МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«26» сентября 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ВИРТУАЛЬНЫЕ СЕТИ
наименование дисциплины

Специальность
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование специальности

Специализация программы
Обеспечение информационной безопасности распределенных информационных систем
наименование специализации

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2018 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«07» сентября 2018 г., протокол № 1.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«26» сентября 2018 г., протокол № 1.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
2.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
3.	7	Переработка фонда оценочных средств	№ 1 от 04.09.2020	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 04.09.2020	

1 Цели освоения дисциплины

Целями освоения дисциплины «Виртуальные сети» являются повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение студентами необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВПО 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 в структуре образовательной программы подготовки специалиста

Дисциплина «Виртуальные сети» относится к вариативной части профессионального цикла дисциплин по специальности «Информационная безопасность автоматизированных систем». Для изучения дисциплины необходимы знания, умения и навыки, сформированные в результате освоения предыдущих дисциплин «Информатика», «Организация ЭВМ и вычислительных систем», «Сети и системы передачи информации», «Безопасность сетей ЭВМ», «Безопасность операционных систем», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем», «Управление информационной безопасностью», «Моделирование угроз информационной безопасности».

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

В результате освоения дисциплины «Безопасность сетей ЭВМ» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-10 - способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать	- Типовые структуры и принципы организации виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. - Программно-аппаратные средства обеспечения информационной безопасности в виртуальных локальных компьютерных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах
Уметь	- Использовать методологию проектирования защищенных вычислительных сетей; применять технологии и средства защиты информации для обеспечения безопасности информации в вычислительных сетях.
Владеть	- Навыками разработки, документирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению безопасности.
ПК-24 - способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований	

Структурный элемент компетенции	Планируемые результаты обучения
информационной безопасности	
Знать	- Типовые структуры и принципы организации виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. - Программно-аппаратные средства обеспечения информационной безопасности в виртуальных локальных компьютерных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах. -Принципы построения и функционирования, примеры реализаций виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. - Основные протоколы виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.
Уметь	- Эффективно использовать различные методы и средства защиты информации для виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.
Владеть	- Навыками использования программно-аппаратных средств обеспечения безопасности виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.
ПСК-7.4 - способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	
Знать	- Последовательность и содержание этапов построения виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. - Принципы построения и функционирования виртуальных локальных и виртуальных частных систем и сетей передачи информации, а также специализированных виртуальных систем и сетей в облачных сетевых структурах.
Уметь	- Проектировать и администрировать виртуальные локальные сети и виртуальные частные сети, а также специализированные виртуальные сети в облачных сетевых структурах. Реализовывать политику безопасности виртуальной локальной сети и виртуальной частной сети, а также специализированной виртуальной сети в облачных сетевых структурах. - Пользоваться профессиональными и нестандартными (в т.ч. собственной разработки) сетевыми средствами виртуальных сетей для обмена данными, в том числе с использованием глобальной информационной сети Интернет.
Владеть	- Навыками обеспечения безопасности информации с помощью стандартных сетевых средств обмена информацией в виртуальных локальных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах. - Навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, авторизации, аутентификации и аудита), виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению информационной безопасности;

4 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

- контактная работа – 106,85 акад. часов:
  - аудиторная – 102 акад. часа;
  - внеаудиторная – 4,85 акад. часа
- самостоятельная работа – 37,45 акад. часов;
  Форма промежуточной аттестации: экзамен;
- подготовка к экзамену – 35,7 акад. часа.

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	гиялаборат.	практич. занятия				
Раздел 1. Виртуальные локальные сети (VLAN).	9							
Тема 1.1. Типы VLAN, сегментация VLAN. голосовые VLAN. Понятие транка. Стандарт 802.1q. Тэгирование Ethernet.	9	4		4/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Построение одноуровневой ЛВС с VLAN на лабораторном стенде»	*ПК-10 -зув*
Тема 1.2. Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Динамический протокол инициализации транка (DTP). Поиск неисправностей при использовании VLAN. Рекомендации по дизайну VLAN.	9	4		4/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Организация магистрального соединения при помощи транковых портов»	*ПК-10-зув*
Тема 1.4. Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.	9	4		4/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Организация маршрутизации между VLAN»	*ПК-10 -зув*

