Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 04.10.2023 10:40:46
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## «Безопасность сетей электронных вычислительных машин»

Направление подготовки
**09.03.01 Информатика и вычислительная техника**

Профиль
**«Кибербезопасность автоматизированных систем»**

Квалификация
**Бакалавр**

Формы обучения
**очная**

Москва, 2023 г.

**Разработчик(и):**

степень, звание, должность / А.А. Набебин /

**Согласовано:**
И.о. заведующего кафедрой «Информационная безопасность»,



/А.Ю. Гневшев/

Руководитель образовательной программы,



/А.Ю. Гневшев/

**Содержание**


| | | |
|---|---|---|
| 1 | Цели, задачи и планируемые результаты обучения по дисциплине | 4 |
| 2 | Место дисциплины в структуре образовательной программы | 5 |
| 3 | Структура и содержание дисциплины | 5 |
| 3.1 | Виды учебной работы и трудоемкость | 5 |
| 3.2 | Тематический план изучения дисциплины | 6 |
| 3.3 | Содержание дисциплины | 9 |
| 4 | Учебно-методическое и информационное обеспечение | 13 |
| 4.1 | Нормативные документы и ГОСТы | 13 |
| 4.2 | Основная литература | 14 |
| 4.3 | Дополнительная литература | 14 |
| 5 | Материально-техническое обеспечение | 15 |
| 6 | Методические рекомендации | 15 |
| 6.1 | Методические рекомендации для преподавателя по организации обучения | 15 |
| 6.2 | Методические указания для обучающихся по освоению дисциплины | 15 |
| 7 | Фонд оценочных средств | 16 |
| 7.1 | Методы контроля и оценивания результатов обучения | 16 |
| 7.2 | Шкала и критерии оценивания результатов обучения | 16 |
| 7.3 | Оценочные средства | 19 |

## 1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Безопасность сетей электронных вычислительных машин» следует отнести:

- теоретическая и практическая подготовка специалистов в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ.

К **основным задачам** освоения дисциплины «Безопасность сетей электронных вычислительных машин» следует отнести:

- овладение механизмами построения систем безопасности сетей ЭВМ.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

| **Код компетенции** | **Перечень планируемых результатов обучения по дисциплине** |
|---|---|
| ПК-1. Способен осуществлять администрирование процесса контроля производительности сетевых устройств и программного обеспечения, проводить регламентированные работы на сетевых устройствах и программном обеспечение инфокоммуникационной системы | ИПК-1.1 Знает: Устройство и принцип работы сетевых устройств<br>Принципы функционирования и архитектуру сетевых аппаратных средств<br>Технологии в сетевом администрировании<br>Модели управления сетью<br>ИПК-1.2. Умеет:<br>Пользоваться нормативно-технической документацией в области ИКТ<br>Использовать современные методы контроля и осуществлять администрирование процесса контроля производительности сетевых устройств и программного обеспечения, проводить регламентированные работы на сетевых устройствах и программном обеспечение инфокоммуникационной системы<br>ИПК-1.3. Владеет: Оценкой производительности критических приложений, планированием требуемой производительности администрируемой сети, способами установки, анализа и контроля кабельных и сетевых анализаторов для контроля изменения номиналов сетевых устройств и ПО администрируемой сети в целом и отдельных подсистем ИКС |

| | |
|---|---|
| ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения | ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети;<br>Классификация ОС согласно классам безопасности;<br>Средства защиты от несанкционированного доступа ОС и СУБД;<br>ИПК-2.2. Уметь: Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа<br>Настраивать параметры и сегментировать элементы администрируемой сети<br>ИПК-2.3. Владеет: Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа<br>Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа<br>Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)<br>Документирование настроек средств обеспечения безопасности удаленного |

## 2 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность сетей электронных вычислительных машин» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1.1) основной образовательной программы (Б1.1.24).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационно-коммуникационных технологий», «Основы веб-технологий», «Основы сетевых технологий», «Системы управления базами данных».

