МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 июня 2019 г.

Кафедра «Управление и защита информации»

Автор Груздева Людмила Михайловна, к.т.н.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Основы информационной безопасности

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 25 июня 2019 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 21 24 июня 2019 г. Заведующий кафедрой  Л.А. Баранов

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины (модуля) «Основы информационной безопасности» являются:
– обучить студентов принципам обеспечения информационной безопасности, подходам к анализу информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;
– содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.
Задачи изучения дисциплины:
- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в компьютерных системах;
- изучение типовых угроз безопасности информации при её обработке в компью-терных системах;
- изучение основных принципов обеспечения информационной безопасности;
- изучение основ построения модели угроз и политики безопасности;
- изучение основных моделей управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Основы информационной 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. Математика:

Знания: Основные методы Математического анализа, Линейной алгебры и Теории Дифференциальных уравнений. Понятия, определения и термины Высшей математики

Умения: Решать дифференциальные уравнения, системы линейных алгебраических уравнений

Навыки: Выполнения математических вычислений с применением стандартных пакетов ПО

2.1.2. Теория автоматического управления:

Знания: Теория автоматического управления. Основы Информатики и программирования на алгоритмических языках высокого уровня. Понятия и определения Теории управления. Явления устойчивости, управляемости и наблюдаемости в системах управления. Параметры и оценки качества систем управления. Качества алгоритмов. Системы управления их звенья. Переходные процессы, в системах управления, Установившиеся режимы и состояния равновесия систем управления. Принципы работы систем управления. Обратные связи. Основы теории управления. Теория устойчивости динамических систем.

Умения: Выбирать, выделять, отделять объекты, регуляторы в системах управления Оформлять, представлять, описывать, характеризовать системы управления с помощью математических формул. Выбирать необходимые приборы и оборудование для снятия характеристик систем управления. Высказывать, формулировать, выдвигать гипотезы о причинах возникновения неустойчивости и неуправляемости в системах управления. Рассчитывать, определять, находить, решать, вычислять, оценивать, измерять параметры, характеристики, величины и установившиеся состояния систем управления, используя их математические модели, методы, применяя, алгоритмы и расчета систем управления. Выбирать способы, методы, приемы, алгоритмы и модели, а также критерии устойчивости для систем управления. Изменять, дополнять, адаптировать, развивать методы, алгоритмы, Формулировать, ставить, формализовать проблемы, вопросы и задачи проектирования систем управления для решения конкретных задач исследования и проектирования систем управления.

Навыки: Ставить цель при проектировании системы управления и организовывать её достижение, уметь пояснить свою цель

2.1.3. Технические средства автоматизации и управления:

Знания: Алгоритмы исследования устойчивости и качества систем управленияМатематические модели и структурные схемы систем управления,Классификация систем управления. Точность и ошибки в системах управления

Умения: Работать с компьютером как средством управления информацией

Навыки: Классифицировать, систематизировать, дифференцировать объекты и системы, управления, методы решения задач автоматического управления, самостоятельно формулируя основания для классификации систем управления

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Модели безопасности компьютерных систем

Знания: основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; различные подходы к классификации угроз безопасности информации компьютерных систем.

Умения: анализировать и оценивать угрозы информационной безопасности объекта; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками.

Навыки: методами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.

2.2.2. Организационное и правовое обеспечение информационной безопасности

Знания: цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества и государства; основные термины по проблематике информационной безопасности; роль и место информационной безопасности в системе национальной безопасности страны.

Умения: пользоваться нормативными документами в области обеспечения информационной безопасности.

Навыки: навыками работы с нормативными правовыми документами в областиобеспечения информационной безопасности; профессиональной терминологией в области информационной безопасности.

