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 Сафонова Ирина Евгеньевна, д.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Теоретические основы компьютерной безопасности

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

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 2/а 27 сентября 2019 г. Заведующий кафедрой Б.В. Желенков

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Теоретические основы компьютерной безопасности» являются - освоение студентами базовых методов и средств защиты компьютерной информации (организационных, технических, программных), ознакомление с законодательством и стандартами в этой области.
Студенты должны изучить теоретические основы компьютерной безопасности и уметь применять теорию на практике.
Основными задачами дисциплины являются:
? Изучение методов и средств защиты при работе в Internet.
? Ознакомление с процессом управления доступом к ресурсам.
? Изучение современных криптосистем,
? Изучение информационного процесса управления криптографическими ключами
? Изучение алгоритмов ЭП и хеш-функций.
? Изучение политики безопасности.
? Изучение основ проектирования систем защиты информации.

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 "Теоретические основы компьютерной безопасности" 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. Криптографические методы защиты информации:

Знания: понятия, определения, термины (понятийный аппарат курса)признаки, параметры, характеристики, свойства изучаемых в курсе объектовметоды, средства, приемы, алгоритмы, способы решения задач курса

Умения: оформлять, представлять, описывать, характеризовать данные, сведения, факты, результаты работы на языке символов (терминов, формул, образов), введенных и используемых в курсерассчитывать, определять, находить, решать, вычислять, оценивать, измерять признаки, параметры, характеристики, величины, состояния, используя известные модели, методы, средства, решения, технологии, приемы, алгоритмы, законы, теории, закономерностивыбирать способы, методы, приемы, алгоритмы, меры, средства, модели, законы, критерии для решения задач курса изменять, дополнять, адаптировать, развивать методы, алгоритмы, средства, решения, приемы, методики для решения конкретных задач

Навыки: работать с компьютером как средством управления информацией

2.1.2. Основы информационной безопасности :

Знания: основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

Умения: анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации; разрабатывать концепции и политикинеобходимые для эффективного функционирования комплексных систем информационной безопасности объектов информатизации;

Навыки: профессиональной терминологией; навыками применения средств антивирусной защиты; навыками организации и обеспечения режима защиты информации; навыками использования технических средств защиты информации; методами и средствами выявления угроз и уязвимостей безопасности объектов информатизации.

2.1.3. Техническая защита информации:

Знания: эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации.

Умения: проверять работоспособность элементов системы защиты с помощью необходимых технических средств

Навыки: основными приемами организации комплексной системы информационной безопасности, включая организационное, правовое и техническое обеспечение.

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	ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать и понимать: математический аппарат, используемый при решении задач защиты информации в компьютерных системах. Уметь: применять известные методы и средства поддержки информационной безопасности в компьютерных системах Владеть: математическими методами анализа безопасности
2	ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Знать и понимать: принципы и методы организационной защиты информации. Уметь: пользоваться нормативными документами по защите информации Владеть: навыками оценки защищенности компьютерных систем
3	ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знать и понимать: принципы организации информационных систем в соответствии с требованиями по защите информации. Уметь: искать и анализировать информацию, четко ставить цель и последовательно добиваться ее осуществления. Владеть: навыками работы с технической документацией; правильно и полно документировать результаты профессиональной деятельности.

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

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 7
Контактная работа	42	42,15
Аудиторные занятия (всего):	42	42
В том числе:		
лекции (Л)	28	28
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	14	14
Самостоятельная работа (всего)	57	57
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)	ПК1, ПК2	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						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
1	7	Раздел 1 Введение в дисциплину. 1. Введение (основные понятия и определения). 2. Характеристики угроз, служб и механизмов безопасности (виды; взаимосвязь между службами и реализующими их механизмами).	2				5	7	
2	7	Раздел 2 Правовые и организационные методы защиты информации. методы и средства защиты (технические, программные, физические, организационные). компьютерной информации. 2. Законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации). 3. Существующие стандарты (оценочные стандарты и технические спецификации; организации-разработчики стандартов).	2				5	7	
3	7	Раздел 3 Угрозы безопасности информации в компьютерных системах. . Классификация угроз (пути их реализации; комплекс требований к	4				5	9	