## 3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 4 семестре.

Структура и содержание дисциплины «Безопасность сетей электронных вычислительных машин» по срокам и видам работы отражены в приложении.

### 3.1 Виды учебной работы и трудоемкость (по очной форме обучения)

| № п/п | Вид учебной работы | Количество часов | Семестры | |
|---|---|---|---|---|
| | | | 4 | |
| 1 | **Аудиторные занятия** | **72** | 72 | |
| | В том числе: | | | |

| | | | | |
|---|---|---|---|---|
| 1.1 | Лекции | | | |
| 1.2 | Семинарские/практические занятия | | | |
| 1.3 | Лабораторные занятия | 72 | 72 | |
| **2** | **Самостоятельная работа** | 72 | 72 | |
| | В том числе: | | | |
| 2.1 | … | | | |
| **3** | **Промежуточная аттестация** | | | |
| | Экзамен | | | |
| | Итого: | **144** | 144 | |

### 3.2 Содержание дисциплины

**Раздел 1.**
Основы современных сетевых технологий.
**Раздел 2.**
Схема взаимодействия с Web-сервером. Распределенная обработка информации на основе мигрирующих программ. Доступ к реляционным базам данных.
**Раздел 3.**
Управление информацией о ресурсах и пользователях сети. Электронная почта и система новостей.
**Раздел 4.**
Безопасное масштабирование компьютерных сетей. Использование повторителей. Сегментация сети с помощью мостов.
**Раздел 5.**
Применение коммутаторов. Построение маршрутизированных сетей. Алгоритмы и протоколы маршрутизации.
**Раздел 6.**
Способы нападений на компьютерные сети.
**Раздел 7.**
Способы несанкционированного доступа к информации в компьютерных сетях. Нападения на политику безопасности и процедуры административного доступа.
**Раздел 8.**
Нападения на постоянные компоненты системы защиты. Нападения на сменные элементы системы защиты.
**Раздел 9.**
Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей.
**Раздел 10.**
Защита от несанкционированного межсетевого доступа.
**Раздел 11.**
Функции межсетевого экранирования на различных уровнях модели OSI. Фильтрация трафика. Выполнение функций посредничества. Критерии оценки и классификация межсетевых экранов. Обзор современных систем FireWall.
**Раздел 12.**
Построение защищенных виртуальных сетей
**Раздел 13.**
Введение в защищенные виртуальные сети. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне.

**Раздел 14.**
Построение защищенных виртуальных сетей на сеансовом уровне. Распределение криптографических ключей и согласование параметров защищенных туннелей.
**Раздел 15.**
Безопасность удаленного доступа к локальной сети. Обзор средств построения защищенных виртуальных сетей.

# 4 Учебно-методическое и информационное обеспечение

## 4.1 Нормативные документы и ГОСТы

1. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) от 18.12.2006 № 230-ФЗ
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).
3. ГОСТ Р ИСО/МЭК 27033-5-2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС).

## 4.2 Основная литература

1.Воробьев, С. П. Компьютерные сети и сетевая безопасность : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. — Новочеркасск : ЮРГПУ (НПИ), 2022. — 216 с. — ISBN 978-5-9997-0805-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292247. — Режим доступа: для авториз. пользователей.
2. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889. — Режим доступа: для авториз. пользователей.

## 4.3 Дополнительная литература

1.Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009. — Режим доступа: для авториз. пользователей.

## 4.4 Электронные образовательные ресурсы

Электронный образовательный ресурс разрабатывается

## 4.5 Лицензионное и свободно распространяемое программное обеспечение

1. Веб-браузер Chrome.
2. Microsoft Office.
3. Cisco Packet Tracer.
4. Wireshark.
5. Cisco Network Academy.
6. Виртуальная машина.

