МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета информационных технологий
/Д. Г. Демидов/
"30" августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность сетей электронных вычислительных машин»
Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Безопасность открытых информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Форма обучения
Очная
Год приема - 2021

Москва 2021 г.

1. Цели освоения дисциплины

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.

2. Место дисциплины в структуре ООП

Дисциплина «Безопасность сетей электронных вычислительных машин» относится к числу профессиональных учебных дисциплин базовой части цикла (Б.1) основной образовательной программы (Б.1.26).

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

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

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

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК—12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	**знать:** принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; основные протоколы сетей ЭВМ; эталонную модель взаимодействия открытых систем; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; последовательность и содержание этапов построения компьютерных сетей; **уметь:** проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; проводить мониторинг угроз безопасности компьютерных сетей; эффективно использовать различные методы и средства защиты информации для компьютерных

		сетей; **владеть:** способностью администрировать систему информационной безопасности; способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы.

4. 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.

5. Образовательные технологии

Методика преподавания дисциплины «Безопасность сетей электронных вычислительных машин» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы.

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к аттестации.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

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

- выполнение лабораторных работ;
- экзамен.

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

6.1.1. 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
ОПК—12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

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.

6.1.2. 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 (модулю):

ОПК—12 Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ЗНАТЬ	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	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.

		переносе на новые ситуации.		
УМЕТЬ	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
ВЛАДЕТЬ	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

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.

7. Учебно-методическое и информационное обеспечение дисциплины

1. **Основная литература:**

   - Мэйволд, Э. Безопасность сетей / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. : схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 18.08.2019). – Текст : электронный.
   - Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=499170 (дата обращения:

18.08.2019). – Библиогр.: с. 221-226. – ISBN 978-5-4475-9823-5. – DOI 10.23681/499170. – Текст : электронный.

2. Дополнительная литература:

- Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. : табл., схем., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 18.08.2019). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.
- Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428820 (дата обращения: 18.08.2019). – Текст : электронный.

8. Материально-техническое обеспечение дисциплины

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.

Оборудование и аппаратура:

1. Компьютер с операционной системой Microsoft Windows.

Программное обеспечение и интернет-ресурсы:

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

9. Методические рекомендации для самостоятельной работы студентов

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.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: ст. преп. Гневшев А.Ю.

Программа утверждена на заседании кафедры “Информационная безопасность” «30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

**Структура и содержание дисциплины «Безопасность сетей электронных вычислительных машин»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)**

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
	4 семестр														
1	Основы современных сетевых технологий.	4	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		5			5	5								

	сетей. 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. Распределение криптографических ключей и согласование параметров защищенных туннелей.		16-17			5	5								
15	Безопасность удаленного доступа к локальной сети. Обзор средств построения защищенных виртуальных сетей.		18			2	2								
	Форма аттестации	4	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: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): «Безопасность открытых информационных 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:

список вопросов для экзамена

Составители: ст. преп. Гневшев А.Ю.

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Безопасность сетей электронных вычислительных машин					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК—12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	**знать:** принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей; основные протоколы сетей ЭВМ; эталонную модель взаимодействия открытых систем; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ; последовательность и содержание этапов построения компьютерных сетей; **уметь:** проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети; проводить мониторинг угроз безопасности компьютерных сетей; эффективно использовать различные методы и средства защиты информации для компьютерных сетей; **владеть:** способностью администрировать систему информационной безопасности; 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: демонстрирует полное соответствие следующих знаний: основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ Повышенный уровень: 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.