

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

УТВЕРЖДАЮ:

Директор РОАТ



В.И. Апатцев

15 октября 2020 г.

Кафедра «Системы управления транспортной инфраструктурой»

Автор Ермаков Александр Евгеньевич, к.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки:	09.03.03 – Прикладная информатика
Профиль:	Прикладная информатика в информационной сфере
Квалификация выпускника:	Бакалавр
Форма обучения:	заочная
Год начала подготовки	2019

Одобрено на заседании Учебно-методической комиссии института Протокол № 1 10 октября 2019 г. Председатель учебно-методической комиссии  С.Н. Климов	Одобрено на заседании кафедры Протокол № 3 03 октября 2019 г. Заведующий кафедрой  А.В. Горелик
---	---

Рабочая программа учебной дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 168572
Подписал: Заведующий кафедрой Горелик Александр Владимирович
Дата: 03.10.2019

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Информационная безопасность» является формирование у обучающихся компетенций в соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС)

по направлению подготовки «Прикладная информатика» и приобретение ими:

- знаний о современных поисковых системах в глобальных компьютерных сетях, об угрозах информационной безопасности, о нормативных правовых документах по информационной безопасности и о методах и средствах обеспечения информационной безопасности;
- умений выявлять угрозы информационной безопасности, использовать нормативные правовые документы по информационной безопасности, использовать методы и средства обеспечения информационной безопасности и проводить обследование организаций;
- навыков определения угроз информационной безопасности, приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Информационная безопасность" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Информатика и программирование:

Знания: Знать основные свойства и технологии использования и обработки информации.

Умения: Уметь использовать технологии информационных систем

Навыки: Навыками внедрения информационных технологий

2.1.2. Математика:

Знания: основные математические понятия

Умения: использовать математические методы в профессиональной деятельности

Навыки: основными математическими методами

2.1.3. Правовые основы информатизации:

Знания: нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий

Умения: использовать нормативно-правовые документы, международные и отечественные

Навыки: способностью использовать нормативно-правовые документы, международные и отечественные стандарты

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Управление информационными системами

**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	ПКС-52 Способен осуществлять эффективное управление материально-техническими и человеческими ресурсами	ПКС- 52.1 Грамотно анализирует задачу и принимает эффективные решения по управлению имеющимися ресурсами

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

4.1. Общая трудоемкость дисциплины составляет:

5 зачетных единиц (180 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 3
Контактная работа	20	20,25
Аудиторные занятия (всего):	20	20
В том числе:		
лекции (Л)	8	8
лабораторные работы (ЛР)(лабораторный практикум) (ЛП)	12	12
Самостоятельная работа (всего)	156	156
ОБЩАЯ трудоемкость дисциплины, часы:	180	180
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	5.0	5.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КРаб (1)	КРаб (1)
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

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	3	Раздел 1 Раздел 1. Правовая основа информационной безопасности информационных систем. Предмет, цели и задачи дисциплины “Информационная безопасность”. Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ.	2				29	31	, выполнение К
2	3	Раздел 2 Раздел 2. Информационная безопасность и методология защиты информации в корпоративных системах ФЖТ Классификация информации, циркулирующей в корпоративных системах федерального железнодорожного транспорта (ФЖТ). Информационные ресурсы и информационная инфраструктура сетей ФЖТ как объекты защиты. Классификация и анализ угроз информационной безопасности корпоративным	2				28	30	, выполнение К

№ 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
		системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический.							
3	3	Раздел 3 Раздел 3. Криптографические методы защиты информации Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блочные и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамала. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная	2				28	30	, выполнение К

№ 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
		хэш-функция.							
4	3	Раздел 4 Раздел 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. Применение паролей и биометрических средств аутентификации пользователей. Протоколы взаимной проверки подлинности объектов сети. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI. Обеспечение целостности информации. Аутентификация информации и ЭЦП сообщений. Однонаправленные хэш-функции. Коды проверки подлинности информации. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика	2	12			28	42	, выполнение К

№ 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
		наиболее популярных антивирусных пакетов.							
5	3	Раздел 5 Раздел 5. Архитектура и методы организации систем защиты информации. Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. Специализированные программно- аппаратные средства защиты информации. Средства и механизмы обеспечения безопасности сетевого оборудования Cisco systems. Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200.					43	43	, выполнение К
6	3	Раздел 6 Дифференцированный зачет						4	ЗаО
7	3	Раздел 7 Контрольная работа						0	КРаб
8		Всего:	8	12			156	180	

4.4. Лабораторные работы / практические занятия

Практические занятия учебным планом не предусмотрены.