### 4.6 Современные профессиональные базы данных и информационные справочные системы

1. Федеральная государственная информационная система - Национальная электронная библиотека (НЭБ) https://нэб.рф
2.

## 5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

## 6 Методические рекомендации

### 6.1 Методические рекомендации для преподавателя по организации обучения

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **09.03.01 «Информатика и вычислительная техника».**

### 6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

## 7 Фонд оценочных средств

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- выполнение лабораторных работ;
- экзамен.

### 7.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

7.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

| Код компетенции | В результате освоения образовательной программы обучающийся должен обладать |
|---|---|
| ПК-1. | Способен осуществлять администрирование процесса контроля производительности сетевых устройств и программного обеспечения, проводить регламентированные работы на сетевых устройствах и программном обеспечение инфокоммуникационной системы |
| ПК-2. | Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения |

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

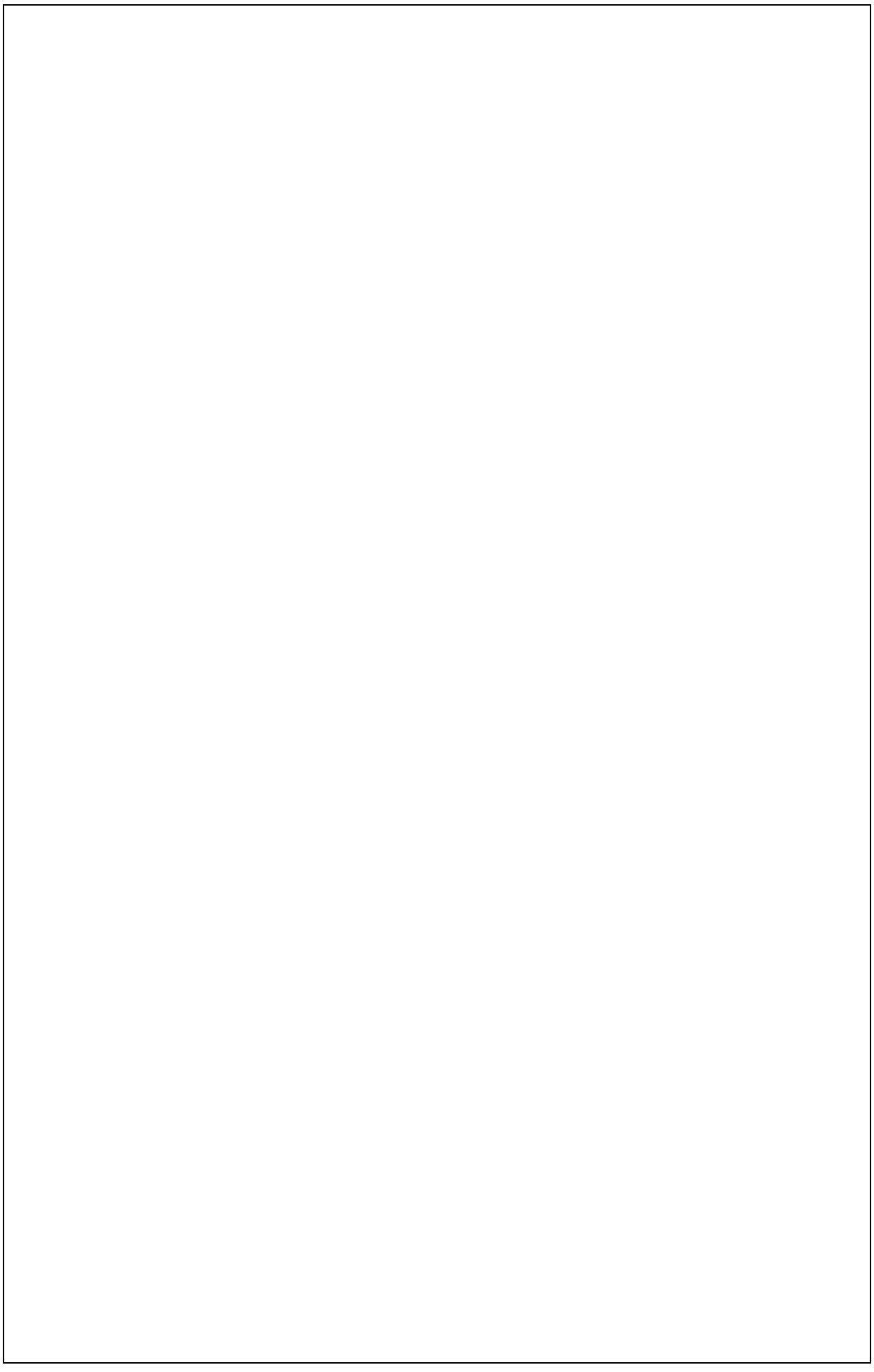
### 7.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

