | | |
| ПК-10 | Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности | Второй |
| **Планируемые результаты обучения**<br>Знать:<br>1) основные принципы построения защищённых компьютерных сетей и систем<br>Уметь:<br>1) Оценивать методы воздействия внутренних злоумышленников в корпоративных сетях<br>Владеть:<br>1) Навыками анализа защищенных сетей | | |
| ПСК-1 | Готовность к администрированию программно-аппаратных | Второй |

| Код компетенции | Формулировка компетенции | Этап формирования |
|---|---|---|
| | средств защиты информации в компьютерных сетях | |

**Планируемые результаты обучения**

Знать:
1) Виды политик управления доступом и информационными потоками в компьютерных системах
Уметь:
1) Настраивать правила фильтрации пакетов в компьютерных сетях
Владеть:
1) Навыками управления средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

**1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:**

- Информатика (ОПК-7)
- Базы данных (ОПК-7)
- Информационные технологии (ОПК-7)
- Защита информации в Internet (ОПК-7)
- Сети и системы передачи информации (ПК-3)
- Операционные системы (ПК-3)
- Среды и оболочки операционных систем с открытым кодом (ПК-3)
- Основы информационной безопасности (ПК-10)
- Программно-аппаратные средства защиты информации (ПСК-1)

## 2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

| Наименование и содержание учебных модулей, тем и форм контроля | Выделяемое время (часы) | | |
|---|---|---|---|
| | очное обучение | очно-заочное обучение | заочное обучение |
| **Учебный модуль 1. Аппаратные и программные средства резервного копирования данных.** | | | |
| Тема 1. Аппаратные средства резервного копирования данных. Программные средства резервного копирования. | 8 | | |
| Тема 2. Виды резервного копирования. Разработка и реализация стратегии резервного копирования. Понятие плана архивации. Выбор архивных устройств и носителей. | 8 | | |
| Тема 3. Примеры построения систем резервного копирования. Теневые копии. Технология хранения резервных копий. | 8 | | |
| Тема 4. Способы резервного копирования перед и после обновления системы. Создание ASR-копии. Алгоритмы резервного копирования. | 8 | | |
| **Текущий контроль 1 (опрос)** | 2 | | |
| **Учебный модуль 2. Восстановление БД и управление доступом БД.** | | | |
| Тема 5. Основные сведения об архитектуре БД. | 8 | | |
| Тема 6. Управление доступом БД. Программы и методы проверки подлинности. | 8 | | |
| Тема 7. Авторизация пользователей. Добавление пользователей БД. | 8 | | |
| Тема 8. Разрешения назначаемые на уровне БД. | 8 | | |
| Тема 9. Создание и управление учетными записями. Доступ к БД. | 8 | | |
| Тема 10. Информационная безопасность систем управления БД. Восстановление БД. Программы восстановления. | 8 | | |
| **Текущий контроль 2 (опрос)** | 2 | | |
| **Учебный модуль 3. Методы обеспечения защиты компьютерных сетей от несанкционированного доступа.** | | | |
| Тема 11. Проблемы несанкционированного доступа. Средства ограничения физического доступа. | 8 | | |
| Тема 12. Средства защиты от НСД по сети. | 8 | | |
| Тема 13. Современная технология и криптография защиты данных в сетях | 8 | | |

| Наименование и содержание учебных модулей, тем и форм контроля | Выделяемое время (часы) | | |
|---|---|---|---|
| | очное обучение | очно-заочное обучение | заочное обучение |
| корпоративного назначения. Сетевой монитор безопасности. | | | |
| **Текущий контроль 3 (опрос)** | 2 | | |
| **Учебный модуль 4. Специализированные средства борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.** | | | |
| Тема 14. Программы-детекторы. Программы-доктора и ревизоры. Программы-фильтры. | 8 | | |
| Тема 15. Спам. Виды спама. Способы распространения спама. Архитектура серверных систем фильтрации спама. | 8 | | |
| Тема 16. Антивирусные программы. | 8 | | |
| Тема 17. Использование антивирусной защиты при заражении сетевой инфраструктуры. | 8 | | |
| **Текущий контроль 4. (опрос)** | 2 | | |
| **Промежуточная аттестация по дисциплине (экзамен)** | **36** | | |
| **ВСЕГО:** | **180** | | |

