



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»



УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ВИРТУАЛЬНЫЕ СЕТИ

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы

10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения

очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3
Семестр	5

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)


Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
25.01.2022, протокол № 4

Зав. кафедрой  И.И. Баранкова


Рабочая программа одобрена методической комиссией ИЭиАС
26.01.2022 г. протокол № 5

Председатель  В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук

 И.И. Баранкова

Рецензент:
начальник УИТиАСУ, канд. техн. наук

 К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Виртуальные сети» являются овладение студентами необходимым и достаточным уровнем профессиональных, профессионально-специализированных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем».

Специальными целями дисциплины «Виртуальные сети» являются:

- изучение архитектуры и настроек виртуальных локальных сетей (VLAN);
- изучение структуры, принципов работы, настроек виртуальных частных сети (VPN) и технологий на их основе Site-to-site VPN, FlexVPN и SSL VPN;
- освоение облачных технологий виртуальных сетей.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Виртуальные сети входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Информатика

Сети и системы передачи информации

Технология построения защищенных распределенных приложений

Программно-аппаратные средства обеспечения информационной безопасности

Информационная безопасность распределенных информационных систем

Разработка и эксплуатация защищенных автоматизированных систем

Криптографические методы защиты информации

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Производственная-преддипломная практика

Научно-исследовательская работа

Подготовка к защите и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Виртуальные сети» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-1	Способен проводить анализ безопасности компьютерных систем
ПК-1.1	Оценивает эффективность защиты информации
ПК-1.2	Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты информации
ПК-2	Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей
ПК-2.1	Разрабатывает профили защиты компьютерных систем
ПК-2.2	Формирует политики безопасности компьютерных систем и сетей

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

- контактная работа – 55 акад. часов;
- аудиторная – 54 акад. часов;
- внеаудиторная – 1 акад. часов;
- самостоятельная работа – 53 акад. часов;
- в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Виртуальные локальные сети (VLAN).								
1.1 Типы VLAN, сегментация VLAN. Понятие голосовых транков. Стандарт 802.1q. Тэгирование Ethernet.	5	2		2/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Построение одноуровневой ЛВС с VLAN на лабораторном стенде»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
1.2 Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Поиск неисправностей при использовании VLAN.		2		2/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Организация магистрального соединения при помощи транковых портов»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
1.3 Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.		2		2/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Организация маршрутизации между VLAN»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
Итого по разделу		6		6/6И	6			
2. Виртуальные частные сети (VPN). Сетевые технологии Site-to-site VPN, FlexVPN и SSL VPN. Настройка и использование Cisco AnyConnect VPN.								

2.1 Задачи VPN-технологий. Защита от угроз для WAN-соединений и безопасность удалённого доступа. Основные компоненты VPN-технологии.	5			2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
2.2 Протоколы работы VPN: GRE, PPTP, L2TP, PPPoE. Конфигурирование соединения				2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Развертывание и конфигурирование PPTP-сервера»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
2.3 Протокол ISAKMP. Технология IPsec, Совместная работа IPSEC и NAT. Транзитная передача зашифрованного трафика.				2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Построение VPN-соединения на базе протокола IPSEC на базе маршрутизаторов CISCO»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
2.4 Dynamic VPN, конфигурирование функций динамического VPN-концентратора. Конфигурирование сервиса DynDNS.				2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Конфигурирование VPN на базе маршрутизаторов CISCO»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
2.5 Конфигурирование классического туннельного соединения для объединения офисных сетей. Развёртывание DMVPN на устройствах с Cisco IOS. IPsec VPN с использованием SDM.				2/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Конфигурирование VPN на базе маршрутизаторов CISCO»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
2.6 Технология FlexVPN. Основные преимущества и возможности технологии FlexVPN.. Централизованное конфигурирование узлов-участников.				2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Конфигурирование VPN на базе маршрутизаторов CISCO»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2

2.7 Технология SSL VPN. Групповые политики SSL-клиентов на Cisco ASA и connection profiles. Настройка SSL VPN на Cisco ASA. Аутентификация через внешний AAA-сервер и использование локального/внешнего CA		2		2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Настройка SSL VPN на CISCO ASA»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
2.8 Настройка и использование Cisco AnyConnect VPN. Мониторинг работы AnyConnect VPN. Настройка специфических аспектов работы AnyConnect VPN.		2		2/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Управление CISCO ASA при помощи CISCO ASDM»	
Итого по разделу		16		16/10И	16			
3. Облачные технологии виртуальных сетей.								
3.1 Характеристики аппаратно-программных платформ виртуализации для построения виртуальных сетей. Характеристики облачных провайдеров для построения виртуальных инфраструктур IaaS	5	2		3/1И	2,1	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
3.2 Построение в облаке изолированной виртуальной подсети для связи между виртуальными машинами.		4		3/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
3.3 Реализации служб DNS, WINS, DHCP, NAT в виртуальной сетевой среде. Создание виртуальных Web-серверов в облаке, балансировка сетевой нагрузки в облаке для веб-серверов (NLB).		2		2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
3.4 Реализации сетевой безопасности в облаке VMware vShield, Cisco Adaptive Security Appliance (ASA).		2		2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2