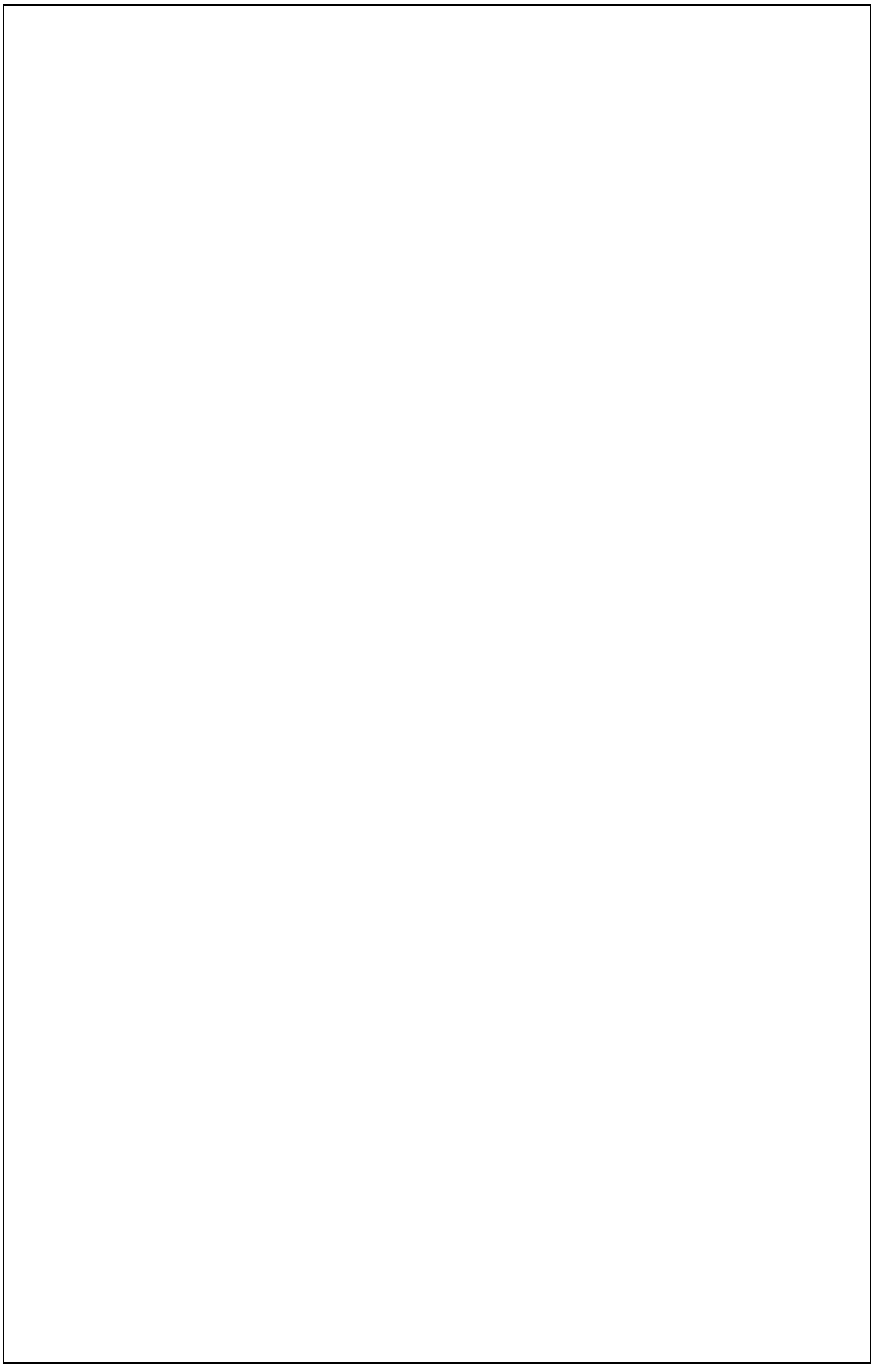
| Показатель | Критерии оценивания | | | |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| ПК-1. Способен осуществлять администрирование процесса контроля производительности сетевых устройств и программного обеспечения, проводить регламентированные работы на сетевых устройствах и программном обеспечение инфокоммуникационной системы | | | | |

