МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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
«15» марта 2017 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
2017 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)

«03» марта 2017 г., протокол № 10.

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

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

«14» марта 2017 г., протокол № 6.

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 20.09.2017	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 20.09.2017	
3.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
4.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
5.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
6.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
7.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
8.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

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 вариативную часть учебного плана образовательной программы.

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

Информа ка
ти

Организация ЭВМ и вычислительных систем

Сети и системы передачи информации

Безопасность сетей ЭВМ

Безопасность операционных систем

Разработка и эксплуатация защищенных автоматизированных систем

Управление информационной безопасностью

Моделирование угроз информационной безопасности

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

Защита электронного документооборота

Информационная безопасность систем организационного управления

Методы проектирования защищенных распределенных информационных систем

Производственная-преддипломная практика

Научно-исследовательская работа

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:

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	- Создавать защищенные вычислительные сети с применением виртуализации; - 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 информационной безопасности	
Знать	-Информационно-технологические ресурсы автоматизированных систем; -Базовые правила построения виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности.
Уметь	-Создавать виртуальные сети для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности; -Конфигурировать сетевое оборудование в соответствии с проектом виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности.
Владеть	-Навыками настройки сетевого оборудования с учетом требований информационной безопасности для эффективного применения информационно-технологических ресурсов автоматизированной системы; -Навыками развертывания виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы.
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; -Основы удаленного администрирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.

Уметь	- Создавать 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, объём и содержание дисциплины (модуля)

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

– контактная работа – 106,85 акад. часов:

– аудиторная – 102 акад. часов;

– внеаудиторная – 4,85 акад. часов

– самостоятельная работа – 37,45 акад. часов;

– подготовка к экзамену – 35,7 акад.

часа Форма аттестации - экзамен

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. голосовые VLAN. Понятие транка. Стандарт 802.1q. Тэгирование Ethernet.	9	4		4/2И	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-10, ПК-24, ПСК-7.4
1.2 Настройка VLAN на коммутаторах. Конфигурирование транковых портов. Поиск неисправностей при использовании VLAN.		4		4/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Организация магистрального соединения при помощи транковых портов»	ПК-10, ПК-24, ПСК-7.4

1.3 Модели Router-on-a-Stick и многоуровневой коммутации. Конфигурация маршрутизации между VLAN. Поиск неисправностей в маршрутизации между VLAN.		4		4/2 И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Организация маршрутизации между VLAN»	ПК-10, ПК-24, ПСК-7.4
Итого по разделу		12		12/ 6И	6			
2. Виртуальные частные сети (VPN). Сетевые технологии Site-to-site VPN, FlexVPN и SSL VPN. Настройка и исполь-зование Cisco AnyConnect VPN.								

2.1 Задачи VPN-технологий. Защита от угроз для WAN-соединений и безопасность удалённого доступа. Основные компоненты VPN-технологии.	9	3		3/1И	1	Самостоятельная работа с интернет-источниками и учебно-методической литературой	Устный опрос	ПК-10, ПК-24, ПСК-7.4
2.2 Протоколы работы VPN: GRE, PPTP, L2TP, PPPoE. Конфигурирование соединения		3		3/1И	1	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Развертывание и конфигурирование PPTP-сервера»	ПК-10, ПК-24, ПСК-7.4
2.3 Протокол ISAKMP. Технология IPSec, Совместная работа IPSEC и NAT. Транзитная передача шифрованного трафика.		3		3/1И	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-10, ПК-24, ПСК-7.4
2.4 Dynamic VPN, конфигурирование функций динамического VPN-концентратора. Конфигурирование сервиса DynDNS.		3		3/1И	2	Самостоятельная работа с интернет- источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Конфигурирование VPN на базе маршрутизаторов CISCO»	ПК-10, ПК-24, ПСК-7.4
2.5 Конфигурирование классического туннельного соединения для объединения офисных сетей. Развёртывание DMVPN		4		4/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой.	Практическая работа «Конфигурирование VPN на базе маршрутизаторов	ПК-10, ПК-24, ПСК-

на устройствах с Cisco IOS. IPSec VPN с использованием SDM.						Подготовка к практическому занятию	CISCO»	7.4
2.6 Технология FlexVPN. Основные преимущества и возможности технологии FlexVPN.. Централизованное конфигурирование узлов-участников.		3		3/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Конфигурирование VPN на базе маршрутизаторов CISCO»	ПК-10, ПК-24, ПСК-7.4