## 3. ТЕМАТИЧЕСКИЙ ПЛАН

**3.1. Лекции**

| Номера изучаемых тем | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|
| | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| 1 | 7 | 2 | | | | |
| 2 | 7 | 2 | | | | |
| 3 | 7 | 2 | | | | |
| 4 | 7 | 2 | | | | |
| 5 | 7 | 2 | | | | |
| 6 | 7 | 2 | | | | |
| 7 | 7 | 2 | | | | |
| 8 | 7 | 2 | | | | |
| 9 | 7 | 2 | | | | |
| 10 | 7 | 2 | | | | |
| 11 | 7 | 2 | | | | |
| 12 | 7 | 2 | | | | |
| 13 | 7 | 2 | | | | |
| 14 | 7 | 2 | | | | |
| 15 | 7 | 2 | | | | |
| 16 | 7 | 2 | | | | |
| 17 | 7 | 2 | | | | |
| **ВСЕГО:** | | 34 | | | | |

**3.2. Практические и семинарские занятия**

| Номера, изучаемых тем | Наименование и форма занятий | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|---|
| | | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| 1 | Определение угроз. Анализ рисков (практикум) | 7 | 1 | | | | |
| 2 | Построение модели защиты ПК и сети от вирусов. Выбор метода защиты ПК от вирусов и от несанкционированного доступа. (практикум) | 7 | 1 | | | | |
| 3 | Установки безопасности систем на базе ОС Windows. | 7 | 1 | | | | |

| Номера, изучаемых тем | Наименование и форма занятий | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|---|
| | | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| | Установка и настройка антивирусного ПО. (практикум) | | | | | | |
| 4 | Обновление антивирусного ПО. Отключение и удаление неиспользованных учетных записей. (практикум) | 7 | 1 | | | | |
| 5 | Установка паролей для всех учетных записей пользователей. Защита сервера от вирусов. (практикум) | 7 | 1 | | | | |
| 6 | Диагностика заражения ПК вирусами. Контроль карантина. Восстановление зараженных файлов, папок. (практикум) | 7 | 1 | | | | |
| 7 | Установка и настройка межсетевого экрана. Защита корпоративных сетей от вирусов и троянских программ. (практикум) | 7 | 1 | | | | |
| 8 | Настройка пакетов межсетевого экрана. Установка и настройка аппаратных средств резервного копирования данных. (практикум) | 7 | 1 | | | | |
| 9 | Установка и настройка программных средств резервного копирования данных. Разработка и реализация стратегии резервного копирования. (практикум) | 7 | 1 | | | | |
| 10 | Резервное копирование данных. Архивирование данных. (практикум) | 7 | 1 | | | | |
| 11 | Выбор архивных устройств и носителей. Определение ограничений для резервного копирования. (практикум) | 7 | 1 | | | | |
| 12 | Теневые копии. Создание ASR-копии. (практикум) | 7 | 1 | | | | |
| 13 | Установка приемлемого окна резервного копирования данных. Установка расписания резервного копирования данных. (практикум) | 7 | 1 | | | | |
| 14 | Разработка политики хранения резервных копий. Тестирование восстановления из резервных копий. (практикум) | 7 | 1 | | | | |
| 15 | Архитектура безопасности данных. Классификация информационных систем персональных данных. (практикум) | 7 | 1 | | | | |
| 16 | Защита информации от утечки по техническим каналам. Защита информации от несанкционированного доступа. (практикум) | 7 | 1 | | | | |
| 17 | Шифрование данных и файлов. Непрерывное обеспечение безопасности данных. (практикум) | 7 | 1 | | | | |

| Номера, изучаемых тем | Наименование и форма занятий | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|---|
| | | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| | **ВСЕГО:** | | 17 | | | | |

