

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

УТВЕРЖДАЮ:

Директор РОАТ

 В.И. Апатцев

21 мая 2019 г.



Кафедра «Железнодорожная автоматика, телемеханика и связь»

Автор Коптева Лариса Георгиевна, д.т.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации в мобильных системах

Направление подготовки:	09.04.03 – Прикладная информатика
Магистерская программа:	Прикладная информатика в обеспечении безопасности бизнеса
Квалификация выпускника:	Магистр
Форма обучения:	заочная
Год начала подготовки	2019

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 1 10 октября 2019 г. Председатель учебно-методической комиссии</p> <p style="text-align: center;"> С.Н. Климов</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 3 03 октября 2019 г. Заведующий кафедрой</p> <p style="text-align: center;"> А.В. Горелик</p>
--	--

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 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Защита информации в мобильных системах» является формирование у обучающихся компетенций в соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по специальности «Прикладная информатика» и приобретение ими:

- знаний об основах , составе мобильных технологий и систем ;
- умений работать , настраивать мобильные системы
- навыков по обеспечению информационной безопасности

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Защита информации в мобильных системах" 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. Информационная безопасность и защита бизнес информации:

Знания: методы и средства способы решения прикладных задач в условиях неопределенности

Умения: применять методы и средства эффективного решения прикладных задач

Навыки: навыками постановки и решения прикладных задач

2.1.2. Современные сетевые технологии:

Знания: способы исследования закономерностей становления и развития информационного общества в области защиты бизнеса методы и средства способы решения прикладных задач в условиях неопределенности способы профессиональной эксплуатации современного электронного оборудования, используемого для проведения экспериментов

Умения: исследовать закономерности становления и развития информационного общества в области защиты бизнеса эксплуатировать современное электронное оборудование, которое используется для проведения научных экспериментов применять методы и средства эффективного решения прикладных задач

Навыки: навыками исследования закономерностей становления и развития информационного общества в области защиты бизнеса навыками постановки и решения прикладных задач навыками оценки результатов исследований

2.1.3. Современные системы программирования:

Знания: различные научные подходы к автоматизации информационных процессов основы информационных процессов и систем методологию и технологию создания ИС предприятий и организаций

Умения: развивать информатизацию предприятий и организаций использовать инновационные инструментальные средства осуществлять анализ проектов по информатизации прикладных задач

Навыки: навыками исследовать различные научные подходы к автоматизации информационных процессов навыками адаптации современных ИКТ к задачам прикладных ИС проектами по информатизации прикладных задач

2.1.4. Современные системы хранения данных:

Знания: основы информационных процессов и систем

Умения: использовать инновационные инструментальные средства

Навыки: навыками адаптации современных ИКТ к задачам прикладных ИС

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Научно-исследовательская работа

**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-51 Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий	ПКС-51.2 Использует знания в области информационных технологий для решения поставленных задач

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

4.1. Общая трудоемкость дисциплины составляет:

3 зачетные единицы (108 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 2
Контактная работа	8	8,25
Аудиторные занятия (всего):	8	8
В том числе:		
лекции (Л)	4	4
практические (ПЗ) и семинарские (С)	4	4
Самостоятельная работа (всего)	96	96
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)		
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 промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	2	<p>Раздел 1</p> <p>Раздел 1. Основы мобильных технологий.</p> <p>Классификация угроз информации в мобильных системах:</p> <p>Внутренние и внешние угрозы.</p> <p>Непреднамеренные ошибки пользователей. Аварии коммуникаций</p> <p>Стихийные бедствия.</p> <p>Вредоносное программное обеспечение.</p> <p>Мошеннический доступ (Access Fraud , AMPS и др.),</p>	2				16	18	
2	2	<p>Раздел 2</p> <p>Раздел 2. Методология защиты информации в мобильных системах</p> <p>Уровни защиты информации в мобильных системах: правовой, организационный, аппаратно-программный, криптографический</p>					20	20	, Опрос
3	2	<p>Раздел 3</p> <p>Раздел 3. Методы защиты от несанкционированного доступа к информации и техническим ресурсам мобильных сетей</p> <p>Идентификация и аутентификация объектов сети.</p> <p>Идентификация и подтверждение подлинности пользователей сети.</p> <p>Применение паролей и</p>					40	40	, Опрос

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		средств аутентификации пользователей. Протоколы IDEA-128 И AES-256 и аналогичные устройства Межсетевое экранирование. Обеспечение целостности информации в мобильных сетях							
4	2	<p>Раздел 4 Раздел 4. Аппаратные и программные и другие средства защиты мобильных устройств</p> <p>Программные решения защиты: Российский комплекс Voice Coder Mobile (VCM), Kashtrsky Mobile Security 8.0, Handy Safe Pro</p> <p>Аппаратные решения: Криптофоны. Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блочные и поточные шифры. Стойкость криптосистем. Российский стандарт криптографической защиты ГОСТ 28147-89 и американский стандарт шифрования данных DES</p> <p>Асимметричные криптосистемы. Управление ключами, методы генерации, хранения и распределения ключей., инфраструктура ключей. Спец. системы</p>	2		4		20	26	, Опрос