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
Итого по разделу		**12**		**12/6И**	**6**			
Раздел 2. Виртуальные частные сети (VPN). Сетевые технологии Site-to-site VPN, FlexVPN и SSL VPN. Настройка и использование Cisco AnyConnect VPN.								
Тема 2.1. Задачи VPN-технологий. Защита от угроз для WAN-соединений и безопасность удалённого доступа. Типы VPN: Site-to-Site VPN (LAN-to-LAN VPN) и Remote access VPN. Основные компоненты для каждой VPN-технологии.	9	3		3/1И	1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ОПК-8 -з
Тема 2.2. Протоколы работы VPN: протокол GRE, конфигурирование простого Site-to-Site туннельного соединения; протокол PPTP, конфигурирование клиент-серверного соединения с использованием PPTP на маршрутизаторе и рабочей станции; протокол L2TP, конфигурирование клиент-серверного соединения с использованием L2TP на маршрутизаторе и рабочей станции; протокол PPPoE, конфигурирование соединения с использованием PPPoE на маршрутизаторах.	9	3		3/1И	1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Развертывание и конфигурирование PPTP-сервера»	ОПК-8-*зув*
Тема 2.3. Протокол ISAKMP, фазы построения туннеля. Технология IPSec, криптографические алгоритмы: алгоритмы	9	3		3/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Лабораторная работа «Построение VPN-соединения на базе протокола IPSEC на базе	ОПК-8-*зув*

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
шифрования, алгоритмы хеширования, алгоритмы безопасного обмена ключами. Совместная работа IPSEC и NAT. Быстрое развертывание IPSec-VPN-соединений (EZ-VPN). Конфиденциальность, целостность, подлинность и неотказуемость. Понятие ключа и ключевого материала. PKI, Next-Generation Encryption. Транзитная передача шифрованного трафика.							маршрутизаторов CISCO RW-120»	
Тема 2.4. Dynamic VPN, конфигурирование функций динамического VPN-концентратора на маршрутизаторе. Remote Access IPSec VPN, конфигурирование L2TP/IPSec VPDN-сервера с локальной аутентификацией на маршрутизаторе, конфигурирование L2TP/IPSec клиента на рабочей станции. Конфигурирование сервиса DynDNS на маршрутизаторе.	9	3		3/1И	2		Лабораторная работа «Конфигурирование VPN на базе маршрутизаторов CISCO ASA 5505»	ОПК-8-*зув*
Тема 2.5. Технологии Site-to-site VPN. Конфигурирование классического туннельного соединения для объединения офисных сетей . Топологии и технологии для S2S VPN. IPsec VPN. Работа IKE и IKEv2. Протокол ESP. Виртуальные интерфейсы VPN (VTI). Работа DMVPN. Настройка Point-to-Point (P2P) VPN на Cisco ASA. Настройка IKE, PSK, создание Transform Set и ACL для	9	4		4/2И	2		Лабораторная работа «Конфигурирование VPN на базе маршрутизаторов CISCO ASA 5505»	ОПК-8-*зув*

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
отбора трафика. Настройка VTI на устройствах с Cisco IOS. Создание динамических туннелей, использующих шаблоны VTI. Развёртывание DMVPN на устройствах с Cisco IOS. Как работает GRE и NHRP. Настройка DMVPN со стороны центрального участника (Hub) и подключающегося (Spoke). Маршрутизация внутри DMVPN. Реализация Site-to-site IPSec VPN с использованием SDM.								
Тема 2.6. Технология FlexVPN. Как работает и устроен FlexVPN. Основные преимущества и возможности технологии FlexVPN. Использование Cisco IOS FlexVPN. Сравнение IKEv2 и IKEv1. Преимущества IKEv2 и реализация защищённой установки соединения. Работа P2P FlexVPN. Типовые сценарии FlexVPN. Работа Point-to-Multipoint (Hub-and-Spoke) IPsec VPN, используя FlexVPN. Централизованное конфигурирование узлов-участников. Сценарий Spoke-to-Spoke - "shortcut", настройка NHRP в данном сценарии. Проверка и оптимизация работы в сценарии с прямой связью между spoke.	9	3		3/1И	2			ОПК-8-*зув*

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	гиялаборат.	практич. занятия				
Тема 2.7. Технология SSL VPN. Преимущества SSL VPN. Установка соединения. Подтверждение подлинности как сервера, так и клиента. Групповые политики SSL-клиентов на Cisco ASA и connection profiles. Настройка SSL VPN на Cisco ASA. Настройка подтверждения подлинности со стороны Cisco ASA и проверки подключающихся клиентов. Работа с плагинами для приложений, работающих через SSL VPN. Как работает и настраивается smart tunnel. Тонкая настройка аутентификации и авторизации клиентов при работе с SSL VPN. Аутентификация через внешний AAA-сервер и использование локального/внешнего CA.	9	3		3/1И	2		Лабораторная работа «Настройка SSL VPN на CISCO ASA»	ОПК-8-*зув*
Тема 2.8. Настройка и использование Cisco AnyConnect VPN. Настройка простого сценария AnyConnect VPN на Cisco ASA. Настройка отдельных компонентов - аутентификации клиента и сервера, назначения IP-адресов, работы split tunneling, групповых политик и Identity NAT. Мониторинг работы AnyConnect VPN. Настройка специфических аспектов работы AnyConnect VPN. Параллельные туннели для TLS и DTLS. Управление ПО клиента со	9	3		3/2И	2		Лабораторная работа «Управление CISCO ASA при помощи CISCO ASDM»	ОПК-8-*зув*