**3.3. Лабораторные занятия**

| Номера изучаемых тем | Наименование и форма занятий | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|---|
| | | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| 1 | Организация и проведение мероприятий по защите персональных данных. Создание системы защиты персональных данных. | 7 | 1 | | | | |
| 2 | Установка программ для проверки подлинности. Выбор методов проверки подлинности. | 7 | 1 | | | | |
| 3 | Архитектура БД. Восстановление данных из резервной копии. | 7 | 1 | | | | |
| 4 | Авторизация пользователей. Добавление пользователей БД. | 7 | 1 | | | | |
| 5 | Управление доступом БД. Работа с учетными записями. Осуществление доступа к БД. | 7 | 1 | | | | |
| 6 | Работа с программами восстановления данных. Информационная безопасность систем управления БД. | 7 | 1 | | | | |
| 7 | Безопасность ресурсов и контроль доступа. Сканирование уязвимостей. | 7 | 1 | | | | |
| 8 | Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Допуск к ресурсам сервера базы данных. | 7 | 1 | | | | |
| 9 | Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. | 7 | 1 | | | | |
| 10 | Применение различных способов разграничения доступа к компьютерным ресурсам. | 7 | 1 | | | | |
| 11 | Разграничение доступа по спискам. Использование матрицы установления полномочий. | 7 | 1 | | | | |
| 12 | Автоматическое шифрование логических дисков ПК. | 7 | 1 | | | | |
| 13 | Борьба со спамом техническими средствами. Фильтрация почты. | 7 | 1 | | | | |
| 14 | Сбор адресов электронной почты. Создание черных списков. | 7 | 1 | | | | |
| 15 | Авторизация почтовых серверов. | 7 | 1 | | | | |
| 16 | Сортировка писем. | 7 | 1 | | | | |
| 17 | Использование антивирусной защиты при заражении | 7 | 1 | | | | |

| Номера изучаемых тем | Наименование и форма занятий | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|---|
| | | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| | сетевой инфраструктуры. | | | | | | |
| | **ВСЕГО:** | | **17** | | | | |

## 4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено.

## 5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

| Номера учебных модулей, по которым проводится контроль | Форма контроля знаний | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|---|
| | | Номер семестра | Кол-во | Номер семестра | Кол-во | Номер семестра | Кол-во |
| 1-4 | Опрос | 7 | 4 | | | | |

## 6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

| Виды самостоятельной работы обучающегося | Очное обучение | | Очно-заочное обучение | | Заочное обучение | |
|---|---|---|---|---|---|---|
| | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) | Номер семестра | Объем (часы) |
| Усвоение теоретического материала | 7 | 46 | | | | |
| Подготовка к практическим занятиям | 7 | 15 | | | | |
| Подготовка к лабораторным занятиям | 7 | 15 | | | | |
| Подготовка к экзамену | 7 | 36 | | | | |
| **ВСЕГО:** | | 112 | | | | |

## 7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

### 7.1. Характеристика видов и используемых инновационных форм учебных занятий

| Наименование видов учебных занятий | Используемые инновационные формы | Объем занятий в инновационных формах (часы) | | |
|---|---|---|---|---|
| | | очное обучение | очно-заочное обучение | заочное обучение |
| Лекции | проблемная лекция, разбор конкретных ситуаций, лекция-диалог | 17 | | |
| Лабораторные занятия | Проведение экспериментов при проектировании ЛВС в виртуальной среде | 7 | | |
| Практические и семинарские занятия | решения проблемных ситуаций (case-study), командное соревнование малых групп | 7 | | |
| | **ВСЕГО:** | 31 | | |