3.5 Создание VPN-серверов для виртуальных частных сетей в облаке.		2		2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
3.6 Облачная среда передачи данных Data Center Bridging (DCB), расширенный протокол xSTP, метод передачи трафика сети хранения данных Fibre Channel по сети Ethernet. FCoE технология		2		2/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Организация ЛВС с VLAN»	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.2
Итого по разделу		14		14/6И	12,1			
Итого за семестр		36		36/22И	34,1		зао	
Итого по дисциплине		36		36/22И	34,1		зачет с оценкой	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Виртуальные сети» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/450234> (дата обращения: 31.08.2020).

2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452430> (дата обращения: 31.08.2020).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/453063> (дата обращения: 31.08.2020).

б) Дополнительная литература:

1. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей : учебное пособие для магистратуры / О. М. Замятина. — Москва : Издательство Юрайт, 2019. — 159 с. — (Университеты России). — ISBN 978-5-534-00335-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/433938> (дата обращения: 31.08.2020).

2. Котенко, В. В. Технологии информационного анализа пользовательского уровня телекоммуникационных систем : учебное пособие / В. В. Котенко ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 194 с. - ISBN 978-5-9275-3176-9. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1088143> (дата обращения: 31.08.2020)

МАКРООБЪЕКТЫ:

3. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] /

[сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true> (дата обращения: 31.08.2020). - Макрообъект. - ISBN 978-5-9967-1305-9. - Текст : электронный. - Сведения доступны также на CD-ROM.

4. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: <https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true> (дата обращения: 31.08.2020). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст : электронный. - Сведения доступны также на CD-ROM.

***РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ**

1. Перейти по адресу электронного каталога <https://magtu.informsystema.ru>
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Виртуальные сети» (Приложение 1)
2. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Виртуальные сети» (Приложение 2)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS SQL Server Management Studio	свободно распространяемое ПО	бессрочно
Oracle My SQL Workbench Community Edition	свободно распространяемое ПО	бессрочно
Oracle SQL Developer	свободно распространяемое ПО	бессрочно
Oracle SQL Developer Data Modeler	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

Информационная система - Нормативные правовые акты, организационно-распорядительн ые документы, нормативные и методические документы и	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
Международная реферативная и полнотекстовая справочная база данных научных изданий	https://www.nature.com/siteindex
Международная реферативная база данных по чистой и	http://zbmath.org/
Международная база справочных изданий по всем отраслям знаний	http://www.springer.com/references
Международная база научных материалов в области	http://materials.springer.com/
Международная коллекция научных протоколов по	http://www.springerprotocols.com/
Международная база полнотекстовых журналов	http://link.springer.com/
Международная реферативная и полнотекстовая справочная база	http://scopus.com
Университетская информационная система	https://uisrussia.msu.ru
Федеральный образовательный портал – Экономика.	http://ecsocman.hse.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И.	https://magtu.informsystema.ru/Marc.html?locale=ru
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к	URL: http://window.edu.ru/
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система – Российский индекс	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East View Information	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)-
Мультимедийные средства хранения, передачи и представления информации

Лаборатория сетей и систем передачи информации. Лаборатория безопасности сетей ЭВМ:

1. Учебно-лабораторный стенд "Кодирование и модуляция информации в системах связи", комплектация полная

2. Учебно-лабораторный стенд "Системы спутниковой навигации" GPS

3. Комплект типового учебного оборудования "Сети сотовой связи GSM"

4. Комплект типового учебного оборудования "Телекоммуникационные линии связи" ТЛС-01

5. Комплект типового учебного оборудования "Сетевая безопасность типа SECURITY-3M"

6. Комплект учебного оборудования "Беспроводные компьютерные сети ЭВМ"

7. Модуль учебно-лабораторный для изучения низкоуровневого контроллера Ethernet

8. Стенд коммуникационного оборудования сервером для моделирования облачного сервиса

Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.) -
Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а -
Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Виртуальные сети» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает выполнение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

1. Цели и задачи защиты информации в вычислительных сетях.
2. Развитие технологий обеспечения безопасности сетей ЭВМ, эволюция подходов к обеспечению безопасности.
3. Угрозы информационной безопасности в современных вычислительных сетях.
4. Виды вычислительных сетей с характеристикой основных принципов построения.
5. Понятие целостности информации в вычислительных сетях. Причины нарушения целостности информации, их последствия и методы предотвращения.
6. Сетевая уязвимость – понятие, виды уязвимостей, их классификация, методы устранения.
7. Семиуровневая эталонная модель межсетевого взаимодействия (модель OSI). Дайте краткую характеристику задач каждого уровня модели.
8. Классификация современного сетевого оборудования с характеристикой каждого из классов.
9. Сетевой протокол – понятие, назначение, классификация с привязкой к уровням модели OSI. Перечислите известные Вам уязвимости современных сетевых протоколов.
10. Протокол TCP/IP как базовый протокол современных вычислительных сетей. Протоколы стека протоколов TCP/IP с краткой характеристикой основных.
11. Принципы работы IP-сетей. Маршрутизация, организация межсетевого взаимодействия, - основные принципы и технологии.
12. Глобальные вычислительные сети – история, технологии, базовые принципы построения, основные сервисы. Использование глобальных вычислительных сетей в контексте сетевой безопасности.
13. Технологии построения защищенной локальной вычислительной сети – структурирование сети, использование технологии VLAN, списков контроля доступа и т.д.