№ 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
		системе компьютерной безопасности). 2. Основные способы и каналы утечки информации (преодоление программных средств защиты; способы несанкционированного доступа).							
4	7	Раздел 4 Аппаратно-программные средства защиты информации. Основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки). 2. Уровни защиты информации (в эталонной модели OSI и в реальных системах; понятие архитектуры систем защиты информации). 3. Средства шифрования (защита от изменения потока сообщений и прерывания передачи; защита от навязывания ложных сообщений в каналы связи компьютерной	2	4/2			5	11/2	ПК1, (выполнение и защита лабораторных работ №1-№2
5	7	Раздел 5 Криптографические методы защиты информации. защиты информации (шифры; особенности реализации методов криптозащиты). 2. Криптоаналитические атаки (виды; противодействия).	2	4/2			5	11/2	
6	7	Раздел 6 Современные	2				4	6	

№ 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
		симметричные криптосистемы. . Стандарты шифрования данных (алгоритм шифрования данных DES; Triple DES; AES; алгоритм Ривеста). 2. Российский стандарт крипто- и имитозащиты сообщений (режимы простой замены, гаммирования, гаммирования с обратной связью).							
7	7	Раздел 7 Ассиметричные криптосистемы. . Концепция криптосистемы с открытым ключом. 2. Криптосистема шифрования данных RSA. 3. Схемы шифрования (Полига-Хеллмана; Эль Гамаля; комбинированный метод шифрования).	2				4	6	
8	7	Раздел 8 . Криптографические ключи. Управление криптографическими ключами (виды ключей; процедуры управления ключами); 2. Генерация ключей (средства генерации случайных значений ключей; ANSI X 9.17). 3. Хранение ключей (устройства хранения закрытого ключа; спецификация TPM, криптопроцессоры). 4. Распределение ключей (задача распределения ключей; распределение ключей с участием ЦРК;	2				4	6	

№ 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
		построение протокола распределения ключей; SKIP).							
9	7	Раздел 9 Управление доступом к ресурсам. Требования, подходы и задачи управления доступом. 2. Модели доступа (механизмы управления доступом; идентификация и установление подлинности). 3. Проверка полномочий субъектов на доступ к ресурсам (регистрация обращений к защищаемым ресурсам; реагирование на несанкционированные действия).	2				4	6	ПК2, (выполнение и защита лабораторных работ №3-№4
10	7	Раздел 10 Электронная подпись. . Проблема аутентификации данных. 2. Однонаправленные хэш-функции (использование в ЭП; стандарты хэш-функций). 3. Алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП). 4. Подписи с дополнительными функциональными свойствами (слепая ЭП, быстрая, неоспоримая).	2	3/2			4	9/2	
11	7	Раздел 11 Методы и средства защиты при работе в Internet. . Способы защиты	2				4	6	

№ 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
		сетей (сетевые атаки и методы противодействия; связь между характеристиками развития вирусной атаки и сетевой структурой). 2. Межсетевые экраны (особенности функционирования; основные компоненты; схемы сетевой защиты на базе межсетевых экранов; программные методы защиты).							
12	7	Раздел 12 Проектирование систем защиты информации. . Основы политики безопасности (понятие политики безопасности; реализация политики безопасности; модели безопасности). 2. Проектирование и реализация системы защиты информации (анализ объекта защиты; этапы проектирования и реализации системы; работы по созданию и сопровождению системы; архитектура системы защиты).	2	3/3			4	9/3	
13	7	Раздел 13 Перспективы развития компьютерной безопасности 1. Перспективные направления исследований в области компьютерной безопасности. 2. Центры компьютерной безопасности.	2				4	6	