### 7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

**Перечень и параметры оценивания видов деятельности обучающегося**

| № п/п | Вид деятельности обучающегося | Весовой коэффициент значимости, % | Критерии (условия) начисления баллов |
|---|---|---|---|
| 1 | Аудиторная активность: посещение лекций и практических | 20 | • 2 балла за каждое занятие (всего 34 занятия в семестре), максимум **68** баллов<br>• 1 балл за каждый правильный ответ на вопрос |

| | | | |
|---|---|---|---|
| | (семинарских) занятий, прохождение промежуточного опроса | | опроса **текущего контроля** (всего 8 вопросов в опросе, 4 опроса в семестр), максимум **32** балла |
| 2 | Выполнение и защита лабораторных работ | 40 | • 3 баллов за каждую работу, всего 17 работ, максимум 51 балл<br>• Качество защиты (полнота ответов на вопросы, владение специальной терминологией, затраченное на ответы время) – максимум **45** баллов. |
| 3 | Сдача экзамена | 40 | • Ответ на теоретический вопрос (полнота, владение терминологией, затраченное время) – максимум **40** баллов;<br>• Решение практической задачи – до 60 баллов |
| | **Итого (%):** | 100 | |

**Перевод балльной шкалы в традиционную систему оценивания**

| Баллы | Оценка по нормативной шкале | |
|---|---|---|
| 86 - 100 | 5 (отлично) | Зачтено |
| 75 – 85 | 4 (хорошо) | |
| 61 – 74 | | |
| 51 - 60 | 3 (удовлетворительно) | |
| 40 – 50 | | |
| 17 – 39 | 2 (неудовлетворительно) | Не зачтено |
| 1 – 16 | | |
| 0 | | |

## 8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**8.1. Учебная литература**

а) основная учебная литература

1. Оливер Ибе Компьютерные сети и службы удаленного доступа [Электронный ресурс]: учебное пособие/ Ибе Оливер— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 333 c.— Режим доступа: http://www.iprbookshop.ru/63577.html.— ЭБС «IPRbooks»
2. Ковган Н.М. Компьютерные сети [Электронный ресурс]: учебное пособие/ Н.М. Ковган— Электрон. текстовые данные.— Минск: Республиканский институт профессионального образования (РИПО), 2014.— 180 c.— Режим доступа: http://www.iprbookshop.ru/67638.html.— ЭБС «IPRbooks»
3. Шелухин О.И. Системы обнаружения вторжений в компьютерные сети [Электронный ресурс]: учебное пособие/ О.И. Шелухин, А.Н. Руднев, А.В. Савелов— Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2013.— 88 c.— Режим доступа: http://www.iprbookshop.ru/63360.html.— ЭБС «IPRbooks»

б) дополнительная учебная литература

1. Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2016.— 42 c.— Режим доступа: http://www.iprbookshop.ru/61546.html.— ЭБС «IPRbooks»
2. Учебно-методическое пособие по выполнению курсового проекта по дисциплине «Методы и средства защиты информации в компьютерных сетях» [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2015.— 35 c.— Режим доступа: http://www.iprbookshop.ru/61741.html.— ЭБС «IPRbooks»
3. Лабораторный практикум по дисциплине Методы и средства защиты информации в компьютерных сетях [Электронный ресурс]/ — Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2015.— 58 c.— Режим доступа: http://www.iprbookshop.ru/61742.html.— ЭБС «IPRbooks»

**8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

1. Сети и системы передачи информации [Электронный ресурс]: методические указания / Сост. Зурахов В. С., Макаров А. Г. — СПб.: СПГУТД, 2014.— 19 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1814, по паролю.
2. Бусыгин К. Н. Корпоративные компьютерные сети [Электронный ресурс]: учебное пособие / Бусыгин К. Н. — СПб.: СПГУТД, 2014.— 91 с.— Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1865, по паролю.
3. Спицкий, С. В. Эффективная аудиторная и самостоятельная работа обучающихся: методические указания / С. В. Спицкий. – СПб.: СПбГУПТД, 2015. – Режим доступа: http://publish.sutd.ru/tp_get_file.php?id=2015811, по паролю.
4. Караулова, И. Б. Организация самостоятельной работы обучающихся / И. Б. Караулова, Г. И. Мелешкова, Г. А. Новоселов. – СПб.: СПГУТД, 2014. – 26 с. – Режим доступа http://publish.sutd.ru/tp_get_file.php?id=2014550, по паролю

