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

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
«28» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность сетей электронных вычислительных машин»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль/специализация
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

доцент, к.п.н., доцент **Д.Ф.Амиров**

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

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 «Безопасность сетей электронных вычислительных машин» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях.

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

Обучение по дисциплине «Безопасность сетей электронных вычислительных машин» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях	ИОПК-1.2.1.Знает принципы организации информационных систем в соответствии с требованиями по защите информации, криптографические стандарты и как их использовать в информационных системах; ИОПК-1.2.2.Умеет развертывать, конфигурировать и настраивать вычислительные сети, формулировать и настраивать политику безопасности
	распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; ИОПК-1.2.3.Владеет навыками использования типовых криптографических алгоритмов.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Безопасность сетей электронных вычислительных машин» относится к числу профессиональных учебных дисциплин обязательной части цикла (Б1) основной образовательной программы (Б1.30).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы ИКТ», «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.

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
1	**Аудиторные занятия**	**72**		
	В том числе:			
1.1	Лекции	-	-	-
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	4	1-19
2	**Самостоятельная работа**	**72**		
	В том числе:			
2.1	СРС	72	4	1-19
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен	-	4	По расписанию
	Итого	**144**		

3.2 Тематический план изучения дисциплины
(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	**Самостоятельная работа**	**72**					**72**
1.1	Основы современных сетевых технологий.	2					2
1.2	Схема взаимодействия с Webсервером. Распределенная обработка информации на основе мигрирующих программ. Доступ к реляционным базам данных.	2					2
1.3	Безопасное масштабирование компьютерных сетей. Использование повторителей. Сегментация сети с помощью мостов.	2					2

1.4	Применение коммутаторов. Построение маршрутизированных сетей. Алгоритмы и протоколы маршрутизации.	2					2
1.5	Способы нападений на компьютерные сети.	2					2
1.6	Способы несанкционированного доступа к информации в компьютерных сетях. Нападения на политику безопасности и процедуры административного доступа.	2					2
1.7	Нападения на постоянные компоненты системы защиты. Нападения на сменные элементы системы защиты.	2					2
1.8	Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей.	2					2
1.9	Защита от несанкционированного межсетевого доступа.	2					2
1.10	Функции межсетевого экранирования на различных	2					2

	уровнях модели OSI. Фильтрация трафика. Выполнение функций посредничества. Критерии оценки и классификация межсетевых экранов. Обзор современных систем FireWall.						
1.11	Построение защищенных виртуальных сетей	2					2
1.12	Введение в защищенные виртуальные сети. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне.	2					2
1.13	Построение защищенных виртуальных сетей на сеансовом уровне. Распределение криптографических ключей и согласование параметров защищенных туннелей.	2					2
1.14	Безопасность удаленного доступа к локальной сети. Обзор средств построения защищенных виртуальных сетей.	2					2

1.15	CMS, самые распространенные CMS, Drupal.	2					2
1.16	Уязвимости, характерные для вебприложений, особенности для CMS.	2					2
1.17	Уязвимости Drupal.	2					2
1.18	Виды терминалов удаленного доступа Telnet и SSH, сходства и различия.	2					2
1.19	Типовые ошибки безопасности использования SSH, best practice.	2					2
1.20	Инструменты для атак по словарю и брутфорса, способы защиты от них.	2					2
1.21	Обнаружение признаков атак на сервисы на уровне хоста, на уровне сети.	2					2
1.22	Характерные действия нарушителя. Обнаружение признаков атак на уровне сети. Обнаружение признаков атак на уровне хоста.	2					2
1.23	Основные уязвимости вебприложений. OWASP TOP 10.	2					2
1.24	Уязвимость SQL-инъекция. Суть. Виды. Угрозы.	2					2
1.25	Что такое веб-шелл и как их искать.	2					2
1.26	Фишинг. Основные способы атаки на пользователя.	2					2
1.27	Протокол RDP. Назначение, уязвимости и способы конфигурирования.	2					2

1.28	Базовые понятия Active Directory. Управление пользователями Active Directory.	2					2
1.29	Логирование событий в вебсервере. Какие данные хранятся в логах.	2					2
1.30	Основные сведения по анализу логов веб-сервера. На что следует обращать внимание.	2					2
1.31	Как проводить анализ базы данных веб-ресурса, на что стоит обращать внимание.	2					2
1.32	Основные сведения о почтовом сервере MS Exchange.	2					2
1.33	Что такое Outlook Web Access и какие угрозы он несет.	2					2

1.34	Маршрутизатор. Назначение и выполняемые функции, способы конфигурирования.	2					2
1.35	Протокол SMB. Основные сведения и применение.	2					2
1.36	Главные известные уязвимости протокола SMB.	2					2
2	**Лабораторные работы**	**72**			**72**		
2.1	Интерфейс Cisco Packet Tracer. Главное окно Cisco Packet Tracer. Оборудование и линии связи в Cisco Packet Tracer. Физическая комплектация оборудования.	8			8		
2.2	Режим симуляции в Cisco Packet Tracer.	6			6		
2.3	Сетевые службы. Настройка сетевых сервисов.	8			8		
2.4	Основные команды операционной системы Cisco IOS.	8			8		
2.5	Статическая маршрутизация. Настройка статической маршрутизации. Построение таблиц маршрутизации.	8			8		
2.6	Динамическая маршрутизация. Настройка протокола RIP. Настройка протокола RIP в корпоративной сети. Настройка протокола OSPF.	8			8		
2.7	Служба NAT. Преобразование сетевых адресов NAT.	6			6		
2.8	Виртуальные локальные сети VLAN. Настройка VLAN на одном коммутаторе Cisco. Настройка VLAN на двух коммутаторах Cisco. Настройка VLAN в корпоративной сети.	8			8		
2.9	Многопользовательский режим работы.	6			6		
2.10	Списки управления доступом ACL (Access Control List).	6			6		
	Итого	**72**			**72**		

Итого	**144**			**72**		**72**

3.3 Содержание дисциплины

Тема 1. Основы современных сетевых технологий.

