

**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  
10.03.01 Информационная безопасность,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Защита программ и данных**

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

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: 4196  
Подписал: заведующий кафедрой Желенков Борис  
Владимирович  
Дата: 29.05.2026

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

Целями освоения учебной дисциплины являются:

- формирование компетенций по основным разделам теоретических и практических основ проектирования современных систем защиты информации в компьютерных системах;

- изучение методов построения систем антивирусной защиты, а также способов сокрытия информации с использованием криптографических и стеганографических методов.

Задачами дисциплины являются:

- изучение особенностей практического применения методов и средств защиты информации;

- ознакомление с особенностями работы и проектирования современных средств защиты программ и данных;

- изучение особенностей практического применения средств антивирусной защиты и ее актуализации;

- изучение технологий обнаружения вирусов в современных системах антивирусной защиты;

- изучение способов сокрытия информации криптографическими методами;

- изучение способов сокрытия информации стеганографическими методами.

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

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

**ОПК-7** - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;

**ПК-2** - способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

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

**Знать:**

- основные методы разработки политик информационной безопасности, администрирования средств защиты информации в компьютерных системах и сетях;

- программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач.

**Уметь:**

- применять на практике программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

- разрабатывать политики информационной безопасности, администрировать подсистемы информационной безопасности объекта защиты.

**Владеть:**

- навыками выбора и применения на практике программных средств системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

- навыками разработки политик информационной безопасности, администрирования подсистем информационной безопасности объекта защиты.

**3. Объем дисциплины (модуля).**

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

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №6
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 60 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>Методы и средства защиты информации</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Классификация методов и средств защиты информации;</li> <li>- Методы: препятствие, управление, маскировка, регламентация, принуждение, побуждение;</li> <li>- Средства: физические, аппаратные, программные, организационные, законодательные, психологические;</li> <li>- Практическое применение методов и средств защиты информации в современных корпоративных сетях.</li> </ul>
2	<p>Антивирусная защита. Вирусы и их классификация</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Информационная и кибербезопасность;</li> <li>- Проблема криминализации информационного пространства;</li> <li>- Вирусные атаки: потенциальные угрозы и методы защиты;</li> <li>- Решение задач антивирусной защиты на мировом уровне;</li> <li>- Вредоносные программы: компьютерные вирусы, черви, трояны и пр;</li> <li>- Загрузочные и файловые вирусы;</li> <li>- Макровирусы и скрипт-вирусы;</li> <li>- Шифрование и метаморфизм;</li> <li>- Черви: сетевые, почтовые, IM, IRC, P2P;</li> <li>- Трояны: клавиатурные шпионы, похитители паролей, утилиты скрытого удаленного управления, анонимные прокси-сервера, утилиты дозвона, логические бомбы, модификаторы настроек браузера;</li> <li>- Условно опасные программы: Riskware, Рекламные утилиты (adware), Pornware, злые шутки;</li> <li>- Поиск и анализ актуальной информации о современных методах и средствах антивирусной защиты;</li> <li>- Применение перспективных методов исследования и решения профессиональных задач при разработке программ антивирусной защиты в государственных и коммерческих предприятиях России.</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
3	<p><b>Современные методы защиты от вирусов</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд);</li> <li>- К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд;</li> <li>- Методы, основанные на отслеживании поведения программ при их выполнении;</li> <li>- Протоколирование всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.</li> </ul>
4	<p><b>Современные методы защиты от вирусов (продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Методы регламентации порядка работы с файлами и программами;</li> <li>- Наиболее популярные антивирусные программы и их особенности: McAfee, Norton, Panda, Avira, Bitdefender, Bullguard, Heimdal; Антивирус Касперского;</li> <li>- Поиск и анализ актуальной информации о применении наиболее популярных антивирусных программ в современных корпоративных системах киберзащиты.</li> </ul>
5	<p><b>Антивирусная защита компьютерной сети и мобильных пользователей</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Корпоративные компьютерной сети;</li> <li>- Рабочие станции и сетевые серверы, почтовые серверы и шлюзы;</li> <li>- Уровни антивирусной защиты: уровень защиты рабочих станций и сетевых серверов, уровень защиты почтовых серверов, уровень защиты шлюзов;</li> <li>- Централизованное управление антивирусной защитой;</li> <li>- Компоненты системы удаленного централизованного управления: клиентская антивирусная программа, сервер администрирования, агент администрирования, консоль администрирования.</li> </ul>
6	<p><b>Антивирусная защита компьютерной сети и мобильных пользователей (продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Организация сбора статистики в системе антивирусной защиты;</li> <li>- Антивирусы для мобильных устройств;</li> <li>- Политики обеспечения информационной безопасности при работе с мобильными устройствами;</li> <li>- Политика «нулевого доверия»;</li> <li>- Поиск и анализ актуальной информации о современных антивирусных программах для защиты компьютерных сетей и их использовании;</li> <li>- Проектирование антивирусного ПО для защиты компьютерных сетей.</li> </ul>
7	<p><b>Криптография и ее применение при защите данных в корпоративной сети предприятия</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Криптография: определение, история, применение в современных задачах сокрытия информации;</li> <li>- Терминология и ГОСТы: открытый (исходный) текст, шифротекст, ключ, шифрование, асимметричный шифр, открытый ключ, закрытый ключ, криптоанализ;</li> <li>- Криптографические методы и алгоритмы.</li> </ul>
8	<p><b>Криптография и ее применение при защите данных в корпоративной сети предприятия (продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Симметричные и асимметричные алгоритмы;</li> <li>- Хеш-функции;</li> <li>- Практическое применение криптографии в задачах защиты информации;</li> <li>- Поиск и анализ актуальной информации о современных методах и средствах криптографической</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	защиты; - Применение перспективных методов и средств криптографии при разработке систем защиты информации.
9	<p>Стеганография и ее применение при защите данных в корпоративной сети предприятия</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Стеганография: определение, история, применение в современных задачах сокрытия информации;</li> <li>- Стеганосистема и ее элементы;</li> <li>- Поточковый и фиксированный контейнеры;</li> <li>- Стежоключ и стегоканал;</li> <li>- Сокрытие информации в фото-, видео- и аудиофайлах.</li> </ul>
10	<p>Стеганография и ее применение при защите данных в корпоративной сети предприятия (продолжение)</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Практическое применение стеганографии;</li> <li>- Совместное применение криптографических и стеганографических методов в задачах защиты данных;</li> <li>- Поиск и анализ актуальной информации о современных методах и средствах стеганографической защиты;</li> <li>- Применение перспективных методов и средств стеганографии при разработке систем защиты информации.</li> </ul>
11	<p>Требования о защите информации, не составляющей государственную тайну (приказ ФСТЭК №17 от 11.02.2013)</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Требования к организации защиты информации, содержащейся в информационной системе;</li> <li>- Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы;</li> <li>- Три класса защищенности информационной системы;</li> <li>- Разработка системы защиты информации информационной системы;</li> <li>- Разработка организационно-распорядительных документов по защите информации;</li> <li>- Аттестация информационной системы и ввод ее в действие;</li> <li>- Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.</li> </ul>
12	<p>Утечки конфиденциальной информации</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Основные виды утечек конфиденциальной информации;</li> <li>- Источники конфиденциальной информации и их уязвимости: персонал, носители информации, технические средства, средства коммуникации, передаваемые по каналам связи сообщения;</li> <li>- Каналы утечки;</li> <li>- Основы организации инженерно-технической защиты информации на предприятии;</li> <li>- Классификация технических каналов утечки информации;</li> <li>- Мероприятия и средства защиты информации от утечки по техническим каналам на объектах информатизации;</li> <li>- Физические средства защиты информации;</li> <li>- Программно-аппаратные средства защиты информации;</li> <li>- Криптографические средства защиты;</li> <li>- Оценка эффективности методов и средств технической защиты информации.</li> </ul>
13	<p>Объекты защиты информации</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Угрозы безопасности информации;</li> <li>- Модель угроз;</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- Источники угроз: нарушитель, аппаратная закладка, вредоносная программа;</li> <li>- Угрозы доступа (проникновения), угрозы создания нештатных режимов работы ПО, угрозы внедрения вредоносных программ;</li> <li>- Оценка угроз безопасности информации;</li> <li>- Виды нарушителей;</li> <li>- Модель нарушителя;</li> <li>- Уязвимости информационной системы (ИС);</li> <li>- Типы уязвимостей ИС;</li> <li>- Уязвимости конфигурации и архитектуры;</li> <li>- Организационная уязвимость;</li> <li>- Технические каналы утечки информации и их особенности;</li> <li>- Объекты информатизации и их характеристики.</li> </ul>
14	<p>Стандартизация и сертификация в области защиты информации</p> <ul style="list-style-type: none"> <li>- Система ГОСТов в области защиты информации: ГОСТ Р 52069;0-2013;</li> <li>- Общие технические требования к защите от несанкционированного доступа к информации в ГОСТ Р 50739;</li> <li>- Основные требования и определения в ГОСТ Р 50922;</li> <li>- Порядок создания автоматизированных систем в защищенном исполнении в ГОСТ Р 51583;</li> <li>- Стандартизация номенклатуры качества защиты информации в ГОСТ Р 52447;</li> <li>- Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633.</li> </ul>
15	<p>Стандартизация и сертификация систем искусственного интеллекта</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Федеральный проект «Искусственный интеллект» и проблемы стандартизации и сертификации;</li> <li>- Стандартизация и унификация представления правовой информации для цифровой платформы «Государственная система правовой информации»;</li> <li>- ПНСТ «Умное производство»;</li> <li>- Двойники цифровые производства» (части 1-4);</li> <li>- ПНСТ «Информационные технологии»;</li> <li>- Умный город;</li> <li>- Функциональная совместимость.</li> </ul>
16	<p>Стандартизация и сертификация систем искусственного интеллекта (продолжение)</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- ПНСТ «Информационные технологии»;</li> <li>- Умный город;</li> <li>- Руководства по обмену и совместному использованию данных»;</li> <li>- ПНСТ «Информационные технологии»;</li> <li>- Интернет вещей;</li> <li>- Протокол обмена для высокочастотных сетей с большим радиусом действия и низким энергопотреблением».</li> </ul>

#### 4.2. Занятия семинарского типа.

##### Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	<p>Изучение функционала пакета антивирусных программ</p> <p>В результате выполнения практического задания студент получает навыки в выборе и практическом использовании функционала антивирусных программ при защите домашнего компьютера и корпоративной сети.</p>

№ п/п	Тематика практических занятий/краткое содержание
2	Разработка концепции информационной безопасности предприятия В результате выполнения практического задания студент получает навыки в разработке концепции информационной безопасности предприятия.
3	Импортозамещение программных средств В результате выполнения практического задания студент получает навыки в обоснованном выборе российских программных средств для замены иностранных.
4	Проверка наличия уязвимостей печатающих устройств в базе данных ФСТЭК В результате выполнения практического задания студент получает навыки в обнаружении известных уязвимостей в КТС предприятия.
5	Криптография. Соккрытие информации криптографическими методами В результате выполнения практического задания студент получает навыки в сокрытии информации криптографическими средствами.
6	Стеганография. Соккрытие информации в фотофайле В результате выполнения практического задания студент получает навыки в сокрытии зашифрованной информации в фотофайле.
7	Стеганография. Соккрытие информации в видео- и аудиофайлах В результате выполнения практического задания студент получает навыки в сокрытии зашифрованной информации в видео- и аудиофайлах.
8	Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633 В результате выполнения практического задания студент получает навыки разработки средств высоконадежной биометрической аутентификации в соответствии с требованиями ГОСТов.

#### 4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Работа с лекционным материалом
3	Изучение вопросов для самостоятельной дополнительной проработки
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	Диогенес Ю., Озкайя Э. Кибербезопасность. Стратегия атак и обороны. Издательство "ДМК Пресс", 2020 - 326с. – ISBN 978-5-97060-709-1	<a href="https://e.lanbook.com/book/183115">https://e.lanbook.com/book/183115</a> (дата обращения: 28.05.2026)- Текст электронный.
2	Мосолов А. С., Акинин Н. И. Компьютерные технологии и методы проектирования в сфере	<a href="https://e.lanbook.com/book/438971">https://e.lanbook.com/book/438971</a> (дата обращения: 16.03.2025)- Текст электронный.

	безопасности. Издательство "Лань", 2021 - 444с. – ISBN 978-5-8114-8034-0	
3	Баланов А. Н. Защита информационных систем. Кибербезопасность: Учебное пособие для вузов. Издательство "Лань", 2025 - 280с. – ISBN 978-5-507-50467-1	<a href="https://e.lanbook.com/book/438971">https://e.lanbook.com/book/438971</a> (дата обращения: 28.05.2026)- Текст электронный.
4	Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1	<a href="https://e.lanbook.com/book/156401">https://e.lanbook.com/book/156401</a> (дата обращения: 28.05.2026)- Текст электронный.
5	Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1	<a href="https://e.lanbook.com/book/130184">https://e.lanbook.com/book/130184</a> (дата обращения: 28.05.2026).- Текст электронный.
6	Прохорова О. В. Информационная безопасность и защита информации. Издательство "Лань", 2022 - 124с. – ISBN 978-5-8114-8924-4	<a href="https://e.lanbook.com/book/185333">https://e.lanbook.com/book/185333</a> (дата обращения: 28.05.2026).- Текст электронный.
7	Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8	<a href="https://e.lanbook.com/book/167186">https://e.lanbook.com/book/167186</a> (дата обращения: 28.05.2026).- Текст электронный.
8	Ермакова А.Ю. Методы и средства защиты компьютерной информации: учебное пособие. МИРЭА - Российский технологический университет, 2020.-223с	<a href="https://e.lanbook.com/book/163844">https://e.lanbook.com/book/163844</a> (дата обращения: 28.05.2026).- Текст электронный
9	Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с	<a href="https://e.lanbook.com/book/18249">https://e.lanbook.com/book/18249</a> (дата обращения: 28.05.2026).- Текст электронный.

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

- Форум специалистов по информационным технологиям <http://citforum.ru/>
- Интернет-университет информационных технологий <http://www.intuit.ru/>
- Тематический форум по информационным технологиям <http://habrahabr.ru/>
- ЭБС "Лань" <https://e.lanbook.com/book/>

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

Microsoft Windows

Microsoft Office

Интернет-браузер (Yandex и др.)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий, лабораторных работ, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации):

- компьютер преподавателя, проектор, экран проекционный, рабочие станции студентов, маркерная доска.

Аудитория подключена к сети «Интернет»

9. Форма промежуточной аттестации:

Зачет в 6 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  
«Вычислительные системы и  
квантовые коммуникации»

С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической  
комиссии

Н.А. Андриянова