

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

СОГЛАСОВАНО:

Выпускающая кафедра ЭТиУЧР  
Заведующий кафедрой ЭТиУЧР



И.А. Епишкин

08 сентября 2017 г.

УТВЕРЖДАЮ:

Директор ИЭФ



Ю.И. Соколов

08 сентября 2017 г.

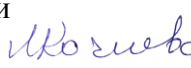

Кафедра «Экономическая информатика»

Автор Морозова Вера Ивановна, к.э.н., доцент

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Информационная безопасность»**

Направление подготовки:	<u>38.03.03 – Управление персоналом</u>
Профиль:	<u>Кадровая безопасность</u>
Квалификация выпускника:	<u>Бакалавр</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2015</u>

Одобрено на заседании Учебно-методической комиссии института Протокол № 1 06 сентября 2017 г. Председатель учебно-методической комиссии  Л.Ф. Кочнева	Одобрено на заседании кафедры Протокол № 2 04 сентября 2017 г. Заведующий кафедрой  Л.А. Каргина
---	---

## 1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины (модуля) «Информационная безопасность в электронном бизнесе» являются ознакомление студентов с основными понятиями и определениями информационной безопасности, источниками, рисками и формами атак на информацию, угрозами и вредоносными программами, защитой от вирусов, методами и средствами защиты информации, криптографическими методами защиты информации, стандартами информационной безопасности.

В результате освоения дисциплины студент должен:

знать:

принципы работы, связанные с обеспечением комплексной защиты информации на основе существующих программ и методик; основные угрозы информации в компьютерных системах; существующие методы и средства, применяемые для контроля и защиты информации; системные вопросы защиты программ и данных; основные категории требований к программной и программно-аппаратной реализации средств защиты информации; требования к защите автоматизированных систем от НСД.

уметь:

проводить анализ материалов учреждений, организаций и предприятий отрасли с целью выработки, и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну; анализировать методы и средства контроля и защиты информации и разрабатывать предложения по их совершенствованию и повышению эффективности защиты информации.

иметь навыки:

работы с действующими нормативными и методическими документами, новыми средствами и системами защиты информации

## 2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Информационная безопасность" относится к блоку 1 "Профессиональный цикл" 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:

ОПК-10	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-13	умением вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами, знанием основ кадровой статистики, владение навыками составления кадровой отчетности, а также навыками ознакомления сотрудников организации с кадровой документацией и действующими локальными нормативными актами, умением обеспечить защиту персональных данных сотрудников
ПК-28	знанием корпоративных коммуникационных каналов и средств передачи информации, владение навыками информационного обеспечения процессов внутренних коммуникаций

#### **4. Общая трудоемкость дисциплины составляет**

5 зачетных единиц (180 ак. ч.).

#### **5. Образовательные технологии**

Контент по дисциплине В обучении студентов по данной дисциплине используются: 1. при проведении лекционных занятий: - вводная; - лекция-информация; - презентации; - классическо-лекционный; - проблемная лекция; - обучение с помощью технических средств обучения - лекция визуализация; - лично-ориентированные; - объяснительно-иллюстративные; 2. для проведения лабораторных занятий: - проектная технология; - технология учебного исследования; - техника «круглый стол»; - объяснительно-иллюстративные- технология обучения в сотрудничестве и в малых группах; - технология проблемного обучения; - групповые; - технологии дистанционного обучения; - индивидуальные; - разбор конкретных ситуаций..

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

##### **РАЗДЕЛ 1**

Актуальность информацион-нойбезопас-ности

Классификация компьютерных преступлений. Понятия и определения в информационнойбе-зопасности.

##### **РАЗДЕЛ 2**

Международ-ные стандарты информацион-ного обмена.

Критерии безопаснос-тикомпью-терных систем «Оранжевая книга».  
Руководящие документы Гостехкомиссии.

##### **РАЗДЕЛ 3**

Угрозы информации

Виды угроз информаци-онная безо-пасности  
РФ. Источники угроз.

##### **РАЗДЕЛ 4**

Защита от компьютер-ных вирусов

Источники компьютерных вирусов. Основные правила защиты. Антивирус-ные програм-мы.

##### **РАЗДЕЛ 5**

Вредонос-ныепрограм-мы

Классификация компьютерных вирусов  
Файловые и загрузочные вирусы.

## РАЗДЕЛ 6

### Методы и средства защиты информации

Ограничение, разграничение и контроль доступа к информации Понятие идентификации и аутентификации. Организационные меры по защите информации.

Криптографические методы защиты информации. Стеганография.

Концепция информационной безопасности.

Экзамен