

**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  
09.03.01 Информатика и вычислительная техника,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Основы информационной безопасности**

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Системы автоматизированного проектирования

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: 2899  
Подписал: заведующий кафедрой Нестеров Иван Владимирович  
Дата: 03.03.2023

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

Целями освоения дисциплины (модуля) являются:

- изучение студентами основных методов защиты компьютерной информации;
- изучение студентами способов защиты при работе в глобальных (Интернет) и локальных сетях, при работе с электронной почтой.

Задачами дисциплины (модуля) являются:

- овладение знаниями о программах-вирусах и антивирусных пакетах;
- овладение основными методами шифрования данных и создания электронной подписи.

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

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

**ОПК-3** - Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

**ОПК-5** - Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем.

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

### **Знать:**

способы защиты компьютерной информации при работе в сети, способы борьбы с программами-вирусами и уметь бороться с ними, алгоритмы шифрования и проверки электронной подписи.

### **Уметь:**

способами защиты компьютерной информации при работе в сети, способами борьбы с программами-вирусами и уметь бороться с ними, способами использования алгоритмов шифрования и проверки электронной подписи.

### **Владеть:**

способами защиты компьютерной информации при работе в сети, способами борьбы с программами-вирусами и уметь бороться с ними, алгоритмами шифрования и проверки электронной подписи.

### 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. №3
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	<p><b>Основные понятия в области информационной безопасности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- базовые понятия (информация, информационная система, доступ к информации, конфиденциальность информации, защита информации и др.)</li> <li>- классификация информации в зависимости от категории доступа к ней</li> <li>- классификация информации, подлежащей защите.</li> <li>- основные положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»</li> </ul>
2	<p><b>Законодательный уровень информационной безопасности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Доктрина информационной безопасности Российской Федерации</li> <li>- Государственные органы РФ, контролирующие деятельность в области защиты информации</li> <li>- Российское законодательство по защите информации</li> <li>- международные стандарты и спецификации</li> </ul>
3	<p><b>Угрозы информационной безопасности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- источники угроз информационной безопасности и их классификация</li> <li>- угрозы доступности, целостности и конфиденциальности</li> <li>- способы и последствия воздействия источников угроз на объекты информационной безопасности</li> </ul>
4	<p><b>Защита данных и конфиденциальности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- меры для защиты устройств от вторжения</li> <li>- идентификация и аутентификация</li> <li>- парольная защита</li> <li>- резервное копирование данных во внешние хранилища</li> </ul>
5	<p><b>Компьютерные вирусы и защита от них</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- хронология развития компьютерных вирусов</li> <li>- классификация компьютерных вирусов</li> <li>- средства антивирусной защиты</li> </ul>
6	<p><b>Основы криптографии</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- основные понятия криптографии, классификация шифров</li> <li>- этапы развития криптографии</li> <li>- симметричные шифры (схема Фейстеля, DES, AES, ГОСТ 28147-89, BlowFish)</li> <li>- асимметричные шифры (схема Диффи-Хеллмана, система RSA)</li> </ul>
7	<p><b>Электронная подпись</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- история и принципы создания ЭП</li> <li>- виды ЭП (простая, усиленная, квалифицированная, неквалифицированная)</li> <li>- сертификаты, удостоверяющие центры</li> </ul>
8	<p><b>Стеганография</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- история и основные понятия стеганографии</li> <li>- хеш-функции</li> <li>- цифровые водяные знаки, цифровые отпечатки пальцев</li> <li>- использование особенностей различных форматов файлов</li> </ul>
9	<p><b>Технические средства обеспечения информационной безопасности</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- классификация технических каналов утечки информации</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	- характеристика технических каналов утечки информации - мероприятия по защите информации от утечки по техническим каналам

#### 4.2. Занятия семинарского типа.

##### Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Основные положения и нормы Федерального закона «Об информации, информационных технологиях и о защите информации».
2	Угрозы безопасности информации. Классификации источников угроз.
3	Численная оценка параметров парольной системы защиты.
4	Программирование алгоритмов шифрования – шифр Цезаря.
5	Программирование алгоритмов шифрования – шифр Виженера.
6	Алгоритм обмена ключами по Диффи-Хелману.
7	Программирование алгоритмов шифрования – схема RSA.
8	Контроль целостности данных с помощью хеш-функции.
9	Стеганография - встраивание и извлечение информации из стегоконтейнера.
10	Средства антивирусной защиты – режимы работы, сравнительная характеристика.

#### 4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

#### 4.4. Примерный перечень тем курсовых работ

1. История криптографии – древний мир.
2. История криптографии – средние века и эпоха Возрождения.
3. История криптографии – знаменитые шифры XX века.
4. Приборы и программы/утилиты для экстренного уничтожения информации.
5. Уязвимости мессенджеров, кибератаки на них, способы обеспечения безопасности и сохранения конфиденциальности.

6. Обзор систем биометрической идентификации.
7. Инженерные конструкции и сооружения для защиты информации.
8. Технические средства обеспечения информационной безопасности – аппаратура активной защиты от ПЭМИН.
9. Технические средства обеспечения информационной безопасности – аппаратура маскирования телефонных переговоров.
10. Технические средства обеспечения информационной безопасности – аппаратура защиты служебных помещений от акустического, виброакустического и оптического несанкционированного снятия информации.
11. Программная реализация алгоритмов шифрования - шифр древней Спарты.
12. Программная реализация алгоритмов шифрования - решётка Кардано.
13. Программная реализация алгоритмов шифрования - шифр четырёх квадратов.
14. Стеганография в HTML-файлах и её программная реализация.
15. Стеганография в BMP-файлах и её программная реализация.
16. Стеганография в JPEG-файлах и её программная реализация.

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

№ п/п	Библиографическое описание	Место доступа
1	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/165837">https://e.lanbook.com/book/165837</a> Л.М. Груздева Книга Юридический институт МИИТа , 2018	Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/165837">https://e.lanbook.com/book/165837</a>
2	Алгоритмы шифрования В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. "САПР транспортных конструкций и сооружений" Однотомное издание МИИТ , 2005	НТБ (ЭЭ); НТБ (уч.1)

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

Официальный сайт РУТ (МИИТ) (<https://www.miit.ru/>).

Научно-техническая библиотека РУТ (МИИТ) (<http://library.miit.ru>).

Образовательная платформа «Юрайт» (<https://urait.ru/>).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (<http://e.lanbook.com/>).

Электронно-библиотечная система [ibooks.ru](http://ibooks.ru) (<http://ibooks.ru/>).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Microsoft Visual Studio C++.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 3 семестре.

Курсовая работа в 3 семестре.

10. Оценочные материалы.

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

Авторы:

старший преподаватель кафедры  
«Системы автоматизированного  
проектирования»

Э.Р. Резникова

Согласовано:

Заведующий кафедрой САП

И.В. Нестеров

Председатель учебно-методической  
комиссии

М.Ф. Гуськова