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-1 Способен представлять роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1 Понимает значение информации и информационной безопасности в развитии современного общества, значимость своей будущей профессии.
2	ОПК-19 Способен в процессе функционирования компьютерных систем и сетей и организовать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-19.1 Участвует в разработке проектной и технической документации, включая технические задания, технико-экономическое обоснование и проектную документацию на разрабатываемые программные средства. ОПК-19.2 Знает и умеет применять на практике нормативные, правовые и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем. ОПК-19.3 Разрабатывает проекты нормативных, правовых и методических материалов, регламентирующих работу по обеспечению информационной безопасности компьютерных систем. ОПК-19.4 Разрабатывает научно-техническую документацию, готовит аналитические отчеты, научно-технические отчеты, обзоры, публикации по результатам выполненных работ. ОПК-19.5 Умеет применять современные программные средства для разработки и редакции проектно-конструкторской и технологической документации.
3	ОПК-9 Способен разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	ОПК-9.1 Владеет методами и средствами моделирования политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации. ОПК-9.2 Знает типовые модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах, угроз безопасности информации. ОПК-9.3 Умеет адаптировать типовые и строить оригинальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.
4	ПКО-1 Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах	ПКО-1.1 Участвует в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах. ПКО-1.2 Изучает и анализирует отечественный и зарубежный опыт по проблемам компьютерной безопасности. ПКО-1.3 Участвует в проведении экспериментально-исследовательских работ при сертификации средств

№ п/п	Код и название компетенции	Ожидаемые результаты
		защиты информации.

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 4
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	36	36
практические (ПЗ) и семинарские (С)	18	18
Самостоятельная работа (всего)	54	54
Экзамен (при наличии)	36	36
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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	4	Раздел 1 Информационная безопасность в системе национальной безопасности Российской Федерации	8		3		12	23	
2	4	Тема 1.2 1.1. Понятие национальной безопасности. Сущность и содержание национальной безопасности. Основные задачи в области обеспечения национальной безопасности. Объект и субъект безопасности. Виды безопасности. Виды защищаемой информации. Основные понятия и общеметодологические принципы информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.	2		1			3	
3	4	Тема 1.3 1.2. Национальные интересы России в информационной сфере. Место и роль России в глобальном информационном пространстве. Национальные интересы России в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы государства в информационной сфере. Основные	2		1			3	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		составляющие национальных интересов Российской Федерации в информационной сфере.							
4	4	Тема 1.4 1.3. Виды угроз информационной безопасности Российской Федерации. Проблемы обеспечения информационной безопасности. Угрозы конституционным правам и свободам человека и гражданина. Угрозы информационному обеспечению государственной политики РФ. Угрозы развитию отечественной индустрии информации, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Классификация угроз безопасности информационных и телекоммуникационных средств и систем. Модель действий нарушителя.	2					2	
5	4	Тема 1.5 1.4. Источники угроз информационной безопасности РФ. Внешние источники угроз. Внутренние источники угроз. Классификация источников угроз и уязвимостей информационной безопасности.	2		1			3	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
6	4	Раздел 2 Информационная война, методы и средства её ведения	6		2		10	18	
7	4	Тема 2.2 2.1. Информационная безопасность и информационное противоборство. Понятие информационной войны. Проблемы информационных войн. Субъекты информационного противоборства. Цель информационного противоборства. Составные части и методы информационного противоборства.	2		1			3	
8	4	Тема 2.3 2.2. Приемы информационного воздействия в информационной войне. Информационная война как целенаправленное информационное воздействие информационных систем. Способы перепрограммирования информационных систем. Проблема начала информационной войны.	2					2	
9	4	Тема 2.4 2.3. Типовая стратегия информационной войны. Обобщенный алгоритм информационной войны. Основные аспекты информационной войны. Последствия информационной войны.	2		1			3	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
10	4	Раздел 3 Защита от несанкционированного доступа (НСД) к информации	6		5		12	23	
11	4	Тема 3.2 3.1. Классификация автоматизированных систем и требования по защите информации. Документы Гостехкомиссии при Президенте Российской Федерации. Концепции защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности. Требования к информационным системам по обеспечению безопасности информации.	2		2			4	
12	4	Тема 3.3 3.2. Структура системы защиты информации от НСД. Назначение и функции элементов. Направления защиты от НСД. Основные способы НСД. Принципы защиты информации от НСД. Структура системы защиты информации от НСД, назначение и функции элементов.	2					2	
13	4	Тема 3.4 3.3. Модели управления доступом. Правила разграничения доступа. Мандатная и дискреционная модели управления доступом. Ролевая и атрибутные модели.	2		3			5	ПК1, Тестирование