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		3		3/1И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой.Под готовка к практическому занятию	Практическая работа «Настройка SSL VPN на CISCO ASA»	ПК-10, ПК-24, ПСК-7.4
2.8 Настройка и использование Cisco AnyConnect VPN. Мониторинг работы AnyConnect VPN. Настройка специфических аспектов работы AnyConnect VPN.		3		3/2И	2	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Управление CISCO ASA при помощи CISCO ASDM»	ПК-10, ПК-24, ПСК-7.4
Итого по разделу		25		25/10И	14			
3. Облачные технологии виртуальных сетей.								
3.1 Характеристики аппаратно-программных платформ виртуализации для построения виртуальных сетей. Характеристики облачных провайдеров для построения виртуальных инфраструктур IaaS	9	3		3/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-10, ПК-24, ПСК-7.4
3.2 Построение в облаке изолированной виртуальной подсети для связи между виртуальными машинами.		3		3/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-10, ПК-24, ПСК-7.4

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	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-10, ПК-24, ПСК-7.4
3.4 Реализации сетевой безопасности в облаке VMware vShield, Cisco Adaptive Security Appliance (ASA).		2		2/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-10, ПК-24, ПСК-7.4

3.5 Создание VPN-серверов для виртуальных частных сетей в облаке.		2		2/1И	3	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к компьютерному тестированию	Компьютерное тестирование	ПК-10, ПК-24, ПСК-7.4
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	2,45	Самостоятельная работа с интернет-источниками и учебно-методической литературой. Подготовка к практическому занятию	Практическая работа «Организация ЛВС с VLAN»	ПК-10, ПК-24, ПСК-7.4
Итого по разделу		14		14/6И	17,45			
4. Экзамен								
4.1 Подготовка к экзамену	9					Самостоятельная работа с интернет-источниками и учебно-методической литературой		ПК-10, ПК-24, ПСК-7.4
Итого по разделу								
Итого за семестр		51		51/22И	37,45		экзамен	
Итого по дисциплине		51		51/22И	37,45		экзамен	ПК-10,ПК-24,ПСК-7.4

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 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.

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. Антивирусная защита в вычислительной сети.
2. Программное обеспечение, предназначенное для поиска и анализа уязвимостей в сетях ЭВМ.
3. Виртуальные частные сети (VPN). Виртуальные защищенные сети. Принципы построения, использование технологии VPN в контексте построения безопасной вычислительной сети.
4. Беспроводные сети. Основные принципы работы, основные уязвимости и методы их устранения.
5. Протокол VTP. Какие существуют режимы работы протокола VTP?
6. Как настроить VTP протокол на коммутаторе? Достоинства протокола VTP.
7. Какие могут быть неисправности при настройке VLAN? Как их искать?
8. Назначение и принцип работы динамического протокол инициализации транка (DTP)
9. Опишите архитектуру Router-on-a-Stick
10. FlexVPN технология соединения сетей. Назначение протокола IKEv2
11. PPTP, L2TP, PPPoE соединения и их отличия.
12. Набор протоколов для обеспечения защиты данных передаваемых по сетевому протоколу в виртуальных частных сетях(IPSec)
13. Совместная работа IPSec и NAT. Основные проблемы при настройке.
14. Механизмы аутентификация для VPN
15. ESP, AH протоколы и их отличия.
16. Выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, сежсетевой экран) для построения разработанной топологии сети соблюдая требования по защите информации;

17. 2.Реализовать разработанную политику сетевой безопасности при настройке и конфигурированию сетевого оборудования.
18. 3. Разработать документация о переводе исходного состояния сети в текущее в соответствии с поставленной задачей

Практическая работа «Организация магистрального соединения при помощи транковых портов»

Выполнить:

1. Построение сети и настройка базовых параметров устройства
2. Создание виртуальных локальных сетей и назначение портов коммутатора
3. Поддержка назначения портов VLAN и базы данных VLAN
4. Конфигурация транкового канала стандарта 802.1Q между коммутаторами

Практическая работа «Построение VPN-соединения на базе протокола IPSEC на базе маршрутизаторов CISCO»

Выполнить:

1. Построение сети и настройка базовых параметров устройства
2. Конфигурацию ASA. Настройка интерфейсов. Настройка политики
3. Настройку интерфейса командой строки маршрутизатора IOS

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 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	Перечень вопросов: 1. Для чего нужны VLAN сети? Характеристики и особенности таких сетей. 2. Транковое соединение выполняет какую роль и какой протокол тегирует пакеты для этого соединения? 3. Протокол VTP. Какие существуют режимы работы протокола VTP? 4. Как настроить VTP протокол на коммутаторе? Достоинства протокола VTP. 5. Какие могут быть неисправности при настройке VLAN? Как их искать? 6. Назначение и принцип работы динамического протокол инициализации транка (DTP) 7. Опишите архитектуру Router-on-a-Stick 8. FlexVPN технология соединения сетей. Назначение протокола IKEv2 9. PPTP, L2TP, PPPoE соединения и их отличия. 10. Набор протоколов для обеспечения защиты данных передаваемых по сетевому протоколу в виртуальных частных сетях(IPSec) 11. Совместная работа IPSec и NAT. Основные проблемы при настройке. 12. Механизмы аутентификация для VPN