**8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины**

1. http://www.iprbookshop.ru
2. http://publish.sutd.ru/

**8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем** *(при необходимости)*

1. Microsoft Office Standart 2016 Russian Open No Level Academic)
2. Microsoft Windows 10 Home Russian Open No Level Academic Legalization Get Genuine (GGK) + Microsoft Windows 10 Professional (Pro – профессиональная) Russian Upgrade Open No Level Academic

**8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

1. Стандартно оборудованная аудитория;
2. Персональный компьютер, оснащенный сетевым адаптером и доступом в Internet;
3. Проектор.

**8.6. Иные сведения и (или) материалы**

Не предусмотрены

## 9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

| Виды учебных занятий и самостоятельная работа обучающихся | Организация деятельности обучающегося |
|---|---|
| Лекции | • проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины;<br>• конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины.<br>• Проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь;<br>• работа с теоретическим материалом (конспектирование источников): найти ответ на вопросы в рекомендуемой литературе. |
| Практические занятия | • подготовка ответов к контрольным вопросам, опросам;<br>• решение задач по алгоритму, решение кейсов |
| Лабораторные занятия | Лабораторные занятия способствуют развитию практических навыков владения изучаемыми методами, оборудованием, технологиями и др. в процессе взаимодействия со специально разработанными образцами реально действующего оборудования, предполагают проведение учебного эксперимента (самостоятельно либо под руководством преподавателя); |
| Самостоятельная работа | При подготовке к экзамену необходимо ознакомиться с демонстрационным вариантом задания (перечнем вопросов, пр.), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя, подготовить презентацию материалов. |

## 10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

# ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

## 10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

### 10.1.1. Показатели оценивания компетенций на этапах их формирования

| Код компетенции / этап освоения | Показатели оценивания компетенций | Наименование оценочного средства | Представление оценочного средства в фонде |
|---|---|---|---|
| ОПК-7/второй | Дает определения основных понятий корпорации, ресурсов, системы | Вопросы для устного собеседования | Перечень вопросов для устного собеседования (9вопросов) |
| | Распознает виды и формы корпоративной информации, подверженной угрозам | Практическое задание | Перечень практических заданий (8 заданий) |
| | Выбирает средства защиты корпоративных сетей современного предприятия и аргументирует свой выбор | | |
| ПК-3/второй | Раскрывает основные стандарты, касающиеся локальных вычислительных сетей | Вопросы для устного собеседования | Перечень вопросов для устного собеседования (9 вопросов) |
| | Исследует схемы подключения межсетевых экранов для обеспечения защиты информации в корпоративных сетях | Практическое задание | Перечень практических заданий (8 заданий) |
| | Приводит технические и экономические преимущества внедрения технологий VPN и МЭ в корпоративные сети | | |
| ПК-10/второй | Перечисляет ключевые средства обеспечения информационной безопасности предприятия или организации, используемые для построения защищённых компьютерных сетей и систем, и принципы их функционирования | Вопросы для устного собеседования | Перечень вопросов для устного собеседования (9 вопросов) |
| | Различает пассивные и активные методы воздействия нарушителя на корпоративную сеть предприятия | Практическое задание | Перечень практических заданий (8 заданий) |
| | Дает рекомендации по усилению защиты корпоративных сетей от внутренних и внешних нарушителей | | |
| ПСК-1/Второй | Формулирует основные понятия и определения, используемые при описании моделей безопасности компьютерных систем | Вопросы для устного собеседования | Перечень вопросов для устного собеседования (9 вопросов) |
| | Задает правила фильтрации данных в соответствии с политикой безопасности | Практическое задание | Перечень практических заданий (8 заданий) |
| | Приводит политика работы МЭ при обеспечении безопасности | | |