№ 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
14	7	Раздел 14 итоговая аттестация						45	ЭК
15		Всего:	28	14/9			57	144/9	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 14 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 4 Аппаратно-программные средства защиты информации.	Лабораторная работа № 1 «Анализ инженерно-технических и программно-аппаратных средств защиты информации. Возможности, преимущества, недостатки».	4 / 2
2	7	РАЗДЕЛ 5 Криптографические методы защиты информации.	Лабораторная работа № 2 «Программная реализация методов шифрования».	4 / 2
3	7	РАЗДЕЛ 10 Электронная подпись.	Лабораторная работа № 3 «Симметричные и ассиметричные криптосистемы».	3 / 2
4	7	РАЗДЕЛ 12 Проектирование систем защиты информации.	Лабораторная работа № 4 «Разработка системы информационной зашиты сети предприятия»	3 / 3
			ВСЕГО:	14/9

4.5. Примерная тематика курсовых проектов (работ)

КП учебным планом не предусмотрен

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Теоретические основы компьютерной безопасности» осуществляется в форме лекций и лабораторных занятий.
Лекции проводятся в традиционной классно-урочной организационной форме в объеме 28 часов, а также с использованием интерактивных (диалоговых) технологий по типу управления познавательной деятельностью (6 часов), являются классически-лекционными (объяснительно-иллюстративными).
Лабораторные работы организованы с использованием технологий развивающего обучения. Курс лабораторных работ (14 часов) проводится с использованием интерактивных (диалоговых) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения (8 часов).
Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (57 часа) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 13 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают вопросы теоретического характера 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 Введение в дисциплину.	самостоятельная работа№1 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Изучение учебной литературы из приведенных источников: [1, стр.10-51], [5, стр.158-203].	5
2	7	РАЗДЕЛ 2 Правовые и организационные методы защиты информации.	Самостоятельная работа №2 . Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Изучение учебной литературы из приведенных источников: [3, стр.46-68], [5, стр.80-103].	5
3	7	РАЗДЕЛ 3 Угрозы безопасности информации в компьютерных системах.	Самомостоятельная работа №3 Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Изучение учебной литературы из приведенных источников: [3, стр. 46-68], [5,стр. 46-65].	5
4	7	РАЗДЕЛ 4 Аппаратно-программные средства защиты информации.	Самостоятельная работа №4 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к выполнению лабораторной работы №1. 3. Изучение учебной литературы из приведенных источников: [2, стр. 140-153], [5, стр. 46-65] [6, стр. 4-12], [9, стр.40-82].	5
5	7	РАЗДЕЛ 5 Криптографические методы защиты информации.	самостоятельная работа №5 Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Подготовка к выполнению лабораторной работы №2. 3. Изучение учебной литературы из приведенных источников: [2, стр. 48-91, 120-230], [5, стр. 46-65], [6, стр.13-19].	5
6	7	РАЗДЕЛ 6 Современные симметричные криптосистемы.	Самостоятельная работа №6 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме. 2. Подготовка к выполнению лабораторной работы №3(1). 3. Изучение учебной литературы из приведенных источников: [2,стр.98-110] [5, стр. 27-55], [6, стр. [20-25].	4
7	7	РАЗДЕЛ 7 Ассиметричные криптосистемы.	Самостоятельная работа №7 . Изучение, анализ и дополнительная проработка лекционного материала по	4