К-1. Способен осуществлят

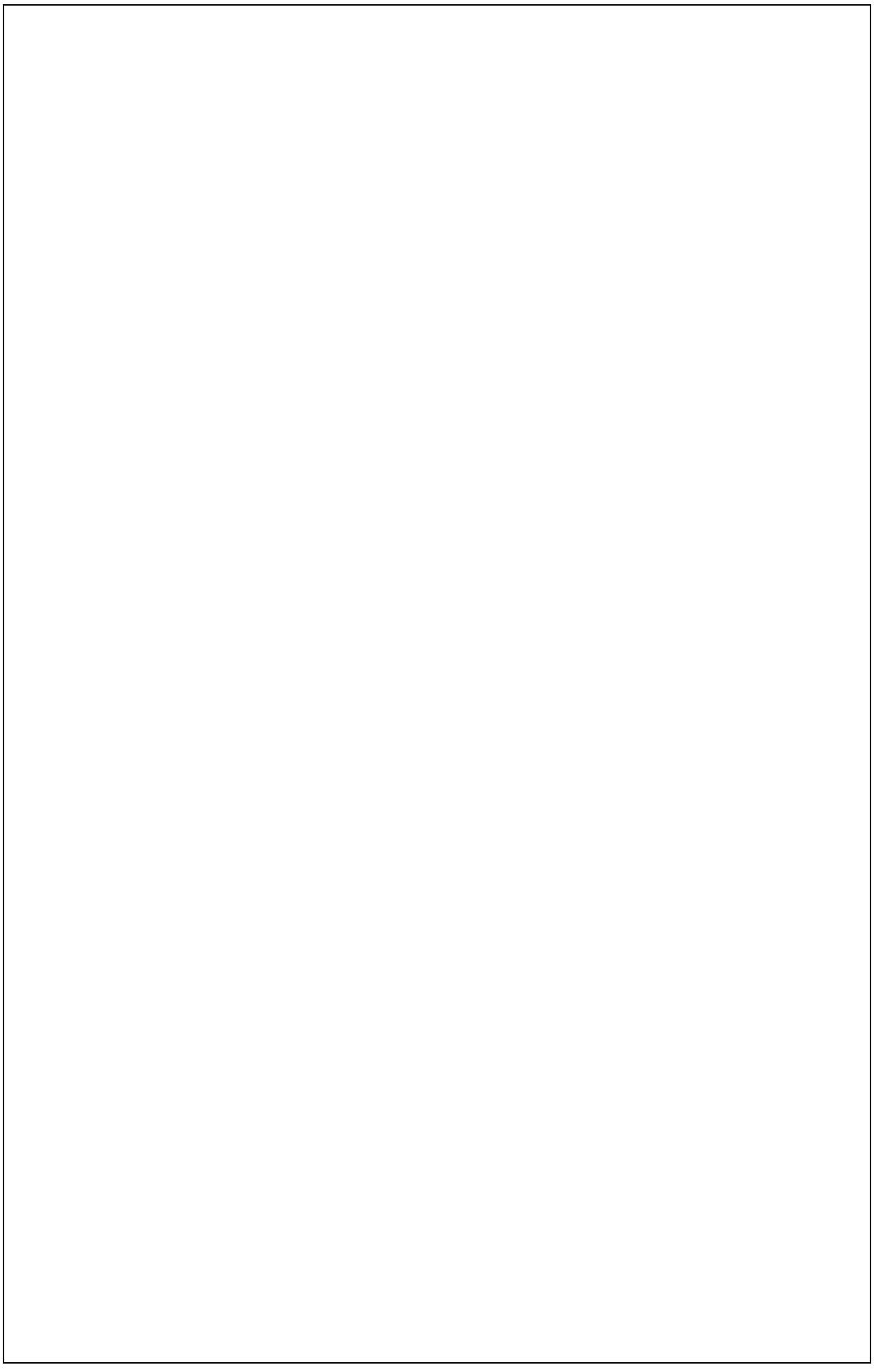
ьадминистрированиепроцессаконтролляпроизводите