### 10.1.2. Описание шкал и критериев оценивания сформированности компетенций

**Критерии оценивания сформированности компетенций**

| Баллы | Оценка по традиционной шкале | Критерии оценивания сформированности компетенций |
|---|---|---|
| | | Устное собеседование |
| 86 - 100 | 5 (отлично) | *Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.* ***Учитываются баллы, накопленные в течение семестра.*** |
| 75 – 85 | 4 (хорошо) | *Ответ полный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный.* ***Учитываются баллы, накопленные в течение семестра***. |
| 61 – 74 | | *Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.* ***Учитываются баллы, накопленные в течение семестра.*** |
| 51 - 60 | 3 | *Ответ воспроизводит в основном только лекционные материалы, без* |

| | | |
|---|---|---|
| | (удовлетво-рительно) | *самостоятельной работы с рекомендованной литературой. Демонстрирует понимание предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам.* ***Учитываются баллы, накопленные в течение семестра.*** |
| 40 – 50 | | *Ответ неполный, основанный только на лекционных материалах. При понимании сущности предмета в целом – существенные ошибки или пробелы в знаниях сразу по нескольким темам, незнание (путаница) важных терминов.* ***Учитываются баллы, накопленные в течение семестра.*** |
| 17 – 39 | 2 (неудовлетво-рительно) | *Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки.* ***Не учитываются баллы, накопленные в течение семестра.*** |
| 1 – 16 | | *Непонимание заданного вопроса. Неспособность сформулировать хотя бы отдельные концепции дисциплины.* ***Не учитываются баллы, накопленные в течение семестра.*** |
| 0 | | *Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).* ***Не учитываются баллы, накопленные в течение семестра.*** |

**10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций**

**10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций**

| № п/п | Формулировка вопросов | № темы |
|---|---|---|
| 1 | Резервное копирование данных. Краткий список программ и их описание. | 1 |
| 2 | Меры по защите компьютерных сетей от несанкционированного доступа. | 1 |
| 3 | Специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами. Краткий список программ и описание. | 2 |
| 4 | Процедуры по восстановлению и проверке корректности восстановленных данных. | 2 |
| 5 | Управления правами доступа пользователей. | 3 |
| 6 | Топология вычислительной сети. Виды топологий. Топология общая шина. | 3 |
| 7 | Сетевые архитектуры Arcnet, Appletalk, SNA, DecNet. | 4 |
| 8 | Сетевые службы и сетевые сервисы. | 4 |
| 9 | Функции администратора сети. | 5 |
| 10 | Обзор служб каталогов. | 5 |
| 11 | Метод доступа CSMA/CD | 6 |
| 12 | Метод доступа TPMA. | 7 |
| 13 | Метод доступа TDMA. | 8 |
| 14 | Метод доступа FDMA. | 8 |
| 15 | Семиуровневая модель OSI. Назначение. Взаимодействие уровней модели OSI. | 8 |
| 16 | Спецификации стандартов 802.1 – 802.7. | 9 |
| 17 | Спецификации стандартов 802.8 - 802.12. | 9 |
| 18 | Спецификации стандартов 802.14- 802.22. | 9 |
| 19 | Понятия протоколов и стеков протоколов. Сетевые протоколы. Транспортные протоколы. Прикладные протоколы. | 10 |
| 20 | Архитектура стека протоколов Microsoft TCP/IP. | 10 |
| 21 | Стек TCP/IP: уровень Приложения, уровень транспорта. | 11 |
| 22 | Стек TCP/IP: межсетевой уровень, уровень сетевого интерфейса. | 11 |
| 23 | Типы адресаций в сетях. Символьная адресация. Протоколы сопоставления адреса ARP и RARP. | 12 |
| 24 | Структура IPv4. Классы IP-адресов. | 12 |
| 25 | Виды основных сетевых атак. | 13 |
| 26 | Понятие шифрования. Классические алгоритмы шифрования данных. | 13 |
| 27 | Стандартные методы шифрования и криптографические системы. | 13 |
| 28 | Общие основы решения практических задач по восстановлению БД и проверке корректности восстановленных данных. | 14 |
| 29 | Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети. | 14 |
| 30 | Модель ISO для управления сетевым трафиком. | |
| 31 | Телекоммуникационные системы: типы сетей, линий и каналов связи, аналоговое и цифровое кодирование цифровых данных, синхронизация элементов ТКС. | 15 |
| 32 | Характеристика ЛВС: типы, основные характеристики, сетевое оборудование (состав назначение), протоколы управления обменом данных, программное обеспечение (структура и функции). | 15 |