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
14	4	Раздел 4 Основные методы обеспечения информационной безопасности	14		6		12	32	
15	4	Тема 4.2 4.1. Основные понятия криптографической защиты информации. Определяются предмет и задачи криптографии, формулируются основополагающие определения и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Рассматривается пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.	2		1			3	
16	4	Тема 4.3 4.2. Идентификация и аутентификация. Понятия идентификации, аутентификации и авторизация. Классификация систем аутентификации. Пароли, сертификаты и цифровые подписи. Методы аутентификации.	2		1			3	
17	4	Тема 4.4 4.3. Разграничение и контроль доступа к информации. Разграничение доступа по виду, характеру, назначению, степени важности и секретности информации; по способам ее обработки: считать, записать,	2		1			3	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		внести изменения, выполнить команду; по условному номеру терминала; по времени обработки и др. Разделение привилегий на доступ к информации.							
18	4	Тема 4.5 4.4. Технологии межсетевых экранов. Технология межсетевых экранов (МЭ) - защита корпоративных сетей от внешних угроз. Функции МЭ. МЭ способствует реализации политики безопасности, определяет разрешенные службы, типы доступа к ним и является реализацией этой политики в терминах сетевой конфигурации, хостов, маршрутизаторов и других мер защиты.	2		1			3	
19	4	Тема 4.6 4.5. Виртуальные частные сети. Основные понятия и функции виртуальных частных сетей (VPN). Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN.	2		1			3	
20	4	Тема 4.7 4.6. Методы обнаружения вторжений (атак). Краткая история вторжений (атак) на интрасети. Основные понятия. Классификация систем обнаружения вторжений. Интеллектуальное и поведенческое	2		1			3	

№ 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	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		обнаружение вторжений.							
21	4	Тема 4.8 4.7. Компьютерные вирусы и средства антивирусной защиты. Вирусы как угроза информационной безопасности. Средства антивирусной защиты.	2					2	
22	4	Раздел 5 Стандарты защищенности информации в компьютерных системах	2		2		8	12	
23	4	Тема 5.2 5.1. Характеристика систем стандартизации в области защиты информации. Информационная безопасность распределенных систем. Европейские критерии безопасности информационных технологий.	2		2			4	ПК2, Тестирование
24	4	Экзамен						36	ЭК
25		Всего:	36		18		54	144	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 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	4	РАЗДЕЛ 1 Информационная безопасность в системе национальной безопасности Российской Федерации Тема: 1.1.	ПЗ №1 Виды информации и основные методы ее защиты, анализ информационной инфраструктуры государства.	1
2	4	РАЗДЕЛ 1 Информационная безопасность в системе национальной безопасности Российской Федерации Тема: 1.2.	ПЗ №2 Основные понятия и общеметодологические принципы информационной безопасности.	1
3	4	РАЗДЕЛ 1 Информационная безопасность в системе национальной безопасности Российской Федерации Тема: 1.4.	ПЗ №3 Виды и источники угроз информационной безопасности Российской Федерации.	1
4	4	РАЗДЕЛ 2 Информационная война, методы и средства её ведения Тема: 2.1.	ПЗ №4 Виды и формы применения информационно-технологического оружия.	1
5	4	РАЗДЕЛ 2 Информационная война, методы и средства её ведения Тема: 2.3.	ПЗ №5 Последствия информационной войны.	1
6	4	РАЗДЕЛ 3 Защита от несанкционированного доступа (НСД) к информации Тема: 3.1.	ПЗ №6 1 Причины, виды, каналы утечки и искажения информации, формальная постановка и решение задачи обеспечения информационной безопасности компьютерных систем.	1
7	4	РАЗДЕЛ 3 Защита от несанкционированного доступа (НСД) к информации Тема: 3.1.	ПЗ №7 Модели организации кибернетической безопасности.	1

