

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

Кафедра «Железнодорожная автоматика, телемеханика и связь»

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Защита информации в мобильных системах»**

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

## 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.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКС-51	Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий
--------	--

## 4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

## 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. 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 2**

Раздел 2. Методология защиты информации в мобильных системах  
Опрос

### **РАЗДЕЛ 2**

Раздел 2. Методология защиты информации в мобильных системах

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

### **РАЗДЕЛ 3**

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

### **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 4**

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

### **РАЗДЕЛ 4**

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

Программные решения защиты: Российский комплекс Voice Coder Mobile (VCM), Kashtrsky 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 5

Допуск к зачету

РАЗДЕЛ 5

Допуск к зачету

тест КСР

РАЗДЕЛ 6

Зачет с оценкой