

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 апреля 2020 г.

Кафедра «Вычислительные системы, сети и информационная
безопасность»

Автор Желенков Борис Владимирович, к.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации в вычислительных сетях

Направление подготовки: 09.03.01 – Информатика и вычислительная
техника

Профиль: Вычислительные системы и сети

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки 2020

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">Н.А. Клычева</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 15 27 апреля 2020 г. Заведующий кафедрой</p>  <p style="text-align: right;">Б.В. Желенков</p>
---	---

Рабочая программа учебной дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: Заведующий кафедрой Желенков Борис
Владимирович
Дата: 27.04.2020

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Защита информации в вычислительных сетях» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих.

Студенты должны научиться применять современные средства защиты информации предоставляемые сетевым оборудованием, являющимся самым уязвимым местом при попытке несанкционированного доступа.

Основными задачами дисциплины являются:

- Ознакомление с основными терминами и определениями.
- Ознакомление с основными типами угроз и атак.
- Изучение механизмов защиты административного интерфейса и разграничения прав доступа.
- Изучение технологии AAA.
- Изучение способов защиты информации в сетях.
- Изучение принципов построения виртуальных частных сетей.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Организационно-управленческая

- разработка политики информационной безопасности
- разработка регламентов и аудит системы безопасности данных
- контроль использования сетевых устройств и программного обеспечения
- оценка производительности сетевых устройств и программного обеспечения
- администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Производственно-технологическая

- осуществляет разработку тестовых документов, включая план тестирования
- разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным
- разработка архитектуры ИС
- коррекция производительности сетевой инфокоммуникационной системы
- установка специальных средств управления безопасностью администрируемой сети

Проектная

- планирование восстановления сетевой инфокоммуникационной системы
- планирование модернизации сетевых устройств
- разработка тестовых программ или генераторов тестовых программ для модели ИС на языках программирования целевой системы

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Защита информации в вычислительных сетях" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Маршрутизация и глобальные сети:

Знания: принципы работы маршрутизаторов и их основные задачи, способы маршрутизации, технологий глобальных сетей

Умения: настраивать протоколы маршрутизации, резервирования шлюзов, выполнять фильтрацию трафика

Навыки: построения распределенных сетей с различными задачами и принципами маршрутизации

2.1.2. Основы сетевых технологий:

Знания: принципы работы сетевых протоколов и сетевых устройств, классификацию сетевого оборудования, методы и системы моделирования работы сети, сетевого оборудования и протоколов, характеристики сетевого оборудования различных уровней, современные элементы архитектуры вычислительных сетей, протоколы и особенности их совместного использования, понимать принципы функционирования программно-аппаратного комплекса.

Умения: оформлять документацию по СКС, настраивать сетевое оборудование в соответствии с решаемыми задачами, применять необходимые сетевые протоколы, выбирать необходимое оборудование для проведения экспериментов и формализовывать полученные результаты, рассчитывать необходимые ресурсы для монтажа и определять методы поиска неисправностей в процессе настройки и отладки работы сети

Навыки: навыками систематизации информации и формулирования задач при эксплуатации СКС, конфигурирования сетевого оборудования для работы в сети, навыками описания результатов и формулированию выводов о результатах экспериментов, корректности и эффективности использования необходимых аппаратно-программных средств, навыками использования монтажного оборудования и программно-аппаратных отладочных средств для введения сети в эксплуатацию, навыками формирования спецификации для вычислительной сети и прогнозирования изменения состояния сети при увеличении нагрузки.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Преддипломная практика

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПКР-3 Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.	<p>ПКР-3.1 Знать общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети; инструкции по установке администрируемых сетевых устройств; инструкции по эксплуатации администрируемых сетевых устройств; инструкции по установке администрируемого программного обеспечения; инструкции по эксплуатации администрируемого программного обеспечения; протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; модель ISO для управления сетевым трафиком; модели IEEE; защищенные протоколы управления; основные средства криптографии; регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе; требования охраны труда при работе с сетевой аппаратурой администрируемой сети.</p> <p>ПКР-3.2 Уметь подключать и настраивать современные межсетевые экраны; пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; работать с контрольно-измерительными аппаратными и программными средствами.</p> <p>ПКР-3.3 Владеть навыками параметризации операционных систем средств удаленного доступа; установки дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация; настройки средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов); документирования настроек средств обеспечения безопасности удаленного.</p>

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

4 зачетные единицы (144 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 8
Контактная работа	64	64,15
Аудиторные занятия (всего):	64	64
В том числе:		
лекции (Л)	32	32
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	32	32
Самостоятельная работа (всего)	35	35
Экзамен (при наличии)	45	45
ОБЩАЯ трудоемкость дисциплины, часы:	144	144
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	4.0	4.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ТК	ТК
Виды промежуточной аттестации (экзамен, зачет)	Экзамен	Экзамен