льностисетевыхустройствипрограммногообеспечен



ия, проводить регламентированные работы на сетевых



устройствах программном обеспечении информационно

| | | | | |
|---|---|---|---|---|
| | | | | |
| ИПК-1.1 Знает: Устройство и принцип работы сетевых устройств Принципы функционирования и архитектуру сетевых аппаратных средств Технологии в сетевом администрировании и Модели управления сетью ИПК-1.2. Умеет: Пользоваться нормативно-технической документацией в области ИКТ Использовать современные методы контроля и осуществлять администрирование процесса контроля производительности сетевых устройств и | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). | Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями. |

кационной системы

| | | | | |
|---|---|---|---|---|
| программного обеспечения, проводить регламентированные работы на сетевых устройствах и программном обеспечение инфокоммуникационной системы<br>ИПК-1.3. Владеет: Оценкой производительности критических приложений, планированием требуемой производительности администрируемой сети, способами установки, анализа и контроля кабельных и сетевых анализаторов для контроля изменения номиналов сетевых устройств и ПО администрируемой сети в целом и отдельных подсистем ИКС | | | | |
| ПК-2. Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения | | | | |
| ИПК-2.1. Знать: Общие принципы функционирования и архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины | Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. | Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. | Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. |

| | | | | |
|---|---|---|---|---|
| Классификация ОС согласно классам безопасности;<br>Средства защиты от несанкционированного доступа ОС и СУБД;<br>ИПК-2.2. Уметь:<br>Применять аппаратные и программные средства защиты сетевых устройств от несанкционированного доступа<br>Настраивать параметры и сегментировать элементы администрируемой сети<br>ИПК-2.3. Владеет:<br>Планированием защиты и оценкой безопасности и защиты приложений и ОС от несанкционированного доступа<br>Установкой специализированных программных и аппаратных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа<br>Настройка средств обеспечения безопасности удаленного доступа (операционной системы и | знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). | 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации. | 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях. | 3). Свободно оперирует приобретенными знаниями. |

| | | | | |
|---|---|---|---|---|
| специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного | | | | |

Шкалы оценивания результатов промежуточной аттестации и их описание:

***Форма промежуточной аттестации: экзамен.***

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

| **Шкала оценивания** | **Описание** |
|---|---|
| Отлично | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| Хорошо | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. |
| Удовлетворительно | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. |
| Неудовлетворительно | Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации. |

**Фонды оценочных средствпредставлены в приложении к рабочей программе.**

Приложение.

