

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



Рабочая программа дисциплины (модуля),  
как компонент образовательной программы  
высшего образования - программы бакалавриата  
по направлению подготовки  
38.03.05 Бизнес-информатика,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Информационная безопасность**

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль): Информационные системы в бизнесе

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде  
электронного документа выгружена из единой  
корпоративной информационной системы управления  
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)  
ID подписи: 564169  
Подписал: заведующий кафедрой Каргина Лариса Андреевна  
Дата: 18.01.2022

## 1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины являются формирование теоретических основ и практических навыков в области защиты информации от несанкционированного доступа, искажения, потери. Рассматриваются тенденции развития защиты информации с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а также с нормативными документами и методами защиты компьютерной информации. Проводится изучение современных методов защиты информации: криптография, стеганография.

## 2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

**ОПК-2** - Способен проводить исследование и анализ рынка информационных систем и информационно-коммуникационных технологий, выбирать рациональные решения для управления бизнесом ;

**ПК-7** - Способен проводить сбор информации о деятельности подразделения организации с целью разработки административного регламента подразделения организации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

### **Знать:**

основные методы и модели обеспечения информационной безопасности для корпоративных и иных систем

### **Уметь:**

проводить исследования и анализ рынка ИС и ИКТ с точки зрения обеспечения информационной безопасности

### **Владеть:**

навыками разработки и внедрения систем защиты информации

## 3. Объем дисциплины (модуля).

### 3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов)).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №5
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 80 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

#### 4. Содержание дисциплины (модуля).

##### 4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Актуальность информационной безопасности мет и метод защиты информации. Рассматриваемые вопросы: -Объект защиты информации. -Угрозы безопасности информации в компьютерных системах.
2	Методы и средства защиты информации. Современные методы защиты информации Рассматриваемые вопросы: -Защита от несанкционированного доступа (НСД).
3	Методы и средства защиты информации. Современные методы защиты информации Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	-Ограничение, разграничение, контроль доступа, идентификация, аутентификация пользователя. -СОРДИ.
4	Методы и средства защиты информации. Современные методы защиты информации Рассматриваемые вопросы: -Таксономия нарушений информационной безопасности ВС и причины, обуславливающие их существование.
5	Методы и средства защиты информации. Современные методы защиты информации Рассматриваемые вопросы: -Криптографические методы защиты информации. -Стеганография
6	Методы и средства защиты информации. Современные методы защиты информации Рассматриваемые вопросы: -Концепция информационной безопасности.
7	Защита документооборота в вычислительных системах Рассматриваемые вопросы: -Угрозы и методы защиты. -Комплексный метод защиты.
8	Компьютерные вирусы и механизмы борьбы с ними Рассматриваемые вопросы: -Источники компьютерных вирусов.
9	Компьютерные вирусы и механизмы борьбы с ними . Рассматриваемые вопросы: -Основные правила защиты. -Антивирусные программы.
10	Международные и отечественные стандарты информационной безопасности. Рассматриваемые вопросы: -Стандарт ISO 15408.
11	Международные и отечественные стандарты информационной безопасности. Рассматриваемые вопросы: -Стандарты безопасности в Интернете, протоколы защиты передачи данных - SSL (TLS), SET, IP v. 6, IPSec.
12	Международные и отечественные стандарты информационной безопасности. Рассматриваемые вопросы: -Нормативные документы, регламентирующие оценку защищенности ИТ.
13	Комплексные системы защиты информации. Рассматриваемые вопросы: -Концепция создания защищенных компьютерных систем.
14	Комплексные системы защиты информации. Рассматриваемые вопросы: -Этапы создания комплексной системы комплексной защиты информации

#### 4.2. Занятия семинарского типа.

##### Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Методы и средства защиты информации. В результате практического занятия у студента формируется навык разработки программ по методам

№ п/п	Тематика практических занятий/краткое содержание
	защиты информации (Криптография)
2	Методы и средства защиты информации. В результате практического занятия у студента формируется навык разработки программ по методам защиты информации (Стеганография)
3	Методы и средства защиты информации На практическом занятии у студента формируется навык описания методов защиты информации
4	Методы и средства защиты информации На практическом занятии студент изучает функциональные возможности метода защиты информации
5	Методы и средства защиты информации. В результате практического занятия студент приобретает навыки анализа криптостойкости метода защиты
6	Методы и средства защиты информации В результате практического занятия студент изучает современные методы защиты информации
7	Методы и средства защиты информации. В результате практического занятия студент приобретает навыки защиты от несанкционированного доступа (НСД).
8	Методы и средства защиты информации. В результате практического занятия студент приобретает навыки ограничения контроля доступа
9	Методы и средства защиты информации. В результате практического занятия студент приобретает навыки разграничения контроля доступа
10	Методы и средства защиты информации В результате практического занятия студент приобретает навыки идентификации
11	Методы и средства защиты информации В результате практического занятия студент изучает таксономию нарушений информационной безопасности ВС
12	Методы и средства защиты информации. В результате практического занятия студент изучает причины существования таксономии нарушений
13	Защита документооборота в вычислительных системах. На практическом занятии у студента формируется навык работы с комплексными методами защиты информации
14	Комплексные системы защиты информации. На практическом занятии студент изучает концепцию создания защищенных компьютерных систем

#### 4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом, литературой, самостоятельное изучение разделов (тем) Дисциплины(модуля)
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	«Криптографические методы защиты информации для изучающих компьютерную безопасность» Лось А. Б., Нестеренко А. Ю., Рожков М. И Юрайт , 2021	<a href="https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-469133#page/1">https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-469133#page/1</a>
2	«Криптографические методы защиты информации» Юрайт , 2021	<a href="https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-469758#page/1">https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-469758#page/1</a>

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Информационный портал Научная электронная библиотека eLIBRARY.RU ([www.elibrary.ru](http://www.elibrary.ru))

Единая коллекция цифровых образовательных ресурсов (<http://window.edu.ru>); Научно-техническая библиотека РУТ (МИИТ) (<http://library.miit.ru>)

<http://edu.emiit.ru/> - Портал дистанционного обучения Института экономики и финансов РУТ (МИИТ)

Электронный контент «Информационная безопасность»

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Windows 8

Microsoft Office 2013

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения лекционных занятий необходима аудитория с мультимедиа аппаратурой. Для проведения практических занятий требуется аудитория, оснащенная мультимедиа аппаратурой и ПК с необходимым программным обеспечением, и подключением к сети интернет.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры  
«Информационные системы  
цифровой экономики»

В.И. Морозова

Согласовано:

Заведующий кафедрой ИСЦЭ  
Председатель учебно-методической  
комиссии

Л.А. Каргина

М.В. Ишханян