		13. ESP, AH протоколы и их отличия. 14. Динамический и статический VTI. Основные настройки параметров. 15. Как работает GRE и NHRP? 16. Назовите основные этапы настройки SSL VPN для удаленного подключения. 17. Назначение и принцип работы межсетевого экрана в виртуальных частных сетях
Уметь	- Создавать защищенные вычислительные сетей с применением виртуализации; - Применять технологии и средства защиты информации для обеспечения безопасности информации в вычислительных сетях.	1. Выполнить 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. Разработать политику аутентификации пользователей специализированных виртуальных сетей в облачных сетевых структурах 4. Произвести конфигурирование SSL для виртуальных локальных сетей и виртуальных частных сетей согласно поставленной задаче
Владеть	- Навыками разработки, внедрения и документирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах, с учетом требований по обеспечению безопасности.	1. Выполнить настройку сетевого оборудования (коммутатор, маршрутизатор, сежсетевой экран) для построения разработанной топологии сети соблюдая требования по защите информации; 2.Реализовать разработанную политику сетевой безопасности при настройке и конфигурированию сетевого оборудования. 3. Разработать документация о переводе исходного состояния сети в текущее в соответствии с поставленной задачей 4. Разработать документацию о внедрении специализированных виртуальных сетей в корпоративную сеть предприятия 5. Разработать журнал настроек для заданных 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 информационной безопасности		
Знать	-Информационно-технологические ресурсы автоматизированных систем -Базовые правила построения виртуальных сетей для обеспечения эффективного	Перечень вопросов: 1. Информационно-технологические ресурсы автоматизированных систем. Состав и назначение. 2. Уязвимости информационно-технологических ресурсов автоматизированных систем 3. Информационно-коммуникационные технологии в информационно-технологические ресурсы автоматизированных систем. Обеспечение требований информационной безопасности. 4.Протокол заголовка идентификации АН. Обеспечение

	применения информационно-технологи ческих ресурсов автоматизированной системы с учетом требований	целостности защищенной части пакета данных 5. Инкапсулирующий протокол безопасности ESP.

	информационной безопасности	Режим транспорта и инкапсуляции 6. IKE протокол. Обмен ключами между узлами VPN 7. Способ идентификации узла в виртуальных частных сетях 8. Организация VPN-туннеля и его шифрование 9. Криптографические карты общедоступных интерфейсов 10. Организация работы динамического VPN сервера 11. Применение виртуализации в частных сетях для обеспечения защиты информации ограниченного доступа 12. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика для обеспечения защиты информации ограниченного доступа? 13. Ключевые аспекты построения набора правил межсетевого экрана 14. Система обнаружения и предотвращения вторжений IDS/IPS. 15. Основные варианты организации виртуальных частных сетей 16. Протоколы формирования каналов для защиты информации ограниченного доступа передаваемой по сети 17. Согласование параметров защищенных каналов и распределение криптографических ключей
Уметь	- Создавать виртуальные сети для обеспечения эффективного применения информационно-технологи ческих ресурсов автоматизированной системы с учетом требований информационной безопасности -Конфигурировать сетевое оборудование в соответствии с проектом виртуальных сетей для обеспечения эффективного применения информационно-технологи ческих ресурсов автоматизированной системы с	1. Выполнить конфигурированиеVPN концентратора для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности 2. Определить настройки ACL в соответствии с поставленной задачей для виртуальных локальных компьютерных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах . 3. Создать виртуальную сеть с применением динамического VPN сервера, учитывая требования информационной безопасности 4. Произвести анализ сети программными сканерами сетевых протоколов и сетевых уязвимостей (например, свободно распространяемые сканеры WireShark и Ethereal) 5. Настроить протокол обмена ключами для установки автоматического VPN соединения в виртуальных сетях обеспечивающих эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом

	учетом требований информационн ой безопасности	
Владеть	- Навыками настройки сетевого оборудования с учетом требований информационной безопасности для	1. Выполнить настройку систем обнаружения и предотвращения вторжений IPS/IDS для виртуальных локальных сетей, обеспечивающих эффективное применение информационно-технологических ресурсов