**Структура и содержание дисциплины «Безопасность сетей электронных вычислительных машин»**
**по направлению подготовки**
**09.03.01 «Информатика и вычислительная техника»**
**(бакалавр)**

| n/n | Раздел | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах | | | | | Виды самостоятельной работы студентов | | | | | Формы аттестации | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Л | П/С | Лаб | СРС | КСР | К.Р. | К.П. | ДЗ | Реферат | К/р | Э | З |
| | **3 семестр** | | | | | | | | | | | | | | |
| 1 | Основы современных сетевых технологий. | 3 | 1 | | | 5 | 5 | | | | | | | | |
| 2 | Схема взаимодействия с Web-сервером. Распределенная обработка информации на основе мигрирующих программ. Доступ к реляционным базам данных. | | 2 | | | 5 | 5 | | | | | | | | |
| 3 | Управление информацией о ресурсах и пользователях сети. Электронная почта и система новостей. | | 3 | | | 5 | 5 | | | | | | | | |
| 4 | Безопасное масштабирование компьютерных сетей. Использование повторителей. Сегментация сети с помощью мостов. | | 4 | | | 5 | 5 | | | | | | | | |
| 5 | Применение коммутаторов. Построение маршрутизированных сетей. | | 5 | | | 5 | 5 | | | | | | | | |

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Алгоритмы и протоколы маршрутизации. | | | | | | | | | | | | | | | | |
| 6 | Способы нападений на компьютерные сети. | | 6 | | | 5 | 5 | | | | | | | | | | |
| 7 | Способы несанкционированного доступа к информации в компьютерных сетях. Нападения на политику безопасности и процедуры административного доступа. | | 7 | | | 5 | 5 | | | | | | | | | | |
| 8 | Нападения на постоянные компоненты системы защиты. Нападения на сменные элементы системы защиты. | | 8 | | | 5 | 5 | | | | | | | | | | |
| 9 | Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей. | | 9 | | | 5 | 5 | | | | | | | | | | |
| 10 | Защита от несанкционированного межсетевого доступа. | | 10 | | | 5 | 5 | | | | | | | | | | |
| 11 | Функции межсетевого экранирования на различных уровнях модели OSI. Фильтрация трафика. Выполнение функций посредничества. Критерии оценки и классификация межсетевых экранов. Обзор современных систем FireWall. | | 11-13 | | | 5 | 5 | | | | | | | | | | |
| 12 | Построение защищенных виртуальных сетей | | 14 | | | 5 | 5 | | | | | | | | | | |
| 13 | Введение в защищенные виртуальные сети. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне. | | 15 | | | 5 | 5 | | | | | | | | | | |
| 14 | Построение защищенных виртуальных сетей на сеансовом уровне. | | 16-17 | | | 5 | 5 | | | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Распределение криптографических ключей и согласование параметров защищенных туннелей. | | | | | | | | | | | | | | |
| 15 | Безопасность удаленного доступа к локальной сети. Обзор средств построения защищенных виртуальных сетей. | | 18 | | | 2 | 2 | | | | | | | | |
| | ***Форма аттестации*** | 3 | 19-21 | | | | | | | . | | | | Э | |
| | Всего часов по дисциплине во четвертом семестре | | | | | 72 | 72 | | | | | | | | |
| | **Всего часов по дисциплине** | | | | | 72 | 72 | | | | | | | | |

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Направление подготовки: 09.03.01 «Информатика и вычислительная техника»

ОП (профиль): «Кибербезопасность автоматизированных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая.