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
8	4	РАЗДЕЛ 3 Защита от несанкционированного доступа (НСД) к информации Тема: 3.3.	ПЗ №8 Модель избирательного (дискреционного) доступа. Модель ролевого (типизованного) доступа.	1
9	4	РАЗДЕЛ 3 Защита от несанкционированного доступа (НСД) к информации Тема: 3.3.	ПЗ №9 Модель Лендвера-Маклина (MMS).	1
10	4	РАЗДЕЛ 3 Защита от несанкционированного доступа (НСД) к информации Тема: 3.3.	ПЗ №10 Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.	1
11	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности Тема: 4.1.	ПЗ №13 Основные понятия криптографической защиты информации. Пример простейшего шифра, на основе которого поясняются сформулированные понятия и тезисы.	1
12	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности Тема: 4.2.	ПЗ №14 Классификация систем аутентификации. Электронная подпись и ее применение для контроля целостности программ и данных.	1
13	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности Тема: 4.3.	ПЗ №12 Построение системы разграничения доступа в базе данных на основе ролевой модели.	1
14	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности Тема: 4.4.	ПЗ №11 Программно-аппаратные средства обеспечения информационной безопасности.	1
15	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности Тема: 4.5.	ПЗ №15 Виртуальные частные сети. Варианты построения виртуальных защищенных каналов.	1
16	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности Тема: 4.6.	ПЗ №16 Антивирусные программные комплексы. Восстановление зараженных файлов. Профилактика проникновения «троянских программ».	1

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
17	4	РАЗДЕЛ 5 Стандарты защищенности информации в компьютерных системах Тема: 5.1.	ПЗ №17 Обобщенная архитектура стандартов обеспечения информационной безопасности организации.	1
18	4	РАЗДЕЛ 5 Стандарты защищенности информации в компьютерных системах Тема: 5.1.	ПЗ №18 Документы по оценке защищенности автоматизированных систем в РФ.	1
			ВСЕГО:	18 / 0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Технология обучения как учебного исследования
Технология педагогических мастерских
Технология коллективной мыследеятельности (КМД)
Технология эвристического обучения

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	4	РАЗДЕЛ 1 Информационная безопасность в системе национальной безопасности Российской Федерации	Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем, презентаций и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014	12
2	4	РАЗДЕЛ 2 Информационная война, методы и средства её ведения	Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем, презентаций и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014	10
3	4	РАЗДЕЛ 3 Защита от несанкционированного доступа (НСД) к информации	Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем; проведение расчетов и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014 Программно-аппаратные средства защиты информации: учебник для студ. вузов, обуч. по напр. "Информационная безопасность" / В. В. Платонов. - М.: Академия, 2013	12
4	4	РАЗДЕЛ 4 Основные методы обеспечения информационной безопасности	Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем; проведение расчетов и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014 Программно-аппаратные средства защиты информации: учебник для студ. вузов / В. В. Платонов. - М.: Академия, 2013	12
5	4	РАЗДЕЛ 5 Стандарты защищенности информации в компьютерных системах	Выполнение заданий; подбор и изучение литературных источников; разработка и составление различных схем, презентаций и др. Защита информации: учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе. - М.: Академия, 2014 Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для студ. вузов ж.-д. трансп. / К. А. Паршин. - М.: ФГБОУ "УМЦ ЖДТ", 2015	8
			ВСЕГО:	54

