**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

## «Аудит безопасности информационных систем»

| | |
|---|---|
| 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 |

**1. Цели освоения учебной дисциплины**

Целью освоения учебной дисциплины «Аудит безопасности информационных систем» является формирование у обучающихся компетенцийв соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по программе подготовки магистров 09.04.03 «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 выполнять экспертизу безопасности информационной системы предприятия;
- 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 "Аудит безопасности информационных систем" 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**

3 зачетные единицы (108 ак. ч.).

**5. Образовательные технологии**

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). Практические 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..

**6. Содержание дисциплины (модуля), структурированное по темам (разделам)**

РАЗДЕЛ 1
Раздел 1. Классификация угроз информационных систем
Опрос

РАЗДЕЛ 1
Раздел 1. Классификация угроз информационных систем

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

РАЗДЕЛ 2
Раздел 2. Методология защиты информационных систем
Опрос

РАЗДЕЛ 2
Раздел 2. Методология защиты информационных систем

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

РАЗДЕЛ 5
Зачет с оценкой