МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

02 июня 2021 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Андреева Татьяна Алексеевна

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

Направление подготовки:	09.03.02 – Информационные системы и технологии
Профиль:	Информационные системы и технологии на транспорте
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 6 01 июня 2021 г. Председатель учебно-методической комиссии  Н.А. Клычева	Протокол № 4 01 июня 2021 г. Заведующий кафедрой  В.Е. Нутович

Москва 2021 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:
• проектно-конструкторская;
• научно-исследовательской.
Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):
проектно- конструкторская:
• использования типовых методов создания изображений;
• разработки технических требований, технических заданий и технических условий на информационные системы, для визуализации результатов испытаний работоспособности информационных систем, при создании сопроводительной документации;
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 языке C++

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-4 пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны	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 проводить рабочее проектирование	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	48	48,15
Аудиторные занятия (всего):	48	48
В том числе:		
лекции (Л)	16	16
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	32	32
Самостоятельная работа (всего)	60	60
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)	2/2	2/2			12	16/4	
2	7	Тема 1.1 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	2/2	2/1			12	16/3	ПК1, текущий контроль по разделам 1 - 2. (Тест №1)
4	7	Тема 2.1 Повышение надежности программных и аппаратных средств ЗИ в КС от преднамеренных угроз	2/2					2/2	
5	7	Раздел 3 Криптографические методы защиты информации	4	16/5			11	31/5	
6	7	Тема 3.1 Основные этапы развития криптографии Криптографические системы с симметричным ключом. Стандарты шифрования. Криптографические системы с открытым ключом	4					4	
7	7	Раздел 4 Стеганографические методы ЗИ	2				4	6	
8	7	Тема 4.1 Стеганографические методы ЗИ Область применения. Основные понятия стеганографии. Классификация методов. Алгоритмы	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
		встраивания информации в изображения, в аудио-сигналы.							
9	7	Раздел 5 Защита данных ЗИ в телекоммуникационных сетях	2/2	4/1			6	12/3	
10	7	Тема 5.1 Категории атак: эксплойт, проникновение, хищение сеанса, отказ от обслуживания, присвоение пакетов. Защита периметра сети, защита от инсайдера, защита от вредоносных программ.	2/2					2/2	
11	7	Раздел 6 Защищенные виртуальные сети	2				8	10	ПК2, текущий контроль по разделам 5 - 6 (Тест №2)
12	7	Тема 6.1 Понятия инкапсуляции и туннелирования. Протоколы канального, сетевого и сеансового уровня.	2					2	
13	7	Раздел 7 Законодательство в области ИБ	2	8/3			7	17/3	
14	7	Тема 7.1 Ответственность в сфере компьютерной безопасности Защита персональных данных	2					2	
15	7	Экзамен						36	ЭК
16		Всего:	16/6	32/12			60	144/18	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 32 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	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	2 / 2
2	7	РАЗДЕЛ 2 Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз	Разработка пользовательского приложения	2 / 1
3	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Шифрование данных путем замены и перестановок	4 / 1
4	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Шифрование с закрытым ключом	4 / 1
5	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Шифрование с открытым ключом	4 / 2
6	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Электронная цифровая подпись	4 / 1
7	7	РАЗДЕЛ 5 Защита данных ЗИ в телекоммуникационных сетях	Защита периметра сети	4 / 1
8	7	РАЗДЕЛ 7 Законодательство в области ИБ	Обеспечение безопасности данных	4 / 2
9	7	РАЗДЕЛ 7 Законодательство в области ИБ	Итоговое занятие	4 / 1
			ВСЕГО:	32/12

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) учебным планом не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Защита информации» осуществляется в форме лекций и лабораторных работ.
Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 50 % являются традиционными классически-лекционными (объяснительно-иллюстративными), на 50 % с использованием интерактивных (диалоговых) технологий
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.

Лабораторные работы организованы с использованием технологий развивающего обучения. Для проведения лабораторных занятий используется компьютерный класс, в котором каждый студент выполняет лабораторную работу индивидуально. Применяются необходимые средства: специальное программное обеспечение, методические указания.
Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы (15 часов) 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, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.
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.

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)	Основные понятия ИБ и ЗИ. Предмет защиты, объект защиты Угрозы ИБ в КС, случайные и преднамеренные	12
2	7	РАЗДЕЛ 2 Защита информации в КС путем разграничения прав доступа ЗИ в КС от случайных угроз	ЗИ в КС от случайных угроз. Повышение надежности программных и аппаратных средств ЗИ в КС от преднамеренных угроз	12
3	7	РАЗДЕЛ 3 Криптографические методы защиты информации	Основные этапы развития криптографии Криптографические системы с симметричным ключом. Стандарты шифрования. Криптографические системы с открытым ключом	11
4	7	РАЗДЕЛ 4 Стеганографические методы ЗИ	Область применения. Основные понятия стеганографии. Классификация методов. Алгоритмы встраивания информации в изображения, в аудио-сигналы.	4
5	7	РАЗДЕЛ 5 Защита данных 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.	6
6	7	РАЗДЕЛ 6 Защищенные виртуальные сети	Понятия инкапсуляции и туннелирования. Протоколы канального, сетевого и сеансового уровня.	8
7	7	РАЗДЕЛ 7 Законодательство в области ИБ	Ответственность в сфере компьютерной безопасности Защита персональных данных	7
			ВСЕГО:	60

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	Жук, Е.П. Жук, О.М. Лепешкин	Издательский центр Инфра-М, РИОР, 2015	Раздел 1, Раздел 3, Раздел 4
2	Основы программно-аппаратной защиты информации	М.А. Борисов, И.В. Заводцев, И.В. Чижов	URSS, Москва, 2016	Раздел 3 (стр. 142-196)
3	ГОСТ Р 50922-96 Защита информации. Основные термины и определения		0 http://standartgost.ru	Раздел 1, Раздел 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.П. Завгородний	Москва Логос, 2001	Все разделы
5	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта	В.В.Яковлев, А.А. Корниенко	Москва УМК МПС России, 2002	Все разделы
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)	Все разделы

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)

- операционная система Windows 7, XP
- программное обеспечение Embarcadero RAD Studio

- пакет прикладных программ Microsoft Office
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, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (аудиовизуальное оборудование,компьютер в сборе Helios Profice VL310)
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (1 рабочая станция для преподавателя (Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.), 14 рабочих станций для студентов (Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.), проектор, экран для проектора, интерактивная 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)

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.