МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

06 октября 2020 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Андреева Татьяна Алексеевна

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Автоматизированные системы обработки информации и управления
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 3 05 октября 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 2 02 октября 2020 г. Заведующий кафедрой В.Е. Нутович

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Защита информации» – является изучение студентами основ создания защищенных компьютерных систем.
Основной целью изучения учебной дисциплины «Защита информации» является формирование у обучающегося компетенций в области защиты информации, необходимых при эксплуатации, техническом обслуживании, проектировании, производстве, испытаниях, модернизации технических и программных средств железнодорожного транспорта для следующих видов деятельности:
- научно-исследовательской;
-проектно-конструкторской.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
проектно-конструкторская деятельность:
- разработки технических требований, технических заданий и технических условий на проекты систем защиты информации с использованием средств автоматизации и информационных технологий;
научно-исследовательская деятельность:
- научных исследований в области эксплуатации и производства систем информационной безопасности железнодорожного транспорта, интерпретации и вероятностного моделирования отказов систем защиты с формулировкой аргументированных умозаключений и выводов; поиска и проверки новых технических и программных решений по совершенствованию этих систем; разработки планов, программ и методик проведения исследований уровня защищенности, анализ их результатов.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

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

2.1. Наименования предшествующих дисциплин

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

2.1.1. Математика:

Знания: основных понятий и методов теории вероятностей, математической статистики, дискретной математики, основ математического моделирования

Умения: применять методы математического анализа и моделирования

Навыки: владения методами математического описания физических явлений и процессов, определяющих принципы работы различных технических устройств

2.1.2. Операционные системы:

Знания: основ функционирования операционных систем, архитектуры компьютерных сетей

Умения: программировать на языках высокого уровня

Навыки: применения средств антивирусной защиты, построения компьютерных сетей

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Проектирование информационных систем

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 осваивать методики использования программных средств для решения практических задач	Знать и понимать: алгоритмические, технические и программные средства защиты информационных систем Уметь: использовать средства защиты для разработки политики информационной безопасности Владеть: средствами разработки программы информационной безопасности
2	ПК-3 способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	Знать и понимать: уязвимости информационной системы, архитектуру систем защиты информации Уметь: создавать системы разграничения прав доступа к информации Владеть: средствами защиты, обеспечивающими целостность, конфиденциальность и доступность 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 7
Контактная работа	54	54,15
Аудиторные занятия (всего):	54	54
В том числе:		
лекции (Л)	18	18
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	36	36
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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	7	Раздел 1 Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС) Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС) Основные понятия ИБ и ЗИ Предмет защиты , объект защиты Угрозы ИБ в КС, случайные и преднамеренные	2/2	4/1			12	18/3	, Контрольная работа
2	7	Тема 1.1 Проблемы информационной безопасности (ИБ) Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС) Основные понятия ИБ и ЗИ Предмет защиты , объект защиты Угрозы ИБ в КС, случайные и преднамеренные	2/2					2/2	
3	7	Раздел 2 Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз Повышение надежности программных и аппаратных средств ЗИ в КС от преднамеренных угроз	2/2	4/1			8	14/3	ПК1, текущий контроль по разделам 1 - 3. (Тест №1)
4	7	Тема 2.1 Защита информации в КС	2/2					2/2	