Лабораторные работы предусмотрены в объеме 12 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего ча- сов/ из них часов в интерак- тивной форме
1	2	3	4	5
1	3	Раздел 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей	Настройка правил фильтрации трафика с помощью межсетевого экрана Agnitum OutPost Firewall Для проведения лабораторного практикума требуется необходимое количество комплектов обучающей компьютерной программы (специализированное программное обеспечение) и соответствующая компьютерная техника, предназначенная для работы с указанной программой, позволяющая использовать сетевой прокол TCP/IP и администратор баз данных ODBC32.	12
ВСЕГО:				12/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые проекты (работы) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями самостоятельно разработанными образовательного стандарта высшего образования для реализации компетентностного подхода и с целью формирования и развития профессиональных навыков студентов по усмотрению преподавателя в учебном процессе могут быть использованы в различных сочетаниях активные и интерактивные формы проведения занятий, включая: Лекционные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; средства и устройства манипулирования аудиовизуальной информацией; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ). Лабораторные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; виртуальные лабораторные работы. Самостоятельная работа. Дистанционное обучение - интернет-технология, которая обеспечивает студентов учебно-методическим материалом, размещенным на сайте академии, и предполагает интерактивное взаимодействие между преподавателем и студентами. Контроль самостоятельной работы. Использование тестовых заданий, размещенных в системе «Космос», что предполагает интерактивное взаимодействие между преподавателем и студентами.

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	3	Раздел 1. Правовая основа информационной безопасности информационных систем.	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1,2 доп.:1,2]	29
2	3	Раздел 2. Информационная безопасность и методология защиты информации в корпоративных системах ФЖТ	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1,2]	28
3	3	Раздел 3. Криптографические методы защиты информации	решение заданий из контрольной работы; самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1 доп.:2]	28
4	3	Раздел 4. Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1 доп.:1,2]	28
5	3	Раздел 5. Архитектура и методы организации систем защиты информации.	самостоятельное изучение и конспектирование отдельных тем учебной литературы, связанных с разделом [осн.: 1,2]	43
ВСЕГО:				156

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	М.: Издательский центр "Академия", 2008. - 336 с., библиотека РОАТ	Используется при изучении разделов, номера страниц 1(23-49), 2(56-87), 3(98- 124), 4(237 – 298), 5(301-322)
2	Комплексная защита информации в корпоративных системах.	Шаньгин В.Ф.	М.:Инфра-М, 2010. – 592 с., Библиотека РОАТ	Используется при изучении разделов, номера страниц 1(78 – 224), 2(240-301), 5(397-423)
3	Электронно-библиотечная система издательства «Лань»		0 http://e.lanbook.com /	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д транспорта.	Яковлев В.В., Корниенко А.А.	М.: УМК МПС России, 2002.– 328 с., Библиотека РОАТ	Используется при изучении разделов, номера страниц 2(105 – 261)3(134 – 235)
5	Защита информации в компьютерных системах и сетях.	Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.	М.: Радио и связь, 2001. – 328 с., Библиотека РОАТ	Используется при изучении разделов, номера страниц 4(115 – 151),
6	Основы информационной безопасности: Курс лекций. Учебное пособие	Галатенко В.А.	М.: ИНТУИТ, 2006. - 205 с., Библиотека РОАТ	Используется при изучении разделов, номера страниц 5(245 – 276)
7	Электронно-библиотечная система Научно-технической библиотеки МИИТ		0 http://library.mii.ru/	Все разделы

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

Официальный сайт РУТ (МИИТ) (<http://mii.ru/>)

Электронно-библиотечная система Научно-технической библиотеки МИИТ
(<http://library.mii.ru/>)