14. Сетевая атака. Классификация, методы проведения, фазы сетевой атаки.
15. Перечислите известные Вам методы сетевых атак. Оцените возможный ущерб для каждой из них и предложите известные методы противодействия.
16. Маршрутизация трафика в IP-сетях. Назначение, основные алгоритмы и принципы. Использование принципов маршрутизации злоумышленником (подмена субъекта или объекта маршрутизации, навязывание ложного маршрута) и методы предотвращения таких действий.
17. Межсетевые экраны – назначение, принцип действия, классификация, характеристики.
18. Построение защищенной вычислительной сети по принципу «оборона в глубину» - базовые понятия, основные структурные зоны и элементы сети.
19. Системы обнаружения вторжений. Системы предотвращения вторжений. Базовые принципы работы и основные характеристики.
20. Антивирусная защита в вычислительной сети.
21. Программное обеспечение, предназначенное для поиска и анализа уязвимостей в сетях ЭВМ.
22. Виртуальные частные сети (VPN). Виртуальные защищенные сети. Принципы построения, использование технологии VPN в контексте построения безопасной вычислительной сети.
23. Беспроводные сети. Основные принципы работы, основные уязвимости и методы их устранения.
24. Использование технологий шифрования и криптографической защиты информации в обеспечении безопасности сетей ЭВМ.7 Оценочные средства для проведения промежуточной аттестации

Приложение 2

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Оценочные средства	
ПК-1 Способен проводить анализ безопасности компьютерных систем	
ПК-1.1	Оценивает эффективность защиты информации
	<ol style="list-style-type: none">1. Анализ тенденций развития технологий современных глобальных и локальных вычислительных сетей с точки зрения специалиста по информационной безопасности;2. Прогнозирование потребности организации в технологиях защиты информации в сетях ЭВМ исходя из характера хозяйственной деятельности организации и обрабатываемой ею информации;3. Рабочие характеристики современного сетевого оборудования, способность к самостоятельному выбору необходимого сетевого оборудования при разработке проекта защищенной вычислительной сети;4. Принципы функционирования средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ)5. Номенклатура сетевого оборудования и средств защиты информации в вычислительных сетях отечественного и мирового производства
ПК-1.2	Применяет разработанные методики оценки защищенности программно-аппаратных средств защиты информации
	<ol style="list-style-type: none">1. Выполнять подбор сетевого оборудования исходя из его рабочих характеристик и наличия средств обеспечения безопасности информации в вычислительных сетях;2. Разработать топологию вычислительной сети согласно поставленной задаче, определить факторы риска с точки зрения информационной безопасности в разработанной сети;3. Выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, межсетевой экран) для построения разработанной топологии сети и соблюдения требований по защите информации;4. Реализовать разработанную политику сетевой безопасности при настройке и конфигурированию сетевого оборудования.
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	
ПК-2.1	Разрабатывает профили защиты компьютерных систем
	<ol style="list-style-type: none">1. Произвести анализ сети программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемые сканеры WireShark и Ethereal)2. Произвести диагностику неисправностей и аномальных состояний вычислительных сетей3. Произвести поиск неисправностей вычислительных сетей и оптимизации их работы4. Разработать профиль защиты компьютерной системы предложенной конфигурации
ПК-2.2	Формирует политики безопасности компьютерных систем и сетей
	<ol style="list-style-type: none">1. физические принципы передачи информации по различным каналам связи2. характерные уязвимости, присущие каналами связи при передаче информации по ним

Оценочные средства

3. методы перехвата информации при передаче ее по различным каналам связи
4. Выполнить диагностику неисправностей и аномалий работы сети ЭВМ
5. Сделать заключение о возможности или невозможности несанкционированного доступа к информации при данной неисправности сети
6. Предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации сети ЭВМ
7. Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ
8. Произвести проверку организации системы защиты информации вычислительной сети на соответствие организационно-техническим требованиям по защите информации.
9. Определить состав методов и объем испытаний для определения наличия уязвимостей вычислительной сети и их характер.
10. Произвести фильтрацию трафика вычислительной сети с помощью свободно распространяемых программ-анализаторов WireShark или Ethereal
11. Определить характерные признаки сетевой атаки на основе анализа сетевого трафика

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.