№ 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
5	7	Раздел 3 Криптографические методы защиты информации Криптографические методы защиты информации Основные этапы развития криптографии Криптографические системы с симметричным ключом. Стандарты шифрования. Криптографические системы с открытым ключом	2/2	16/3			9	27/5	
6	7	Тема 3.1 Криптографические методы защиты информации Криптографические методы защиты информации Основные этапы развития криптографии Криптографические системы с симметричным ключом. Стандарты шифрования. Криптографические системы с открытым ключом	2/2					2/2	
7	7	Раздел 4 Стеганографические методы ЗИ Стеганографические методы ЗИ Область применения. Основные понятия стеганографии. Классификация методов. Алгоритмы встраивания информации в изображения, в аудио-сигналы.					4	4	
8	7	Раздел 5 ЗИ в телекоммуникационных сетях ЗИ в телекоммуникационных сетях Категории атак: эксплойт, проникновение, хищение сеанса, отказ	8/2	4/1			6	18/3	ПК2, Опрос,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/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		от обслуживания, присвоение пакетов. Защита периметра сети, защита от инсайдера, защита от вредоносных программ.							
9	7	Тема 5.1 ЗИ в телекоммуникационных сетях Категории атак: эксплойт, проникновение, хищение сеанса, отказ от обслуживания, присвоение пакетов. Защита периметра сети, защита от инсайдера, защита от вредоносных программ.	8/2					8/2	
10	7	Раздел 6 Защищенные виртуальные сети Защищенные виртуальные сети Понятия инкапсуляции и туннелирования. Протоколы канального, сетевого и сеансового уровня.	2				8	10	ПК2, текущий контроль по разделам 5 - 6 (Тест №2)
11	7	Тема 6.1 Защищенные виртуальные сети Понятия инкапсуляции Защищенные виртуальные сети Понятия инкапсуляции и туннелирования. Протоколы канального, сетевого и сеансового уровня.	2					2	
12	7	Раздел 7 Законодательство в области ИБ Законодательство в области ИБ Ответственность в сфере компьютерной безопасности Защита персональных данных	2	8/2			7	17/2	
13	7	Тема 7.1 Законодательство в области ИБ Законодательство в области ИБ Ответственность в	2					2	

№ 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
		сфере компьютерной безопасности Защита персональных данных							
14	7	Экзамен						36	ЭК
15		Тема 4.1 Стеганографические методы ЗИ Стеганографические методы ЗИ Область применения. Основные понятия стеганографии. Классификация методов. Алгоритмы встраивания информации в изображения, в аудио-сигналы.							
16		Всего:	18/8	36/8			54	144/16	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 36 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 1 Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС)	Защита информации в персональном компьютере с помощью стандартных средств ОС Windows 7 и пакета Microsoft Office	4 / 1
2	7	РАЗДЕЛ 2 Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз	Разработка пользовательского приложения, обеспечивающего авторизацию пользователя	4 / 1
3	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Шифрование данных путем замены и перестановок	4
4	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Шифрование с закрытым ключом	4 / 1
5	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Алгоритмы шифрования с открытым ключом.	4 / 1
6	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Электронная цифровая подпись	4 / 1
7	7	РАЗДЕЛ 5 ЗИ в телекоммуникационных сетях	Защита периметра сети	4 / 1
8	7	РАЗДЕЛ 7 Законодательство в области ИБ	Обеспечение безопасности данных	4 / 1
9	7	РАЗДЕЛ 7 Законодательство в области ИБ	Итоговое занятие	4 / 1
			ВСЕГО:	36/8

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) не предусмотрены учебным планом.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Защита информации» осуществляется в форме лекций и лабораторных работ.
Лекции проводятся в традиционной классно-урочной организационной форме, и на 50 % являются традиционными классически-лекционными (объяснительно-иллюстративными), на 50 % с использованием интерактивных (диалоговых) технологий.
Лабораторные занятия проводятся в компьютерном классе, оснащенном персональными компьютерами с предустановленным необходимым программным обеспечением. Каждый студент выполняет лабораторную работу индивидуально. Время лабораторных занятий используется в том числе для демонстрации студентами результатов выполненных работ и сдачи отчетов по лабораторным работам.
Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы (23 часа) относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям (10 часов) относится отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, подготовка отчетов по выполненным лабораторным работам.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 7 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (анализ конкретных ситуаций, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.
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 Проблемы информационной безопасности (ИБ) и защиты информации (ЗИ) в компьютерных системах (КС)	Подготовка к контрольной работе 1. Подготовка к контрольной работе 2. Проработка учебного материала по литературе [1 стр.7-28, 3, 6 стр.6-34] [1]; [3]; [4]	12
2	7	РАЗДЕЛ 2 Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз	Проработка учебного материала по литературе [3]; [5]; [6]	8
3	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Подготовка к промежуточному контролю по тесту №2 1. Подготовка к промежуточному контролю по тесту ПК 1 2. Проработка учебного материала по литературе [2 стр.146-192] [1]; [2]; [5]	9
4	7	РАЗДЕЛ 4 Стеганографические методы ЗИ	Проработка учебного материала по литературе[1 стр. 119-137, 4 стр.184-223, 6 стр. 115-203] [1]; [4]; [5]	4
5	7	РАЗДЕЛ 5 ЗИ в телекоммуникационных сетях	Проработка учебного материала по литературе [1 стр.213-323, 5 стр. 275-321] 1. Проработка учебного материала по литературе [1 стр.213-323, 5 стр. 275-321] 3. 2 Подготовка к промежуточному контролю по тесту ПК 2	6
6	7	РАЗДЕЛ 6 Защищенные виртуальные сети	Проработка учебного материала по литературе [1 стр.226-330, 2 стр.146-192]	8
7	7	РАЗДЕЛ 7 Законодательство в области ИБ	Проработка учебного материала по литературе [1 стр.253-334, 2 стр.156-201]	7
			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	Информационная безопасность и защита информации	В.П. Мельников, С.А. Клейменов, А.М. Петраков	Издательский центр "Академия", 2011 ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)	1,3,4
2	Защита программ и данных	В.Г. Проскурин	Москва Академия 004 П 82 , 2011	3 стр. 142-196
3	ГОСТ Р 50922-96 Защита информации. Основные термины и определения	http://standartgost.ru/	0	1, 2