| | | |
|---|---|---|
| 33 | Криптографические методы защиты информации: классификация методов, сущность методов шифрования с симметричным ключом и с открытым ключом, стандарты 16шифрования, перспективы использования криптозащиты информации в ККС. | 15 |
| 34 | Криптографические системы с закрытым ключом: принципы построения, особенности применения и реализации, примеры криптосистем. | 16 |
| 35 | Криптографические системы с открытым ключом: математическая основа, алгоритм работы. Сравнение криптосистем с открытым ключом. | 17 |
| 36 | Этапы создания системы безопасности объекта информатизации. | 17 |

**Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций**

Не предусмотрено

**10.2.2. Перечень тем докладов** *(рефератов, эссе, пр.)***, разработанных в соответствии с установленными этапами формирования компетенций**

Не предусмотрено

**Вариант типовых заданий (задач, кейсов), разработанных в соответствии с установленными этапами формирования компетенций**

| № п/п | Условия типовых задач (задач, кейсов) | Ответ |
|---|---|---|
| 1 | В сетях данные на пути до узла назначения обычно проходят через несколько транзитных промежуточных этапов обработки, то в качестве критерия эффективности может рассматриваться пропускная способность отдельного промежуточного элемента сети: | отдельного канала, сегмента или коммуникационного устройства. |
| 2 | Отказоустойчивость сети (fault tolerance). | В сетях под отказоустойчивостью понимается способность системы скрыть от пользователя отказ отдельных ее элементов. В отказоустойчивой системе отказ одного из ее элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову. В целом система будет продолжать выполнять свои функции; |
| 3 | Опишите основные виды технологий и устройств защиты от взлома, НСД или атаки на корпоративную сеть | - Межсетевые экраны UTM/Firewall;<br>- Системы предотвращения вторжений IPS/IDS;<br>- Системы защиты от распределённых атак DDoS;<br>- Контроль доступа к сети NAC;<br>- Виртуальные частные сети VPN;<br>- Аутентификации и авторизации пользователей AAA;<br>- Системы управления доступом IDM |

**10.3. Методические материалы,**
**определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций**

**10.3.1. Условия допуска обучающегося к сдаче экзамена и порядок ликвидации академической задолженности**

К экзамену допускается студент, выполнивший в течение семестра все виды учебных заданий по соответствующему предмету (практические и лабораторные работы, курсовая работа). В случае пропуска учебных занятий по уважительной причине (подтвержденной документально) студент обязан отработать пропущенные занятия.

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся

**10.3.2. Форма проведения промежуточной аттестации по дисциплине**

устная [X] письменная [ ] компьютерное тестирование [ ] иная* [ ]

**В случае указания формы «Иная» требуется дать подробное пояснение*

**10.3.3. Особенности проведения** *(экзамена, зачета и / или защиты курсовой работы)*

Обучающийся тянет билет, в котором содержится теоретический вопрос и практическое задание. После этого готовится в течении как минимум 20 минут с использованием конспекта лекций и других материалов. Обучающийся в устной форме доводит до преподавателя ответ на вопрос, при необходимости прямо во время ответа составляет необходимые схемы или диаграммы.

После ответа на теоретический вопрос обучающийся приступает к решению практического задания, гарантированно на решение задачи времени дается 30 минут, решение формулируется с использованием конспекта лекций и иных материалов, при правильном решении задачи преподаватель задает вопросы по методам или технологиям решения.