Тема 2. Схема взаимодействия с Web-сервером. Распределенная обработка информации на основе мигрирующих программ. Доступ к реляционным базам данных.

Тема 3. Безопасное масштабирование компьютерных сетей. Использование повторителей. Сегментация сети с помощью мостов.

Тема 4. Применение коммутаторов. Построение маршрутизированных сетей. Алгоритмы и протоколы маршрутизации.

Тема 5. Способы нападений на компьютерные сети.

Тема 6. Способы несанкционированного доступа к информации в компьютерных сетях. Нападения на политику безопасности и процедуры административного доступа.

Тема 7. Нападения на постоянные компоненты системы защиты. Нападения на сменные элементы системы защиты.

Тема 8. Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей.

Тема 9. Защита от несанкционированного межсетевого доступа.

Тема 10. Функции межсетевого экранирования на различных уровнях модели OSI. Фильтрация трафика. Выполнение функций посредничества. Критерии оценки и классификация межсетевых экранов. Обзор современных систем FireWall.

Тема 11. Построение защищенных виртуальных сетей

Тема 12. Введение в защищенные виртуальные сети. Туннелирование на канальном уровне. Защита виртуальных каналов на сетевом уровне.

Тема 13. Построение защищенных виртуальных сетей на сеансовом уровне. Распределение криптографических ключей и согласование параметров защищенных туннелей.

Тема 14. Безопасность удаленного доступа к локальной сети. Обзор средств построения защищенных виртуальных сетей.

Тема 15. CMS, самые распространенные CMS, Drupal.

Тема 16. Уязвимости, характерные для веб-приложений, особенности для CMS.

Тема 17. Уязвимости Drupal.

Тема 18. Виды терминалов удаленного доступа Telnet и SSH, сходства и различия.

Тема 19. Типовые ошибки безопасности использования SSH, best practice.

Тема 20. Инструменты для атак по словарю и брутфорса, способы защиты от них.

Тема 21. Обнаружение признаков атак на сервисы на уровне хоста, на уровне сети.

Тема 22. Характерные действия нарушителя. Обнаружение признаков атак на уровне сети. Обнаружение признаков атак на уровне хоста.

Тема 23. Основные уязвимости веб-приложений. OWASP TOP 10.

Тема 24. Уязвимость SQL-инъекция. Суть. Виды. Угрозы.

Тема 25. Что такое веб-шелл и как их искать.

Тема 26. Фишинг. Основные способы атаки на пользователя.

Тема 27. Протокол RDP. Назначение, уязвимости и способы конфигурирования.

Тема 28. Базовые понятия Active Directory. Управление пользователями Active Directory. Тема 29. Логирование событий в веб-сервере. Какие данные хранятся в логах.

Тема 30. Основные сведения по анализу логов веб-сервера. На что следует обращать внимание.

1

Тема 31. Как проводить анализ базы данных веб-ресурса, на что стоит обращать внимание.

Тема 32. Основные сведения о почтовом сервере MS Exchange.

Тема 33. Что такое Outlook Web Access и какие угрозы он несет.

Тема 34. Маршрутизатор. Назначение и выполняемые функции, способы конфигурирования.

Тема 35. Протокол SMB. Основные сведения и применение. Тема

36. Главные известные уязвимости протокола SMB.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Лабораторные занятия

Лабораторная работа №1. Режим симуляции в Cisco Packet Tracer
Лабораторная работа №2. Настройка сетевых сервисов
Лабораторная работа №3. Знакомство с командами IOS
Лабораторная работа №4. Настройка статической маршрутизации
Лабораторная работа №5. Построение таблиц маршрутизации
Лабораторная работа №6. Настройка протокола RIP
Лабораторная работа №7. Настройка протокола RIP в корпоративной сети
Лабораторная работа №8. Настройка протокола OSPF
Лабораторная работа №9. Преобразование сетевых адресов NAT Лабораторная работа № 10. Настройка VLAN на одном коммутаторе Cisco
Лабораторная работа № 11. Настройка VLAN на двух коммутаторах Cisco
Лабораторная работа № 12. Настройка VLAN в корпоративной сети
Лабораторная работа № 13. Многопользовательский режим работы
Лабораторная работа № 14. Списки доступа

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

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

2

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. (дата обращения: 01.09.2022)

2. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. - Москва : Директ-Медиа, 2019. - 240 с. - ISBN 978-5-4475-9823-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1908083. (дата обращения: 01.09.2022)

3. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. — 120 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/257564. (дата обращения: 01.09.2022).

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. (дата обращения: 01.09.2023).

2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401. (дата обращения: 01.09.2023).

3. 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. (дата обращения: 01.09.2023).

4.4 Электронные образовательные ресурсы

https://www.cisco.com/c/m/en_sg/partners/cisco-networking-academy/index.html

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. VBox

4.6 Современные профессиональные базы данных и информационные справочные системы

Локальный научно-образовательный комплекс по дисциплине «Безопасность сетей электронных вычислительных машин».

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

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

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 и практической подготовки студентов являются лекции и лабораторные работы.

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

7.1 Методы контроля и оценивания результатов обучения

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

4

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины; - экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.

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.

7.3 Оценочные средства

7.3.1 Оценочные средства для текущей аттестации

Компьютерное тестирование.

7.3.2 Оценочные средства для промежуточной аттестации

Экзамен.

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.