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Комплексная защита информации в компьютерных системах	В.И. Завгородний	Логос, 2001 НТБ (фб.)	1,3,4
5	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта	В.В. Яковлев, А.А. Корниенко	УМК МПС России, 2002 НТБ (уч.4); НТБ (фб.); НТБ (чз.1)	2,3,4
6	Безопасность систем баз данных	В.П. Соловьев, В.В. Гуренко, Н.Н. Пуцко; Ред. В.П. Соловьев; МИИТ. Центр компетентности "Защита и безопасность информации"	МИИТ, 2007 НТБ (ЭЭ); НТБ (фб.); НТБ (чз.2)	2 стр. 46 - 78

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

1. http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ.
2. http://rzd.ru/ - сайт ОАО «РЖД».
3. http://elibrary.ru/ - научно-электронная библиотека.
4. Поисковые системы: Yandex, Google, Mail.
5. Википедия, www.asu-miit.ru

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

1) Embarcadero RAD Studio
2) Windows 7, Microsoft Office 2013, Microsoft Office 2007, Microsoft Essential Security 2012
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)

Для проведения занятий по учебной дисциплине «Защита информации» необходимо:
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.
Аудиовизуальное оборудование для аудитории, компьютер в сборе Helios Profice VL310, комп.в сборе ПЭВМ HELiOS VL310 – 13,
компьютер Processor – 1, персональный компьютер категории 1 -4, проектор NEC VT, экран с электроприводом (потолочное крепление,комплект кабелей), экран моторизованный 127*169.
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)

Лекционные занятия проводятся в режиме презентации. Перед началом занятий преподаватель передает студентам электронную или твердую копию презентационного лекционного материала в форме опорного конспекта. Студент должен приходить на лекции с заранее распечатанным материалом по тематике текущей лекции. Опорный конспект включает основные определения, схемы, графические иллюстрации, примеры и другие важные материалы курса.
В ходе лекции преподаватель демонстрирует на экране слайды презентации, комментирует и поясняет их содержание. Студентам рекомендуется делать дополнительные пометки и записи непосредственно в опорном конспекте. При необходимости, можно вести записи в традиционной форме в отдельной тетради.
Для подготовки и выполнения лабораторных работ рекомендуется использовать опубликованные и электронные методические указания. Необходимое программное обеспечение предоставляется преподавателем по мере выполнения лабораторных работ. Защита лабораторных работ предполагает обязательную демонстрацию полученных в ходе работы результатов и предоставление отчета.
Опорный конспект лекций, методические указания для лабораторных работ, примеры

контрольных заданий, а также другие материалы размещаются на сервере кафедры и доступны для скачивания.
При самостоятельной подготовке студенты могут воспользоваться материалами, доступными в сети Интернет на официальных сайтах, а также на специализированных сайтах, содержащих учебную и справочную информацию.