

**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**

**«Основы информационной безопасности бизнеса»**

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 «Основы информационной безопасности бизнеса» является формирование у обучающихся компетенций в соответствии с федеральными государственными образовательными стандартами по специальности «Прикладная информатика» и приобретение ими:

- знаний об основных угрозах бизнес информации, отечественных и международных стандартов в области защиты информации, методах и средствах защиты бизнес информации;
- умений выявлять опасности и угрозы, возникающие в современном информационном обществе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны ;
- навыков выявления опасностей и угроз информационной безопасности, построения политики информационной безопасности и систем защиты бизнес информации.

## 2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Основы информационной безопасности бизнеса" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую 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

5 зачетных единиц (180 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). 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. Классификация угроз бизнес информации

Опрос

### **РАЗДЕЛ 1**

Раздел 1. Классификация угроз бизнес информации

Внутренние и внешние угрозы. Непреднамеренные ошибки пользователей. Кражи и подлоги. Аварии коммуникаций. Стихийные бедствия. Вредоносное программное обеспечение. Хакеры.

### **РАЗДЕЛ 2**

Раздел 2. Методология защиты бизнес информации

Опрос

### **РАЗДЕЛ 2**

Раздел 2. Методология защиты бизнес информации

Уровни защиты бизнес информации: правовой, организационный, аппаратно-программный, криптографический

### **РАЗДЕЛ 3**

Раздел 3. Криптографические методы защиты бизнес 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 хэш-функция.

### **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 меж сетевого экранирования на различных уровнях модели OSI. Обеспечение целостности информации.

Дифференцированный зачет