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Всего	Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР			
1	2	3	4	5	6	7	8	9	10	
1	8	Раздел 1 Защита информации.	2				2	4		
2	8	Тема 1.1 Основные термины и определения Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. Рассматриваются основные направления действия системы защиты информации и принципы ее организации.	2					2		
3	8	Раздел 2 Политика защиты	6	6			10	22		
4	8	Тема 2.1 Сетевая безопасность Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты.	2				2	4		
5	8	Тема 2.2 Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними.	2				4	6		
6	8	Тема 2.3 Вирусы. Описываются типы вирусов, среда обитания, способы	2	6			4	12		

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		заражения, вредоносное воздействие							
7	8	Раздел 3 Защита сети.	6	10			8	24	
8	8	Тема 3.1 Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий.	2	6			2	10	
9	8	Тема 3.2 Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации. Приводятся методы ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика.	2				2	4	
10	8	Тема 3.3 Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и	2	4			4	10	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		конфигурирования.							
11	8	Раздел 4 Защита сетевых соединений	8	6			6	20	
12	8	Тема 4.1 Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки.	2					2	ТК, Вып. лаб. работ №1-3
13	8	Тема 4.2 Защита периметра сети. Описывается зонная архитектура защиты сети и ее компоненты.	2				2	4	
14	8	Тема 4.3 Контроль сервисов ТСП/IP. Рассматриваются средства контроля сервисов ТСП/IP на уровне глобальной конфигурации и конфигурации интерфейсов.	2				2	4	
15	8	Тема 4.4 Контроль доступа. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, СВАС и их конфигурация, а также настройка средств защиты от синхронных атак.	2	6			2	10	
16	8	Раздел 5 Шифрование.	6	4			5	15	
17	8	Тема 5.1 Механизмы шифрования Рассматриваются различные варианты построения систем шифрования и их свойства.	2					2	
18	8	Тема 5.2	2				3	5	,

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA.							Вып. лаб. работ №4-5
19	8	Тема 5.3 Шифрование на сетевом уровне Приводится обзор задач и средств шифрования на сетевом уровне.	2				2	4	
20	8	Раздел 6 Построение виртуальных частных сетей с использованием IPSec.	4	6			4	59	
21	8	Тема 6.1 Обзор технологии виртуальных частных сетей. Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки.	1				2	3	
22	8	Тема 6.2 Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE.	1					1	
23	8	Тема 6.3 Настройка IPSec VPN. Описывается настройка политики ISAKMP,	2	6			2	10	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу- точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		определение наборов преобразований IPSec и настройка криптографических карт.							
24	8	Экзамен						45	Экзамен
25		Всего:	32	32			35	144	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 32 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	8	РАЗДЕЛ 2 Политика защиты Тема: Вирусы.	Лабораторная работа №1 Вирусы.	6
2	8	РАЗДЕЛ 3 Защита сети. Тема: Защита административного доступа к сетевым устройствам.	Лабораторная работа №2. Защита административного доступа и связи между маршрутизаторами.	6
3	8	РАЗДЕЛ 3 Защита сети. Тема: Технология защиты AAA.	Лабораторная работа №3. Настройка системы защиты AAA.	4
4	8	РАЗДЕЛ 4 Защита сетевых соединений Тема: Контроль доступа.	Лабораторная работа №4. Защита периметра сети с помощью средств контроля доступа.	6
5	8	РАЗДЕЛ 5 Шифрование.	Лабораторная работа №5. Изучение методов шифрования.	4
6	8	РАЗДЕЛ 6 Построение виртуальных частных сетей с использованием IPSec. Тема: Настройка IPSec VPN.	Лабораторная работа №6. Конфигурирование VPN соединения	6
ВСЕГО:				32/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовой проект учебным планом не предусмотрен

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Защита информации в вычислительных сетях» осуществляется в форме лекций и лабораторных работ.

Лекции проводятся в традиционной классно-урочной организационной форме в объеме 24 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).

Лабораторные работы организованы с использованием технологий развивающего обучения.

Курс лабораторных работ (24 часов) проводится с использованием сетевого оборудования и на специальных программных симуляторах, разработанных на кафедре, основанных на интерактивных (диалоговых) технологиях, в том числе на сетевом оборудовании (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы.

Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (38 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям, подготовка к интерактивным практическим и лабораторным работам.

Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически заверченный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	8	РАЗДЕЛ 1 Защита информации.	Изучение терминологии 1 [стр. 4-93], 2 [стр. 6-46] ГОСТ Р 50922-2006	2
2	8	РАЗДЕЛ 2 Политика защиты Тема 1: Сетевая безопасность	Изучение видов политик защиты и проведение их сравнительного анализа. 1 [стр. 95-100], 2 [стр. 70-110]	2
3	8	РАЗДЕЛ 2 Политика защиты Тема 2: Анализ угроз безопасности.	Изучение типов угроз и проведение их сравнительного анализа 1 [стр. 95-100], 2 [стр. 70-110]	4
4	8	РАЗДЕЛ 2 Политика защиты Тема 3: Вирусы.	Разработка сценария работы вируса, написание программы-вируса и антивируса. 1 [стр. 95-100], 2 [стр. 70-110]	4
5	8	РАЗДЕЛ 3 Защита сети. Тема 1: Защита административного доступа к сетевым устройствам.	Изучение способов формирования парольной защиты. 2 [стр. 111-120]	2
6	8	РАЗДЕЛ 3 Защита сети. Тема 2: Защита связи между маршрутизаторами.	Изучение механизмов протоколов маршрутизации, обеспечивающих аутентификацию и их сравнительный анализ. 2 [стр. 111-120]	2
7	8	РАЗДЕЛ 3 Защита сети. Тема 3: Технология защиты AAA.	Сравнение серверов AAA 2 [стр. 111-120]	4
8	8	РАЗДЕЛ 4 Защита сетевых соединений Тема 2: Защита периметра сети.	Проведение сравнительного анализа моделей обороны. Анализ зонных архитектур 1 [стр. 100-111]	2
9	8	РАЗДЕЛ 4 Защита сетевых соединений Тема 3: Контроль сервисов TCP/IP.	Анализ уязвимостей сервисов TCP/IP. 1 [стр. 100-111]	2
10	8	РАЗДЕЛ 4 Защита сетевых соединений Тема 4: Контроль доступа.	Анализ работы контекстных списков доступа с протоколом TCP и UDP. 1 [стр. 100-111]	2
11	8	РАЗДЕЛ 5 Шифрование. Тема 2: Блочное шифрование и цифровая подпись.	Написание программ алгоритма шифрования DES. 3 [стр. 4-33]	3
12	8	РАЗДЕЛ 5	Анализ средств шифрования	2

		Шифрование. Тема 3: Шифрование на сетевом уровне	предоставляемых сетевым оборудованием. 3 [стр. 4-33]	
13	8	РАЗДЕЛ 6 Построение виртуальных частных сетей с использованием IPSec. Тема 1: Обзор технологии виртуальных частных сетей.	Сравнительный анализ технологии виртуальных частных сетей. 1 [стр. 112-140]	2
14	8	РАЗДЕЛ 6 Построение виртуальных частных сетей с использованием IPSec. Тема 3: Настройка IPSec VPN.	Выбор средств аутентификации и шифрования при построении VPN туннеля. 1 [стр. 112-140]	2
ВСЕГО:				35

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Основы построения опорных сетей ISP. Учебное пособие.	Желенков Б.В.	М.: МИИТ;147с. http://library.miit.ru/ , 2009	1 стр. 4-93,2 стр. 95-100,4 стр. 100-111,6 стр. 112-140
2	Проектирование кампусных сетей: Учебное пособие.	Голдовский Я.М.	М.: МИИТ;130с., http://library.miit.ru/ , 2009	1 стр. 6-46,2 стр. 70-110,3 стр. 111-120
3	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам.	Голдовский Я.М. Желенков Б.В. Сафонова И.Е.	М.: МИИТ;36с., http://library.miit.ru/ , 2013	5 стр. 4-33

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
-------	--------------	-----------	--------------------------------------	--

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- Форум специалистов по информационным технологиям <http://citforum.ru/>
- Интернет-университет информационных технологий <http://www.intuit.ru/>
- Тематический форум по информационным технологиям <http://habrahabr.ru/>

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

- Foxit Reader/Acrobat Reader
- Microsoft Office (Power Point)
- Установлен мультимедийный курс лекций.

Для проведения практических занятий необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

- Foxit Reader/Acrobat Reader
- Microsoft Office (Word).

На рабочие места должны быть установлены программные разработки кафедры

«Вычислительные системы и сети»:

- Обучающая система «netlab»

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№1327 Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, межсетевой экран Cisco, сетевое оборудование, АПКШ Континент ЦУС-СД – 2шт, АПКШ «Континент» Криптошлюз – 2шт, Идентификатор Rutoken ЭЦП – 6 шт., ПАК Соболь – 5 шт., ПАК ViPNet xFirewall 100– 1шт., ПАК ViPNet xFirewall 1000– 1шт., ПАК ViPNet Coordinator HW 100 – 2шт., ПАК ViPNet Coordinator HW 1000 – 1шт., ПАК ViPNet IDS NS 100 – 1шт., ПАК ViPNet IDS NS 1000 -1шт., рабочая станция преподавателя, проектор, экран.

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе.

Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления. Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций:

- познавательно-обучающая;
- развивающая;
- ориентирующе-направляющая;
- активизирующая;
- воспитательная;
- организующая;
- информационная.

Выполнение лабораторных работ служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике.

Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение лабораторных работ не сводится только к органичному дополнению

лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Каждому студенту следует составлять еженедельный семестровый план работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были – по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной работы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к зачету и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит, как приложение, в состав рабочей программы дисциплины.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература.