

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



Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной первым проректором ФГАОУ ВО
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 ФГАОУ ВО РУТ
(МИИТ)

ID подписи: 2899

Подписал: заведующий кафедрой Нестеров Иван
Владимирович

Дата: 01.09.2026

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-4 - Способен решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и технологий искусственного интеллекта, а также с учетом основных требований информационной безопасности.

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	Семестр №4
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	Основные понятия в области информационной безопасности Рассматриваемые вопросы: - базовые понятия (информация, информационная система, доступ к информации, конфиденциальность информации, защита информации и др.) - классификация информации в зависимости от категории доступа к ней - классификация информации, подлежащей защите. - основные положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

№ п/п	Тематика лекционных занятий / краткое содержание
2	Законодательный уровень информационной безопасности Рассматриваемые вопросы: - Доктрина информационной безопасности Российской Федерации - Государственные органы РФ, контролирующие деятельность в области защиты информации - Российское законодательство по защите информации - международные стандарты и спецификации
3	Угрозы информационной безопасности Рассматриваемые вопросы: - источники угроз информационной безопасности и их классификация - угрозы доступности, целостности и конфиденциальности - способы и последствия воздействия источников угроз на объекты информационной безопасности
4	Защита данных и конфиденциальности Рассматриваемые вопросы: - меры для защиты устройств от вторжения - идентификация и аутентификация - парольная защита - резервное копирование данных во внешние хранилища
5	Компьютерные вирусы и защита от них Рассматриваемые вопросы: - хронология развития компьютерных вирусов - классификация компьютерных вирусов - средства антивирусной защиты
6	Основы криптографии Рассматриваемые вопросы: - основные понятия криптографии, классификация шифров - этапы развития криптографии - симметричные шифры (схема Фейстеля, DES, AES, ГОСТ 28147-89, BlowFish) - асимметричные шифры (схема Диффи-Хеллмана, система RSA)
7	Электронная подпись Рассматриваемые вопросы: - история и принципы создания ЭП - виды ЭП (простая, усиленная, квалифицированная, неквалифицированная) - сертификаты, удостоверяющие центры
8	Стеганография Рассматриваемые вопросы: - история и основные понятия стеганографии - хеш-функции - цифровые водяные знаки, цифровые отпечатки пальцев - использование особенностей различных форматов файлов
9	Технические средства обеспечения информационной безопасности Рассматриваемые вопросы: - классификация технических каналов утечки информации - 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». Рассмотрение основных положений и норм Федерального закона «Об информации, информационных технологиях и о защите информации»
2	Угрозы безопасности информации. Классификации источников угроз. Рассмотрение классификации источников угроз информационной безопасности
3	Численная оценка параметров парольной системы защиты. Изучение численной оценки параметров парольной системы защиты
4	Программирование алгоритмов шифрования – шифр Цезаря. Программирование защиты информации на основе шифра Цезаря
5	Программирование алгоритмов шифрования – шифр Виженера. Программирование защиты информации на основе шифра Виженера
6	Алгоритм обмена ключами по Диффи-Хелману. Программирование защиты информации по алгоритму Диффи-Хелмана
7	Программирование алгоритмов шифрования – схема RSA. Программирование защиты информации на основе схемы RSA
8	Контроль целостности данных с помощью хеш-функции. Программирование контроля целостности данных с помощью хеш-функции
9	Стеганография - встраивание и извлечение информации из стегоконтейнера. Изучение стеганографического способа кодирования информации
10	Средства антивирусной защиты – режимы работы, сравнительная характеристика. Изучение средств 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	Гулятьева Т.А. Основы информационной безопасности: учебное пособие / Т.А. Гулятьева. - Новосибирск : Новосибирский государственный технический университет, 2018. - 79 с. - ISBN 978-5-7782-3640-0	https://ibooks.ru/bookshelf/367759/reading . - Текст: электронный.
2	Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3	https://urait.ru/bcode/544029 .
3	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для	https://urait.ru/bcode/536132

вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3	
--	--

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

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

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

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 4 семестре.

Курсовая работа в 4 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 в строительстве»

Э.Р. Резникова

Согласовано:

Заведующий кафедрой САПвС

И.В. Нестеров

Председатель учебно-методической
комиссии

М.Ф. Гуськова