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
стороны Cisco ASA. Работа с Trusted Network Detection и настройка AnyConnect SBL (Start Before Logon). Аутентификация на базе x.509-сертификатов. Отзыв сертификатов и проверка на отзыв у клиентов. Многофакторная аутентификация и авторизация с Cisco ISE. Настройка AnyConnect IPsec с IKEv2. Особенности IKEv2 и настройка его в данном сценарии.								
Итого по разделу		**25**		**25/10 И**	**14**			
Раздел 3. Облачные технологии виртуальных сетей.								
Тема 3.1. Характеристики аппаратно-программных платформ виртуализации (VMware vSphere, Microsoft HyperV, Citrix XenServer, RedHat RHEV) для построения виртуальных сетей. Характеристики облачных провайдеров для построения виртуальных инфраструктур IaaS (Amazon Web Services Elastic Compute Cloud, Cisco Systems CloudVerse, Google Compute Engine, Microsoft Azure, AT&T Cloud Services, CA Technologies Private Cloud Accelerator, Dell vCloud Datacenter Service, Eucalyptus Systems, Hewlett-Packard Converged Cloud, IBM	9	3		3/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПСК-7.4 - зу

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
SmartCloud, OpenStack Foundation, Rackspace Hosting, Virtustream xStream).								
Тема 3.2. Отличия технологий построения виртуальных сетей в физической сетевой среде и в облачной (виртуальной) сетевой среде. Построение в облаке изолированной виртуальной подсети для связи между виртуальными машинами. Организация виртуальных подсетей в облаке с использованием комбинированного подхода: построение одновременно внутренних и внешних подсетей, либо выдача двух и более внешних или внутренних сетей. Построение внешней маршрутизируемой виртуальной подсети с количеством IPv4/IPv6-адресов согласно требованиям клиента облака. Технология организации демилитаризованной зоны (DMZ) в виртуальной сетевой среде.	9	3		3/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПК-24 -зу
Тема 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).	9	2		2/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПСК-7.4 -зу
Тема 3.4. Реализации сетевой безопасности в облаке VMware vShield, Cisco Adaptive Security Appliance (ASA).	9	2		2/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Подготовка самостоятельного сообщения на заданную тему	ПСК-7.4 -зу

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	гиялаборат.	практич. занятия				
Тема 3.5. Создание VPN-серверов для виртуальных частных сетей в облаке. Преимущества и особенности использования по сравнению с VPN-серверами без облака.	9	2		2/1И	3			
Тема 3.6. Сетевая архитектура облака, развитие технологии Ethernet в облачной среде передачи данных Data Center Bridging (DCB), расширенный протокол xSTP (Spanning Tree Protocol, технология VEB (Virtual Ethernet Bridge), метод передачи трафика сети хранения данных Fibre Channel по сети Ethernet FCoE (Fibre Channel over Ethernet), технология расширения концепции использования Fabric Extender до уровня виртуальных машин VM-FEX (Virtual Machine Fabric Extender), распределенные виртуальные коммутаторы, интегрированные со средой виртуализации Cisco Nexus 1000V.	9	2		2/1И	2,45	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Защита лабораторной работы «Организация ЛВС с VLAN»	ПСК-7.4-*зув*
Итого по разделу		**14**		**14/6И**	**17,45**			
Подготовка к экзамену	**9**				**35,7**		Подготовка к экзамену	
Итого за семестр		**51**		**51/22И**	**73,15**		**Промежуточная аттестация (экзамен)**	
Итого по дисциплине		**51**		**51/22И**	**73,15**		**Экзамен**	ОПК-8-*зув* *ПК-10 -зув* ПСК-7.4-

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	гиялаборат.	практич. занятия				
								зув

5 Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Безопасность сетей ЭВМ» 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 у 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.