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	Защита информации	В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе	Академия, 2014	Все разделы
2	Программно-аппаратные средства защиты информации	В. В. Платонов	Академия, 2013	Все разделы
3	Оценка уровня информационной безопасности на объекте информатизации: учебное пособие для студ. вузов ж.-д. трансп.	К. А. Паршин	ФГБОУ "УМЦ ЖДТ", 2015	Все разделы
4	Информационная безопасность и защита информации на железнодорожном транспорте: учебник для студ., обуч. по спец. "Информационная безопасность телекоммуникационных систем": в 2 ч. Ч.1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте.	С. Е. Ададуров [и др.]; под ред. А. А. Корниенко	ФГБОУ "УМЦ ЖДТ", 2014	Все разделы
5	Основы информационной безопасности	Л.М. Груздева	Юридический институт МИИТа, 2018	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
6	Криптографические методы защиты информации	Б. Я. Рябко, А. Н. Фионов	Горячая линия-Телеком, 2014	Все разделы
7	Компьютерные сети и сетевая безопасность	В. П. Соловьев, Н. Н. Пуцко	МГУПС (МИИТ), 2014	Все разделы
8	Информационная безопасность и защита информации на железнодорожном транспорте: учебник для студ., обуч. по спец. "Информационная безопасность телекоммуникационных	С. Е. Ададуров [и др.]; под ред. А. А. Корниен-ко	ФГБОУ "УМЦ ЖДТ", 2014	Все разделы

	систем": в 2 ч. Ч.2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте.			
9	Региональная и национальная безопасность	А.Б. Логунов	ИНФРА-М, 2015	Все разделы
10	Информационное право	И.Л. Бачило	Издательство Юрайт, 2013	Все разделы

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

Сайты содержат учебно-методическую документацию, научно-практические публикации, руководящие документы в области информационной безопасности, информационные и аналитические материалы, необходимые для качественного изучения учебной дисциплины.

1. http://citforum.ru — большой учебный сайт по технике и новым технологиям
2. http://www.ict.edu.ru — портал «Информационно-коммуникационные технологии в образовании»
3. http://www.iso27000.ru – портал «Искусство управления информационной безопасностью»
4. http://www.itsec.ru – журнал «Information Security»
5. http://www.inside-zi.ru – журнал «Защита информации»
6. http://www.inside-zi.ru – журнал «Инсайд»
7. http://www.xakep.ru – журнал «Хакер»
8. http://www.compress.ru – журнал «Компьютер пресс»
9. http://www.osp.ru – журнал «Открытые системы»
10. http://www.miit.ru — сайт Московского государственного университета путей сообщения Императора Николая II
11. http://garant.ru – Гарант: законодательство РФ
12. http://www.consultant.ru – Консультант +: законодательство РФ
13. http://www.consultantplus.ru – База данных «Консультант +»
14. http://fstec.ru/ – Федеральная служба по техническому и экспортному контролю (ФСТЭК России)
15. http://www.scrf.gov.ru/ – Совет безопасности РФ
16. http://fsb.ru – ФСБ России

Студентам обеспечена возможность свободного доступа к фондам учебно-методической документации и Интернет-ресурсам. Все студенты имеют возможность открытого доступа:

- к вузовской ЭБС на платформе Oracle http://miit.ru/portal/page/portal/miit/library/e-catalogue,
- к ЭБС Научно-технической библиотеки МИИТа http://library.miit.ru/,
- к Российской универсальной научной электронной библиотеке «eLibrary» http://elibrary.ru/,
- к электронной библиотеке Book.ru http://book.ru/
- к ЭБС Лань https://e.lanbook.com/,
- к ЭБС Юрайт https://biblio-online.ru/,
- к ЭБС ibooks.ru http://ibooks.ru/.

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

Установленное лицензионное программное обеспечение.
1. Операционная система Microsoft Windows 8
2. Пакет офисных программ Microsoft Office 2013
3. Браузер Internet Explorer
4. Антивирусные программы
5. http://www.consultant.ru – Консультант +: законодательство РФ
6. http://garant.ru – Гарант: законодательство РФ
7. http://fstec.ru/ – ФСТЭК России
8. http://www.iso27000.ru – портал «Искусство управления информационной безопасностью»

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

Компьютерный класс, оборудованный для проведения лекций и практических работ средствами оргтехники, проекторам, персональными компьютерами, объединенными в сеть с выходом в Интернет.