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Всего	Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего		
1	2	3	4	5	6	7	8	9	10	
		конференц связи; спец. терминалы для защиты разговоров по мобильным сетям; системы перехвата (Эшелон, СОУД и др.); системы внутреннего мониторинга информации. Использование дополнительных устройств: скремблеры, специальные телефоны для конфиденциальной связи.								
5	2	Раздел 6 Зачет с оценкой						4	ЗаО	
6		Раздел 5 Допуск к зачету							, тест КСР	
7		Всего:	4		4		96	108		

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 4 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	2	Раздел 4. Аппаратные и программные и другие средства защиты мобильных устройств	Методы защиты от несанкционированного доступа Комплекты технических средств и оборудования для проведения лабораторного практикума с использованием компьютерной техники на базе IBM PC/AT (примерный вариант комплектации) (Возможны также комплекты на базе Macintosh)	4
ВСЕГО:				4/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовая работа по дисциплине «Защита информации в мобильных системах» -не предусмотрена

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательные технологии, используемые для реализации компетентного 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. Практические занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ). 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, что предполагает интерактивное взаимодействие между преподавателем и студентами. При изучении дисциплины используются технологии электронного обучения (информационные, интернет ресурсы, вычислительная техника) и, при необходимости, дистанционные образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающегося и педагогических работников.

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	2	Раздел 1. Основы мобильных технологий. Классификация угроз информации в мобильных системах:	Проработка учебного материала [осн.: 1-4, доп.:1].	16
2	2	Раздел 2. Методология защиты информации в мобильных системах	Проработка учебного материала [осн.: 2-4, доп.:1].	20
3	2	Раздел 3. Методы защиты от несанкционированного доступа к информации и техническим ресурсам мобильных сетей	Проработка учебного материала ; выполнение курсовой работы (проекта) [осн.: 1, доп.:1].	40
4	2	Раздел 4. Аппаратные и программные и другие средства защиты мобильных устройств	Проработка учебного материала ; выполнение курсовой работы (проекта) [осн.: 1-4, доп.:1].	20
ВСЕГО:				96

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(28 – 59), 2(82 – 145), 3(181 – 216), 4(259 – 308)
2	Сети мобильной связи LTE/LTE ADVANCED	В.О. Тихвинский, С.В. Терентьев, В.П. Высотин	М.: Медиа Паблишер, 2014, 329с, библиотека РОАТ	Используется при изучении разделов, номера страниц 1(170 – 276)
3	Защита информации в сетях сотовой подвижной связи	Максименко В.Н	М., 2007-452с, библиотека РОАТ	Используется при изучении разделов, номера страниц 1(70 – 78), 2(133 – 141), 3(176 – 199), 4(306 – 309)
4	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
5	Стандартизация, спецификации, эволюция технологии и архитектура базовой сети LTE// Сети и средства связи. Специальный выпуск "Сети доступа", № 3, стр34-39	В.О. Тихвинский, С.В. Терентьев, И.В. Минаев	2009, 203с, библиотека РОАТ	Используется при изучении разделов, номера страниц 1(112 – 179)
6	Электронно-библиотечная система Научно-технической библиотеки МИИТ		0 http://library.miiit.ru/	Все разделы

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

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

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

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

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

Электронно-библиотечная система «УМЦ» (<http://www.umcздt.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)

Программное обеспечение должно позволять выполнить все предусмотренные учебным планом виды учебной работы по дисциплине «Защита информации в мобильных системах»: теоретический курс, практические занятия, , тестовые вопросы по курсу.

- Программное обеспечение для выполнения практических заданий включает в себя специализированное прикладное программное обеспечение, а также программные продукты общего применения
- Программное обеспечение для проведения лекций, демонстрации презентаций и ведения интерактивных занятий: Microsoft Office 2003 и выше.
- Программное обеспечение, необходимое для оформления отчетов и иной документации: Microsoft Office 2003 и выше.
- Программное обеспечение для выполнения текущего контроля успеваемости: Браузер Internet Explorer 6.0 и выше.

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
4. Для проведения практических 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 и практические занятия в соответствии с учебным планом, сдать зачет с оценкой

1. Указания для освоения теоретического материала и сдачи зачет с оценкой
 - 1.1. Обязательное посещение лекционных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.
 - 1.2. Получение в библиотеке рекомендованной учебной литературы и электронное

копирование конспекта лекций, презентаций .

1.3. Копирование (электронное) перечня вопросов к зачет с оценкой по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины».

1.4. Рекомендуется 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 зачет с оценкой по дисциплине.

1.5. После проработки теоретического материала согласно рабочей программе курса необходимо подготовить ответы на вопросы к зачет с оценкой

1.6. Студент допускается до сдачи зачет с оценкой если выполнены практические задания.

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