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

а) **Традиционная технология**, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям.

b) ***Вводная лекция*** – для целостного представления об учебном предмете и анализа учебно-методической литературы;

c) ***Обзорные лекции*** – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

d) ***Проблемные лекции*** – для ведения диалога обучающихся с преподавателем по сложным темам, для более полного раскрытия содержания проблемы по некоторым темам, а так же для развития исследовательских навыков и изучения способов решения задач;

2) ***Лекции-визуализации*** – для наглядного представления материалов курса. Лекционные занятия проводятся с использованием презентационного оборудования (проектор, экран, ноутбук), в качестве наглядных материалов используются: Web-ориентированные программные учебные материалы, электронные плакаты, презентации к лекциям.

3) **Модульно-компетентностная технология**, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Для формирования у обучающихся основных понятий дисциплины используются:

a) ***Кейс-методы*** – для овладения системой знаний и умений и творческого их

использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

4) **Интерактивное обучение**. Все лабораторные занятия проводятся в интерактивной форме. В рамках интерактивного обучения обучающихся применяются:

   a) *Case-study* – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.
   b) *Методы IT* – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.
   c) *Проблемное обучение* – для стимулирования к самостоятельной «добыче» знаний, необходимых для решения конкретной проблемы. Для этого каждому обучающемуся выдаётся индивидуальная тема, по которой он должен выполнить курсовую работу.

5) ***Контекстное обучение*** – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации в виртуальных сетях, обучающийся приобретет способность участвовать в разработке защищенных виртуальных сетей и обеспечению безопасности виртуальных сетей по профилю своей профессиональной деятельности;

   a) ***Междисциплинарное обучение*** – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

6) Для приобретения **новых фактических знаний и практических умений** используются лабораторные занятия:
   a) компьютерный практикум;
   b) разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

6 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

7. Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-10 - способность к освоению новых образцов программных, технических средств и информационных технологий		
Знать	Типовые структуры и принципы организации виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. Программно-аппаратные средства обеспечения информационной безопасности в виртуальных локальных компьютерных сетях и виртуальных частных сетях, а также специализированных виртуальных сетях в облачных сетевых структурах	1. Способность к самостоятельному анализу тенденций развития технологий современных глобальных и локальных вычислительных сетей с точки зрения специалиста по информационной безопасности; 2. Способность прогнозировать потребности организации в технологиях защиты информации в сетях ЭВМ исходя из характера хозяйственной деятельности организации и обрабатываемой ею информации; 3. Знание основных рабочих характеристик современного сетевого оборудования, способность к самостоятельному выбору необходимого сетевого оборудования при разработке проекта защищенной вычислительной сети; 4. Понимание принципов функционирования средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ) 5. Знание номенклатуры сетевого оборудования и средств защиты информации в вычислительных сетях отечественного и мирового производства

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Уметь:	- анализировать основные характеристики и возможности сетей ЭВМ по передаче информации; - самостоятельно разработать топологию вычислительной сети исходя из заданных требований; - самостоятельно выполнить настройку управляемого сетевого оборудования (коммутатор, маршрутизатор, межсетевой экран); - разработать политику сетевой безопасности для заданной сети ЭВМ исходя из заданных требований с использованием современных технологий сетевой безопасности.	Самостоятельно выполнить подбор сетевого оборудования исходя из его рабочих характеристик и наличия средств обеспечения безопасности информации в вычислительных сетях; Уметь разработать топологию вычислительной сети согласно поставленной задаче, определить факторы риска с точки зрения информационной безопасности в разработанной сети; Уметь выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, сежсетевой экран) для построения разработанной топологии сети и соблюдения требований по защите информации; Уметь реализовать разработанную политику сетевой безопасности при настройке и конфигурированию сетевого оборудования.
Владеть	профессиональным языком и терминологией предметной области (сети ЭВМ) - современным сетевым и диагностическ	Навыками работы с программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемые сканеры WireShark и Ethereal) Навыками диагностики неисправностей и аномальных состояний вычислительных сетей Навыками решения задач по поиску неисправностей

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	им оборудованием и программным обеспечением, предназначенным для построения вычислительных сетей (сетей ЭВМ) -методикой проектирования защищенных сетей ЭВМ	вычислительных сетей и оптимизации их работы
ПК-23 - способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа		
Знать	- принципы передачи информации по телекоммуникационным каналам; - принципы функционирования и основные рабочие характеристики оборудования сетей ЭВМ; - основные меры и механизмы защиты информации в сетях ЭВМ; - меры предотвращения утечки информации по техническим каналам сетей ЭВМ; - базовую модель угроз и модель нарушителя в сетях ЭВМ; - принципы функционирования средств защиты информации в сетях ЭВМ;	1. знать физические принципы передачи информации по различным каналам связи 2. знать и понимать характерные уязвимости, присущие каналами связи при передаче информации по ним 3. Четко представлять методы перехвата информации при передаче ее по различным каналам связи
Уметь	- применять действующую нормативную базу при	Самостоятельно диагностировать неисправность или аномалию работы сети ЭВМ Сделать самостоятельное заключение о возможности или

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	обеспечении безопасности сетей ЭВМ; - Самостоятельно диагностировать неисправности и аномалии сетей ЭВМ; - выявлять основные угрозы безопасности в сетях ЭВМ; - контролировать безотказное функционирование средств защиты информации в сетях ЭВМ; - осуществлять подбор инструментальных и программных средств тестирования систем защиты сетей ЭВМ; – разработать комплекс организационных и технических мероприятий для предотвращения несанкционированного доступа к защищаемой информации в сетях ЭВМ;	невозможности несанкционированного доступа к информации при данной неисправности сети Предложить комплекс мер по устранению неисправности и предотвращению несанкционированного доступа к информации сети ЭВМ Разработать комплекс мер для контроля безотказного функционирования сетей ЭВМ
Владеть	- методиками определения и поиска уязвимостей систем защиты информации в сетях ЭВМ; - навыками настройки	1. Произвести проверку организации системы защиты информации вычислительной сети на соответствие организационно-техническим требованиям по защите информации. 2. Определить состав методов и объем испытаний для определения наличия уязвимостей вычислительной сети и их

Структурный элемент	Планируемые результаты обучения	Оценочные средства
	сетевого оборудования; - методиками определения и классификации сетевых атак; - методиками предотвращения сетевых атак; - методиками составления политик сетевой безопасности;	характер. 3. Произвести фильтрацию трафика вычислительной сети с помощью свободно распространяемых программ-анализаторов WireShark или Ethereal 4. 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.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Операционная система Linux: Курс лекций [Электронный ресурс]: Учебное пособие/ Г.В. Курячий, К.А.Маслинский. - М.: ДМК Пресс, 2010. – 348 с. - Режим доступа: http://e.lanbook.com/view/book/1202/ –Заглавие с экрана. – ISBN 978-5-94074-591-4.

2. Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с. Режим доступа: http://znanium.com/bookread.php?book=463062. -Заглавие с экрана.

б) Дополнительная литература:

1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс]: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил. - (Высшее образование). Режим доступа: http://znanium.com/bookread.php?book=402686 –Заглавие с экрана.– ISBN 978-5-8199-0411-4

2. Компьютерные сети [Электронный ресурс]: Учебное пособие для студ. учреждений СПО/ Н.В. Максимов, И.И. Попов. - 6-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2013. - 464 с.: ил.- (Профессиональное образование). Режим доступа: http://znanium.com/bookread.php?book=163728. -Заглавие с экрана.– ISBN 978-5-91134-764-2.

3. Исаченко, О.В Программное обеспечение компьютерных сетей сценариев [Электронный ресурс]: Учебное пособие / Исаченко О.В.. - М.: ИНФРА-М, 2012. - 117 с- (Среднее профессиональное образование). Режим доступа: http://znanium.com/bookread.php?book=232661. - Заглавие с экрана.- ISBN 978-5-16-004858-1.

4. Васильков, А.В. Безопасность и управление доступом в информационных системах [Электронный ресурс]: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.(Профессиональное образование). - Режим доступа: http://znanium.com/bookread.php?book=405313.- Заглавие с экрана. ISBN 978-5-91134-360-6.

5. Хорев, П.Б. Программно-аппаратная защита информации [Электронный ресурс]: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.: ил. Режим доступа: http://znanium.com/bookread.php?book=489084 – Заглавие с экрана. - ISBN 978-5-00091-004-7.

6. Грибунин, В.Г. Комплексная система защиты информации на предприятии [Текст]: учеб. пособие/ В.Г. Грибунин. – М.: Академия, 2009. –416 с. - ISBN 978-5-7695-5448-3.

в) Программное обеспечение и Интернет-ресурсы:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.

3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД".http://www.osp.ru/os/– Загл. с экрана. Яз. рус.

5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.

6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. Яз. рус.

7. Компьютерра: все новости про компьютеры, железо, новые технологии, информационные : периодич. интернет-изд. URL: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория	Мультимедийные средства хранения, передачи и представления информации
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	K Комплект учебного оборудования «Криптографические системы» K Комплект учебного оборудования «Сетевая безопасность» SECURITY-CISCO-3M K Комплект учебного оборудования «Беспроводные компьютерные сети ЭВМ» K Модуль «Низкоуровневый контроллер Ethernet» K Комплекс средств защиты информации ViPNet: криптошлюз и межсетевой экран (3шт)
Компьютерный класс 372-2,3	Персональные компьютеры с пакетом MS Office и выходом в Интернет