Электронно-библиотечная система издательства «Лань» (<http://e.lanbook.com/>)

Электронно-библиотечная система ibooks.ru (<http://ibooks.ru/>)

Электронно-библиотечная система «УМЦ» (<http://www.umczdt.ru/>)

Электронно-библиотечная система «Intermedia» (<http://www.intermedia-publishing.ru/>)

Электронно-библиотечная система РОАТ (<http://biblioteka.rgotups.ru/jirbis2/>)

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

Для осуществления учебного процесса с использованием дистанционных образовательных технологий: операционная система Windows, Microsoft Office 2003 и выше, Браузер Internet Explorer 8.0 и выше с установленным Adobe Flash Player версии 10.3 и выше, Adobe Acrobat.

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

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET.

2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

3. Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

Для проведения лабораторных занятий: компьютерный класс; кондиционер; компьютеры с минимальными требованиями - Pentium 4, ОЗУ 4 Гб, HDD 100 Гб, USB 2.0

Технические требования к оборудованию для осуществления учебного процесса с использованием дистанционных образовательных технологий:

колонки, наушники или встроенный динамик (для участия в аудиоконференции); микрофон или гарнитура (для участия в аудиоконференции); веб-камеры (для участия в видеоконференции);

для ведущего: компьютер с процессором Intel Core 2 Duo от 2 ГГц (или аналог) и выше, от 2 Гб свободной оперативной памяти.

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

В процессе освоения дисциплины студенты должны посетить лекции, выполнить лабораторные работы и контрольную работу в соответствии с учебным планом, получить зачеты по контрольным работам и сдать зачет с оценкой.

1. Указания (требования) для выполнения контрольных работ.

1.1. Методические рекомендации по выполнению контрольных работ размещены в системе «КОСМОС» или получает у преподавателя в начале установочной сессии.

1.2. Контрольные работы должны быть выполнены в установленные сроки и оформлены в соответствии с утверждёнными требованиями, которые приведены в методических рекомендациях.

1.3. Выполнение контрольных работ рекомендуется не откладывать на длительный срок: решить большую часть задач имеет смысл практически после аудиторных занятий, пока хорошо помнишь то, что было рассказано на лекции.

При таком подходе возникает возможность получить оперативную очную консультацию у лектора в течение периода прохождения сессии.

1.4. Если возникают трудности по выполнению контрольных работ, можно получить консультацию по решению у преподавателя между сессиями.

1.5. В установленные сроки производится защита контрольных работ по тестовым задачам по изучаемому теоретическому материалу.

2. Указания для освоения теоретического материала и сдачи зачета

2.1. Обязательное посещение лекционных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.

2.2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование конспекта лекций, презентаций и методических рекомендаций по выполнению контрольных работ из системы "КОСМОС".

2.3. Копирование (электронное) перечня вопросов к зачёту с оценкой по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины, которая размещена в системе «КОСМОС».

2.4. Рекомендуются следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет - поиск информации (видеофайлов, файлов-презентаций, файлов с учебными пособиями) по ключевым словам курса и ознакомиться с найденной информацией при подготовке к зачету с оценкой по дисциплине.

2.5. После проработки теоретического материала согласно рабочей программе курса необходимо подготовить ответы на вопросы для защиты контрольных работ и вопросы к зачету с оценкой.

2.6. Студент допускается до сдачи зачета с оценкой, если выполнена и защищена контрольная работа.

Контактная работа осуществляется в соответствии с расписанием занятий.

Контактная работа может быть организована с использованием дистанционных образовательных технологий.

Если дисциплина осваивается с использованием элементов дистанционных образовательных технологий:

Лекционные занятия проводятся в формате вебинара в режиме реального времени.

Практические занятия проводятся в формате вебинара или онлайн формате в режиме реального времени. Практические занятия проводятся в интерактивном (диалоговом) режиме

Если лабораторные работы могут быть выполнены с использованием дистанционных образовательных технологий. В этом случае студенту с помощью сети

Internet предоставляется доступ к дистанционному лабораторному стенду, размещенному на сервере академии

Для выполнения лабораторных работ используется свободно распространяемое программного обеспечение