	эффективного применения информационно-технологических ресурсов автоматизированной системы -Навыками развертывания виртуальных сетей для обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы	автоматизированной системы 2. Настроить Native VLAN внутри виртуальной локальной сети для защиты от атак двойного тегирования 3. Создать виртуальную сеть для обмена данными, настроить SPAN и выполнить мониторинг трафика 4. Выполнить настройку Site-to-Site GRE туннеля для локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. 5. Создать виртуальную сеть и выполнить объединение настроек IPSec используя crypto map. Произвести отладку и мониторинг процесса установления соединения.
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. -Основы удаленного администрирования виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.	Перечень вопросов: 1. Межсетевая операционная система Cisco IOS 2. Командные режимы CLI Cisco IOS 2. Система аутентификации, авторизации и учета событий, встроенная в операционную систему Cisco IOS 3. Настройка и использование Cisco AnyConnect VPN. 4. Предоставление удаленного доступа с использованием протокола SSH 5. Линии виртуальных терминалов VTY для удаленного административного доступа 6. Настройка hostname и доменное имя для удаленного доступа SSH 7. Генерирование ключей и создание учетных записей пользователей SSH 8. Разграничение ролей с помощью уровня привилегий 9. Присваивание команд к уровням привилегий 10. Система доступа на уровне ролей 11. Резервное копирование и восстановление конфигурации Cisco IOS 12. Средства удаленного мониторинга виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах. 13. Аутентификация с помощью сервера RADIUS 14. Учет выполняемых действий учетной записи виртуальных локальных сетей и виртуальных частных сетей, а также специализированных виртуальных сетей в облачных сетевых структурах.

Уметь	- Создавать и администрировать виртуальные локальные сети и виртуальные частные сети, а также специализированные виртуальные сети в облачных сетевых структурах. - Реализовывать политику	1. Выполнить проектирование виртуальной локальной сети и виртуальной частной сети в соответствии с политикой безопасности. 2. Разработать политику безопасности для удаленного администрирования виртуальной локальной сети и виртуальной частной сети, а также специализированной виртуальной сети в облачных сетевых структурах.

	безопасности виртуальной локальной сети и виртуальной частной сети, а также специализированной виртуальной сети в облачных сетевых структурах. - Пользоваться сетевыми средствами виртуальных сетей для обмена данными, в том числе с использованием глобальной информационной сети Интернет.	3. Используя сетевые средства виртуальных сетей для обмена данными, произвести резервное копирование конфигурации 4. Выполнить учет выполняемых действий учетной записи виртуальных локальных сетей и виртуальных частных сетей, а также
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;	1. Выполнить разграничение ролей с помощью уровня привилегий и присвоить команды к уровням привилегий 2. Настроить виртуальный терминал VTY для удаленного административного доступа 3. Произвести настройку удаленного доступа с применением SSH 4. Произвести настройку аудита действий пользователя с помощью стандартных средств обмена в виртуальных локальных сетях

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, 020. —363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450234 (дата обращения: 12.03.2020).

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: 12.03.2020).

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: 12.03.2020).

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: 12.03.2020).

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.znanium.com/catalog/product/1088143 (дата обращения: 26.02.2020)

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: 22.10.2019). - 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)

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 Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
Kaspersky Endpoint Security для бизнеса-Стандарт	Д-300-18 от 21.03.2018	28.01.2020
7Zip	свободно распространяемое ПО	бессрочно
MS Office Access Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
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
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка

Международная справочная система «Полпред» polpred.com отрасль «Образование, наука»	URL: http://education.polpred.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория Мультимедийные средства хранения, передачи и представления информации

Лаборатория сетей и систем передачи данных. 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.(2 шт)
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"(2шт. cisco и d-link)
6. Комплект учебного оборудования "Беспроводные компьютерные сети ЭВМ"
7. Модуль учебно-лабораторный для изучения низкоуровнего контроллера Ethernet
8. Стенд коммуникационного оборудования сервером для моделирования облачного сервиса
9. Комплекс программно-аппаратный ViPNet

Компьютерный класс - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

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

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Рекомендации направлены на оказание методической помощи студентам при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;

- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности студентов к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения в компьютерном классе и противопожарным мерам.
2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы студент демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ ПО ДИСЦИПЛИНЕ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов по дисциплине «Информатика и информационные технологии» и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Особенностью изучения дисциплины «Информатика» является освоение теоретического материала и получение практических умений, направленных на использование современных информационных технологий.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины (модуля)» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.

3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований и к решению олимпиадных заданий.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: защита реферата, индивидуальные домашние задания, аудиторные контрольные работы, компьютерное тестирование, участие в конкурсах и олимпиадах.

Максимальное количество баллов обучающийся получает, если:

- выполняет ИДЗ в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.