			соответствующей теме.2. Подготовка к выполнению лабораторных работ №3(2). 3. Изучение учебной литературы из приведенных источников: [4, стр.220-280], [5, стр.146-175], [6, стр.19-21].	
8	7	РАЗДЕЛ 8 . Криптографические ключи.	Самостоятельная работа №8 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Подготовка к выполнению лабораторной работы №3(3). 3. Изучение учебной литературы из приведенных источников: [1, стр. 130-250], [4, стр.155-190], [5, стр. 46-65], [6, стр.13-27].	4
9	7	РАЗДЕЛ 9 Управление доступом к ресурсам.	Самостоятельная работа №9 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Изучение учебной литературы из приведенных источников: [3, стр.74-80], [4, стр.189-210], [5, стр. 211-231].	4
10	7	РАЗДЕЛ 10 Электронная подпись.	Самостоятельная работа №10 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Подготовка к выполнению лабораторной работе №3(4). 3. Изучение учебной литературы из приведенных источников: [3, стр.50-69], [5, стр. 46-65], [6, стр.28-35].	4
11	7	РАЗДЕЛ 11 Методы и средства защиты при работе в Internet.	Самостоятельная работа №11 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Изучение учебной литературы из приведенных источников: [4, стр.197-214], [6, стр.46-65].	4
12	7	РАЗДЕЛ 12 Проектирование систем защиты информации.	Самостоятельная работа №12 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Подготовка к выполнению лабораторной работе №4. 3. Изучение учебной литературы из приведенных источников: [4, стр.22-88], [5, стр. 96-165].	4
13	7	РАЗДЕЛ 13 Перспективы развития компьютерной безопасности	Самостоятельная работа№13 1. Изучение, анализ и дополнительная проработка лекционного материала по соответствующей теме.2. Изучение учебной литературы из приведенных источников: [4, стр.134-201], [5, стр. 46-65].	4
			ВСЕГО:	57

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	Введение в информационную безопасность: учебное пособие для вузов.	А.А.Малюк [и др.] ; под ред. В.С.Горбатова.	М. : Горячая линия-Телеком, 288 с.МИИТ НТБ , 2014	1[10-51],2[33-57],3[46-68], 9[130-250].
2	Криптографические методы защиты информации : учеб.пособие для студ. Вузов.	С.Б.Гашков,	М.: Академия, 304с. МИИТ НТБ , 2010	4 [22-88],5[140-153],6[48-91, 120-230], 7 [98-110].
3	4 [22-88],5[140-153],6[48-91, 120-230], 7 [98-110].	К. А. Паршин.	М.: ФГБОУ "УМЦ ЖДТ", 2015. 95 с. МИИТ НТБ, 2015	10 [74-80], 11 [50-69].
4	Защита информации: учебник.	В.П.Мельников,	М.: Академия, 304 с. МИИТ НТБ, 2014	8 [220-280],9[155-190],10[189-210], 12 [197-214],13[134-201].
5	Программно-аппаратные средства защиты информации : учебник для студ. Вузов.	В. В. Платонов	М.: Академия, 332с. МИИТ НТБ(004 П37)., 2013	Всех разделов
6	Криптографическая защита компьютерной информации.	Я.М.Голдовский, Б.В. Желенков,	М.: МГУПС(МИИТ), 36 с. МИИТ НТБ, 2013	5 [4-12],6[13-19],7[20-25], 8 [19-21],9[13-27], 11 [28-35].

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
7	Криптографические методы защиты информации : учебное пособие для вузов.	Б. Я.Рябко, А. Н. Фионов.	М.: Горячая линия-Телеком, 229 с.МИИТ НТБ, 2014	7 [125-300],8[70-119].
8	Компьютерные сети и сетевая безопасность: учебное пособие.	В. П.Соловьев,Н. Н. Пуцко	.: МГУПС (МИИТ), 130 с.МИИТ НТБ, 2014	5 [40-82].

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/
- http://dehack.ru
- www.securitylab.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 проведении 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
Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.
Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ
№1327
Рабочие станции для студентов 17шт, коммутатор CISCO – 9шт, маршрутизатор CISCO – 9шт, сетевое оборудование, рабочая станция преподавателя, проектор, экран, доска
В случае проведении 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.
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.
Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену; выполнение лабораторных работы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания; составление отчетов по лабораторным работам; вопросы к защите лабораторных работ.
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.