Кафедра: «Информационная безопасность»

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

# ПО ДИСЦИПЛИНЕ

## «Безопасность сетей электронных вычислительных машин»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

**Составители: ст. преп. Гневшев А.Ю.**

Москва, 2023 год

Таблица 1

**ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ**

| **Безопасность сетей электронных вычислительных машин** | | | | | |
|---|---|---|---|---|---|
| ФГОС ВО **09.03.01 «Информатика и вычислительная техника»** | | | | | |
| В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**: | | | | | |
| **КОМПЕТЕНЦИИ** | | **Перечень компонентов** | **Технология формирования компетенций** | **Форма оценоч-ного средств** | **Степени уровней освоения компетенций** |
| **ИН-ДЕКС** | **ФОРМУЛИРОВКА** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| ОПК-1.2. | Способен администрировать средства защиты информации в компьютерных системах и сетях | **знать:**<br>принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;<br>основные протоколы сетей ЭВМ;<br>эталонную модель взаимодействия открытых систем;<br>основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ;<br>последовательность и содержание этапов построения компьютерных сетей;<br><br>**уметь:**<br>проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;<br>проводить мониторинг угроз безопасности компьютерных сетей;<br>эффективно использовать различные методы и средства защиты информации для компьютерных сетей;<br><br>**владеть:**<br>способностью администрировать систему информационной безопасности;<br>способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы. | самостоятельная работа, лабораторная работа | экзамен | Базовый уровень:<br>демонстрирует полное соответствие следующих знаний: основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ<br>Повышенный уровень:<br>демонстрирует полное соответствие следующих знаний: основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ, свободно оперирует приобретенными знаниями. |

Приложение 2
к рабочей программе

**Оценочные средства для промежуточной аттестации**

**Список вопросов для экзамена по дисциплине**

1. Виды сетевых атак и вредоносных программ, механизм реализации и сетевая уязвимость.
2. Классификации способов несанкционированного доступа к сетевой информации.
3. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
4. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI (службы безопасности и механизмы их реализации).
5. Этапы построения системы информационной безопасности.
6. Способы несанкционированного доступа к информации в компьютерных сетях.
7. Нападения на политику безопасности и процедуры административного доступа.
8. Нападения на постоянные компоненты системы защиты.
9. Нападения на сменные элементы системы защиты.
10. Нападения на протоколы информационного взаимодействия.
11. Нападения на функциональные элементы компьютерных сетей.
12. Функции межсетевого экранирования на различных уровнях модели OSI.
13. Фильтрация трафика.
14. Функции посредничества.
15. Критерии оценки и классификация межсетевых экранов.
16. Особенности работы межсетевых экранов экспертного уровня.
17. Установка, конфигурирование и настройка систем защиты FireWall.
18. Защита информации в процессе передачи по сети (*технология VPN*).
19. Туннелирование на канальном уровне.
20. Защита виртуальных каналов на сетевом уровне.
21. Построение защищенных виртуальных сетей на сеансовом уровне.
22. Виды, распределение криптографических ключей и согласование параметров защищенных туннелей.
23. Безопасность удаленного доступа к локальной сети.
24. Защита информации от несанкционированного доступа (*межсетевые экраны*).
25. Требования к ОС компьютера, на который устанавливается брэндмауэр.
26. Какие элементы внутренней политики безопасности сети предприятия позволяет организовать использование МЭ, и каким образом?
27. Способы организации защищенных виртуальных каналов.
28. Варианты технической реализации VPN-сетей.
29. Защита внутрисетевого трафика.
30. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.
31. Межсетевые экраны.
32. Задачи межсетевых экранов в обеспечении сетевой безопасности.
33. Классификация межсетевых экранов.
34. Построение правил фильтрации.
35. Требования к межсетевым экранам.
36. Шлюзы уровня приложений.
37. Экранирующий маршрутизатор (*пакетный фильтр*).
38. Экранирующий транспорт (*шлюз сеансового уровня*).
39. Комплексные межсетевые экраны.
40. Реализация сетевой политики безопасности с использованием.
41. Методы обхода межсетевых экранов
42. Основные возможности и схемы развертывания межсетевых экранов.
43. Достоинства и недостатки межсетевых экранов.

44. Способы изоляции потоков информации в сети.