

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

УТВЕРЖДАЮ:

Директор ИУЦТ



С.П. Вакуленко

30 сентября 2019 г.



Кафедра «Вычислительные системы, сети и информационная
безопасность»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 2 30 сентября 2019 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 № 2/а 27 сентября 2019 г. Заведующий кафедрой</p>  <p style="text-align: right;">Б.В. Желенков</p>
---	--

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Программно-аппаратные средства защиты информации» 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 аппаратно-программные 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 аппаратно-программной защиты сетевых соединений.
- Изучение принципов построения виртуальных частных сетей.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):

Эксплуатационная:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологическая:

- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов;

Экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств.

Организационно-управленческая деятельность:

- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;

- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.?

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Программно-аппаратные средства защиты информации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Информатика:

Знания: современное состояние уровня и направлений развития вычислительной техники и программных средств, основные алгоритмы типовых численных методов решения математических задач, один из языков программирования, структуру локальных и глобальных компьютерных сетей.

Умения: работать в качестве пользователя персонального компьютера, использовать внешние носители информации для обмена данными между машинами, создавать резервные копии данных и программ, использовать языки и системы программирования, работать с программными средствами общего назначения; использовать основные приемы обработки экспериментальных данных, подготовить проектно-конструкторскую документацию разрабатываемых изделий и устройств с применением электронно-вычислительных машин.

Навыки: методами поиска и обмена информацией в глобальных и локальных компьютерных сетях, техническими и программными средствами защиты информации при работе с компьютерными сетями, включая навыками работы с программными средствами общего назначения, соответствующими со-временным требованиям мирового рынка, включая приемы антивирусной защиты.

2.1.2. Компьютерные сети:

Знания: принципы работы сетевых протоколов и сетевых устройств, классификацию сетевого оборудования.методы и системы моделирования работы сети, сетевого оборудования и протоколовсовременные элементы архитектуры вычислительных сетей

Умения: оформлять документацию по СКСрассчитывать 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 навыками использования монтажного оборудования и программно-аппаратных отладочных средств для введения сети в эксплуатацию

2.1.3. Сети и системы передачи информации:

Знания: принципы работы сетевых протоколов и сетевых устройств, классификацию сетевого оборудования.методы и системы моделирования работы сети, сетевого оборудования и протоколовсовременные элементы архитектуры вычислительных сетей

Умения: оформлять документацию по СКСрассчитывать 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 навыками использования монтажного оборудования и программно-аппаратных отладочных средств для введения сети в эксплуатацию

2.1.4. Электроника:

Знания: основные законы естественнонаучных дисциплин; сущность и основные свойства информации, основные методы и средства получения, хранения и переработки информации; технические характеристики и экономические показатели отечественных и зарубежных образцов программно-технических комплексов и систем управления; положения нормативных документов в соответствии с которыми разрабатывается проектная документация

Умения: использовать упомянутые законы в профессиональной деятельности, применять на практике методы математического анализа, моделирования, теоретического и экспериментального исследования; выбрать оптимальный метод и средство получения, хранения и переработки информации применительно к условиям поставленной задачи; изменять, дополнять, адаптировать, развивать методы, алгоритмы, средства, решения, приемы, методики для решения конкретных задач; разрабатывать проектную документацию в соответствии с имеющимися стандартами и техническими условиями.

Навыки: методами математического анализа и моделирования, теоретического и экспериментального исследования; основными методами, способами и средствами получения, хранения, переработки информации; навыками сбора и анализа исходных данных для расчета и проектирования систем и средств автоматизации и управления; навыками использования средств автоматизированного проектирования при разработке проектной документации.

2.2. Наименование последующих дисциплин

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	ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	<p>Знать и понимать: понятия информационной безопасности, составные элементы подсистем и их характеристики, правила эксплуатации используемых подсистем информационной безопасности, методы и средства конфигурирования и контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами.</p> <p>Уметь: контролировать работу подсистем и изменять конфигурационные параметры при необходимости, применять методы и средства контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами, находить наиболее уязвимые места в системе, оценивать возможные вредоносные действия и решать задачи по минимизации вредоносных воздействий.</p> <p>Владеть: навыками по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации, прогнозирования поведения подсистемы информационной безопасности объекта при изменении внешних воздействий; навыками эксплуатации подсистем управления информационной безопасностью предприятия построенных с использованием современного оборудования.</p>
2	ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	<p>Знать и понимать: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации.</p> <p>Уметь: проверять работоспособность элементов системы защиты с помощью необходимых технических средств</p> <p>Владеть: навыками интерпретировать полученные результаты для получения оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</p>
3	ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	<p>Знать и понимать: основные принципы формального представления информации, понятия информационной безопасности, составные элементы подсистем и их характеристики.</p> <p>Уметь: искать и анализировать информацию, четко ставить цель и последовательно добиваться ее осуществления, определять уязвимости объектов защиты; осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов</p>

№ п/п	Код и название компетенции	Ожидаемые результаты
		Владеть: навыками поиска и анализа информации, определения взаимосвязи явлений и объектов; навыками составления обзора по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

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

4.1. Общая трудоемкость дисциплины составляет:

5 зачетных единиц (180 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 7
Контактная работа	56	56,15
Аудиторные занятия (всего):	56	56
В том числе:		
лекции (Л)	28	28
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	28	28
Самостоятельная работа (всего)	70	70
Экзамен (при наличии)	54	54
ОБЩАЯ трудоемкость дисциплины, часы:	180	180
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	5.0	5.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

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	7	Раздел 1 Защита информации.	2				4	6		
2	7	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				4	6		
3	7	Раздел 2 Политика защиты.	6	4/2			12	22/2		
4	7	Тема 2.1 Сетевая безопасность Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты.	2				4	6		
5	7	Тема 2.2 Анализ угроз безопасности Описываются типы угроз и общие рекомендации по борьбе с ними.	2				4	6		
6	7	Тема 2.3 Вирусы. Описываются типы вирусов, среда обитания, способы	2	4/2			4	10/2		

№ 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	7	Раздел 3 Защита сети.	6	8/2			17	31/2	
8	7	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				4	6	
9	7	Тема 3.2 Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика.	2	4/2			4	10/2	
10	7	Тема 3.3 Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования	2	4			9	15	ПК1, Выполнение лаб. работ 20%

№ 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
11	7	Раздел 4 Защита сетевых соединений	6	4/2			16	26/2	
12	7	Тема 4.1 Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки.					4	4	
13	7	Тема 4.2 Защита периметра сети Описывается зонная архитектура защиты сети и ее компоненты.	2				4	6	
14	7	Тема 4.3 Контроль сервисов TCP/IP Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов.	2				4	6	
15	7	Тема 4.4 Контроль доступа по ACL. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа.	1					1	
16	7	Тема 4.5 Контроль доступа по СВАС Описываются средства контроля доступа с СВАС и их конфигурация, а также настройка средств защиты от синхронных атак.	1	4/2			4	9/2	
17	7	Раздел 5 Шифрование.	6	10/3			13	29/3	
18	7	Тема 5.1 Механизмы шифрования. Рассматриваются	2					2	

№ 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
		различные варианты построения систем шифрования и их свойства.							
19	7	Тема 5.2 Блочное шифрование. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES.	1				4	5	
20	7	Тема 5.3 Блочное шифрование. Рассматривается алгоритм шифрования AES, ГОСТ 28147, RSA RC5.	1	10/3				11/3	
21	7	Тема 5.4 Цифровая подпись. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA.	1					1	ПК2, Выполнение лаб. работ 80%
22	7	Тема 5.5 Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне.	1				9	10	
23	7	Раздел 6 Построение виртуальных частных сетей с использованием IPSec.	2	2			8	12	
24	7	Тема 6.1 Обзор технологии виртуальных частных сетей Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки.					4	4	

№ 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	Всего		
1	2	3	4	5	6	7	8	9	10	
25	7	Тема 6.2 Механизмы IPSec. Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE.	1					1		
26	7	Тема 6.3 Настройка IPSec VPN. Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.	1	2			4	7		
27	7	Раздел 7 Итоговая аттестация						54	КР, ЭК	
28		Всего:	28	28/9			70	180/9		

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 28 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	7	РАЗДЕЛ 2 Политика защиты. Тема: Вирусы.	Вирусы.	4 / 2
2	7	РАЗДЕЛ 3 Защита сети. Тема: Защита связи между маршрутизаторами.	Защита административного доступа и связи между маршрутизаторами.	4 / 2
3	7	РАЗДЕЛ 3 Защита сети. Тема: Технология защиты AAA.	Настройка системы защиты AAA.	4
4	7	РАЗДЕЛ 4 Защита сетевых соединений Тема: Контроль доступа по СВАС	Защита периметра сети с помощью средств контроля доступа.	4 / 2
5	7	РАЗДЕЛ 5 Шифрование. Тема: Блочное шифрование.	Алгоритм шифрования DES	4
6	7	РАЗДЕЛ 5 Шифрование. Тема: Блочное шифрование.	Алгоритм шифрования RC5	2
7	7	РАЗДЕЛ 5 Шифрование. Тема: Блочное шифрование.	Шифрование с помощью временных ключей.	2 / 3
8	7	РАЗДЕЛ 5 Шифрование. Тема: Блочное шифрование.	Алгоритм электронной цифровой подписи шифрования DSA.	2
9	7	РАЗДЕЛ 6 Построение виртуальных частных сетей с использованием IPSec. Тема: Настройка IPSec VPN.	Конфигурирование VPN соединения.	2
ВСЕГО:				28/9

4.5. Примерная тематика курсовых проектов (работ)

Разработать защищенное пространство обработки и хранения данных.

Int traf Структура зоны AAA CBAC DYN REF TIME IPSec
ICMP 1 шлюз
2 шлюза AH ESP DES 3DES AES MD-5 SHA-1 PSK RSA
1 + Lok3 + + + + +
2 + Lok4 + + + + +
3 + Lok5 + + + + +
4 + Lok3 + + + + +
5 + Lok4 + + + + +
6 + Lok5 + + + + +
7 + Lok3 + + + + +
8 + Lok4 + + + + +
9 + Lok5 + + + + +
10 + Lok3 + + + + +
11 + Lok4 + + + + +
12 + Lok5 + + + + +

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Программно-аппаратные средства защиты информации» осуществляется в форме лекций и лабораторных работ.

Лекции проводятся в традиционной классно-урочной организационной форме в объеме 28 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).

Лабораторные работы организованы с использованием технологий развивающего обучения.

Курс лабораторных работ (28 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 (70 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.

Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):

- использование современных средств коммуникации;
- электронная форма обмена материалами;
- дистанционная форма групповых и индивидуальных консультаций;
- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д.

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	7	РАЗДЕЛ 1 Защита информации. Тема 1: Основные термины и определения	Изучение терминологии. 1 [стр. 4-93], 2 [стр. 6-46] ГОСТ Р 50922-2006	4
2	7	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]	4
3	7	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	7	РАЗДЕЛ 2 Политика защиты. Тема 3: Вирусы.	Разработка сценария работы вируса, написание программы-вируса и антивируса.	4
5	7	РАЗДЕЛ 3 Защита сети. Тема 1: Защита административного доступа к сетевым устройствам.	Изучение способов формирования парольной защиты. 2 [стр. 111-120]	4
6	7	РАЗДЕЛ 3 Защита сети. Тема 2: Защита связи между маршрутизаторами.	Изучение механизмов протоколов маршрутизации, обеспечивающих аутентификацию и их сравнительный анализ. 2 [стр. 111-120]	4
7	7	РАЗДЕЛ 3 Защита сети. Тема 3: Технология защиты AAA.	Сравнение серверов AAA 2 [стр. 111-120]	9
8	7	РАЗДЕЛ 4 Защита сетевых соединений Тема 1: Модели обороны.	Проведение сравнительного анализа моделей обороны. 1 [стр. 100-111]	4
9	7	РАЗДЕЛ 4 Защита сетевых соединений Тема 2: Защита периметра сети	Анализ зонных архитектур. 1 [стр. 100-111]	4
10	7	РАЗДЕЛ 4 Защита сетевых соединений Тема 3: Контроль сервисов TCP/IP	Анализ уязвимостей сервисов TCP/IP.	4
11	7	РАЗДЕЛ 4 Защита сетевых соединений Тема 5: Контроль доступа по СВАС	Анализ работы контекстных списков доступа с протоколом TCP и UDP.	4
12	7	РАЗДЕЛ 5	Написание программ алгоритма	4

		Шифрование. Тема 2: Блочное шифрование.	шифрования DES.	
13	7	РАЗДЕЛ 5 Шифрование. Тема 5: Шифрование на сетевом уровне.	Анализ средств шифрования предоставляемых сетевым оборудованием.	9
14	7	РАЗДЕЛ 6 Построение виртуальных частных сетей с использованием IPSec. Тема 1: Обзор технологии виртуальных частных сетей	Сравнительный анализ технологии виртуальных частных сетей.	4
15	7	РАЗДЕЛ 6 Построение виртуальных частных сетей с использованием IPSec. Тема 3: Настройка IPSec VPN.	Выбор средств аутентификации и шифрования при построении VPN туннеля.	4
ВСЕГО:				70

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, 2009	Все разделы
2	Проектирование кампусных сетей. Учебное пособие.	Голдовский Я.М.	М.: МИИТ, 2009	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
3	Криптографическая защита компьютерной информации. Методические указания к лабораторным работам.	Голдовский Я.М. Желенков Б.В. Сафонова И.Е.	М.: МИИТ, 2013	Все разделы

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)

Microsoft Windows

Microsoft Office

Подписка МИИТ, Контракт №0373100006514000379, датадоговора 10.12.2014

Microsoft Windows

Microsoft Office

Подписка МИИТ, Контракт №0373100006514000379, датадоговора 10.12.2014

Putty

Бесплатноеиспользование (MIT)

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

№1329

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером (CPU Core i3, 8GB RAM, 1TB HDD, GeForce GT Series),. Аудитория подключена к интернету МИИТ.

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

№1327

Рабочие станции для студентов 17 шт, коммутатор CISCO CATALYST WS-C3560E, маршрутизатор CISCO 2921/K9, маршрутизатор CISCO 2921-V/K9, межсетевой экран Cisco ASA5510-K8, межсетевой экран Cisco PIX 515E-UR-FE, коммутатор Cisco Catalyst 2960, коммутатор Cisco Catalyst 3560, коммутатор 12port.10/100 autosensing.autonegotiating Catalyst Switch, маршрутизатор Cisco, сетевое оборудование, рабочая станция преподавателя, проектор, экран, доска

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.