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

Изучение данной дисциплины направлено на формирование у обучающихся знаний и профессиональных навыков в сфере информационной безопасности. Учебный курс имеет свою систему, представляющую определенную, логически завершенную и стройную последовательность изучения разделов курса.
Учебный курс ориентирован на освоение знаний о принципах обеспечения информационной безопасности компьютерных систем. Его содержание направлено на развитие навыков использования современных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в компьютерных системах.
Настоящая рабочая программа учебной дисциплины включает в себя цели освоения учебной дисциплины, место учебной дисциплины в структуре ОП ВО, компетенции обучающегося, формируемые в результате освоения учебной дисциплины (ожидаемые результаты образования и компетенции студента по завершении освоения программы учебной дисциплины), структуру и содержание учебной дисциплины; виды самостоятельной работы студентов; учебно-методическое и информационное обеспечение учебной дисциплины; список основной и дополнительной литературы. Все это поможет студентам при подготовке к итоговой форме контроля и самостоятельному изучению разделов и тем учебной дисциплины.
Основным методом изучения учебного курса является самостоятельная работа студента, состоящая из изучения научных трудов, учебной литературы, первоисточников по информационной безопасности. Основными видами аудиторной работы студентов являются лекционные занятия.
Методические указания к лекционным занятиям
В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал

прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Методические рекомендации студентам к практическим занятиям
Важной составной частью учебного процесса в вузе являются практические занятия. Практические занятия по дисциплине «Основы информационной безопасности», требующей помимо знаний теоретического материала еще и навыков в области информационных технологий, помогают студентам глубже усвоить учебный материал, приобрести практические навыки работы на компьютере и навыки творческой работы над учебной и научной литературой.
На практическом занятии происходит обсуждение заданий, выполненных студентами самостоятельно дома. Это возможность для студентов еще раз обратить внимание на непонятные до сих пор моменты и окончательно разобрать их. Преподаватель может (выборочно) проверить записи с самостоятельно выполненными заданиями.
Во время практического занятия преподаватель может провести опрос по теме, обозначенной для данного практического занятия. В процессе этого опроса студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия. Творческое обсуждение, дискуссии вырабатывают умения и навыки использовать приобретенные знания для различного рода ораторской деятельности.
На практическом занятии каждый его участник должен быть готовым к ответам на все теоретические вопросы, поставленные в плане, проявлять максимальную активность при их рассмотрении. Ответы должны строиться свободно, убедительно и аргументирова-но. Преподаватель следит, чтобы ответы были точными, логично построенным и не сводилось к чтению конспекта. Необходимо, чтобы выступающий проявлял глубокое понимание того, о чем он говорит, сопоставлял теоретические знания с их практическим применением, был способен привести конкретные примеры объектов и положений, о которых рассуждает теоретически.

Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к практическим занятиям
В ходе подготовки к практическому занятию необходимо прочитать конспект лекции, изучить основную литературу, ознакомиться с дополнительной литературой. При этом учесть рекомендации преподавателя и требования учебной программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.
В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Готовясь к докладу или реферативному сообщению, обращаться за методической помощью к преподавателю. Составить план-конспект своего выступления. Продумать практические примеры, с целью обеспечения тесной связи изучаемой теории с практическим применением.
Методические рекомендации студентам по изучению рекомендованной литературы
Изучение дисциплины следует начинать с проработки настоящей рабочей программы,

особое внимание, уделяя целям и задачам, структуре и содержанию курса. Студентам рекомендуется получить в библиотеке учебную литературу по дисциплине, необходимую для эффективной работы на всех видах аудиторных занятий, а также для самостоятельной работы по изучению дисциплины. Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении рекомендованной литературы. Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и дипломных работ. Успешное освоение курса предполагает активное, творческое участие студента путем планомерной, повседневной работы.