

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор РОАТ



В.И. Апатцев

29 мая 2018 г.

Кафедра «Железнодорожная автоматика, телемеханика и связь»

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

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ 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	2018

Одобрено на заседании Учебно-методической комиссии института Протокол № 2 22 мая 2018 г. Председатель учебно-методической комиссии  С.Н. Климов	Одобрено на заседании кафедры Протокол № 10 15 мая 2018 г. Заведующий кафедрой  А.В. Горелик
---	--

Москва 2018 г.

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Защита информации в мобильных системах» является формирование у обучающихся компетенций в соответствии с федеральными государственными образовательными стандартами 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.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПК-1	способностью использовать и развивать методы научных исследований и инструментария в области проектирования и управления ИС в прикладных областях
------	---

4. Общая трудоемкость дисциплины составляет

4 зачетных единиц (144 ак. ч.).

5. Образовательные технологии

В соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального 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. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1

Раздел 1. Основы мобильных технологий. Классификация угроз информации в мобильных системах:

Внутренние и внешние угрозы. Непреднамеренные ошибки пользователей. Аварии коммуникаций Стихийные бедствия. Вредоносное программное обеспечение. Мошеннический доступ (Access Fraud , AMPS и др.),

РАЗДЕЛ 1

Раздел 1. Основы мобильных технологий. Классификация угроз информации в мобильных системах:

экзамен

РАЗДЕЛ 2

Раздел 2. Методология защиты информации в мобильных системах

Уровни защиты информации в мобильных системах: правовой, организационный, аппаратно-программный, криптографический

РАЗДЕЛ 2

Раздел 2. Методология защиты информации в мобильных системах

экзамен

РАЗДЕЛ 3

Раздел 3. Методы защиты от несанкционированного доступа к информации и техническим ресурсам мобильных сетей

Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. Применение паролей и средств аутентификации пользователей. Протоколы IDEA-128 И AES-256 и аналогичные устройства Межсетевое экранирование. Обеспечение целостности информации в мобильных сетях

РАЗДЕЛ 3

Раздел 3. Методы защиты от несанкционированного доступа к информации и техническим ресурсам мобильных сетей

выполнение КР, экзамен

РАЗДЕЛ 4

Раздел 4. Аппаратные и программные и другие средства защиты мобильных устройств

Программные решения защиты: Российский комплекс Voice Coder Mobile (VCM), Kashtsky Mobile Security 8.0, Handy Safe Pro

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 Асимметричные криптосистемы.

Управление ключами , методы генерации, хранения и распределения ключей., инфраструктура ключей.

Спец. системы 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.

РАЗДЕЛ 4

Раздел 4. Аппаратные и программные и другие средства защиты мобильных устройств

выполнение КР, экзамен

РАЗДЕЛ 5

допуск к экзамену

РАЗДЕЛ 5

допуск к экзамену

защита КР

Экзамен

Экзамен

экзамен

Экзамен

Тема: Курсовая работа