**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 специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Основы информационной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе 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 ФГАОУ ВО РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины (модуля) «Основы информационной безопасности» являются:

– обучить студентов принципам обеспечения информационной безопасности, подходам к анализу информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;

– содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи изучения дисциплины:

- изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации в компьютерных системах;

- изучение типовых угроз безопасности информации при её обработке в компьютерных системах;

- изучение основных принципов обеспечения информационной безопасности;

- изучение основ построения модели угроз и политики безопасности;

- изучение основных моделей управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

**ОПК-1** - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

**ПК-3** - Способен принимать участие в теоретических и экспериментальных исследованиях систем защиты информации, проводить научно-исследовательские работы по оценке защищенности информации в компьютерных системах.

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

**Знать:**

- Основные нормативные правовые акты и доктринальные документы (Доктрина информационной безопасности РФ), определяющие национальные интересы в информационной сфере.

- Основные методы и механизмы защиты информации в ОС (управление доступом, аудит, шифрование дисков), в КС (межсетевое экранирование, VPN, IDS/IPS) и в СУБД (избирательное и мандатное управление доступом, шифрование данных, ролевая модель).

- Современные методы и средства оценки защищенности компьютерных систем, включая стандарты и методики (PCI DSS, методики ФСТЭК, BAS (Breach and Attack Simulation) и др.).

**Уметь:**

- Анализировать события и явления общественной жизни с точки зрения их информационной составляющей и влияния на безопасность.

- Выбирать и применять адекватные программные и аппаратные средства защиты для конкретных условий эксплуатации системы.

- Проводить сбор и анализ исходных данных, необходимых для расчета показателей защищенности информации.

**Владеть:**

- Навыками критического анализа информации, получаемой из различных источников (СМИ, соцсети, научная литература), для выявления деструктивных воздействий.

- Навыками администрирования средств защиты информации в составе ОС, КС и СУБД (настройка прав доступа, создание правил МЭ, разграничение доступа к таблицам БД).

- Навыками работы со специализированными инструментальными средствами для анализа защищенности (сканеры уязвимостей, фреймворки для пентеста, анализаторы протоколов).

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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): | 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 24 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 | Национальная безопасность Российской Федерации: понятие, структура и место информационной безопасности<br>Рассматриваемые вопросы:<br>- Понятие, сущность и содержание национальной безопасности.<br>- Основные задачи, объекты и субъекты обеспечения национальной безопасности.<br>- Виды безопасности и виды защищаемой информации.<br>- Место и роль России в глобальном информационном пространстве.<br>- Понятие и роль информационной безопасности в обеспечении национальной безопасности государства.<br>- Национальные интересы России в информационной сфере (интересы личности, общества и государства). |
| 2 | Система угроз информационной безопасности Российской Федерации<br>Рассматриваемые вопросы:<br>- Общая характеристика проблем обеспечения информационной безопасности.<br>- Виды угроз: угрозы конституционным правам, угрозы информационному обеспечению госполитики, угрозы развитию отечественной индустрии информации.<br>- Классификация угроз безопасности информационных и телекоммуникационных систем.<br>- Модель действий нарушителя.<br>- Внешние и внутренние источники угроз ИБ РФ.<br>- Классификация источников угроз и уязвимостей. |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| 3 | Информационное противоборство и информационная война: основные концепции<br>Рассматриваемые вопросы:<br>- Информационная безопасность и информационное противоборство.<br>- Понятие, цели и проблемы информационных войн.<br>- Субъекты информационного противоборства.<br>- Составные части и методы информационного противоборства. |
| 4 | Методология и стратегия ведения информационной войны<br>Рассматриваемые вопросы:<br>- Информационная война как целенаправленное воздействие на информационные системы.<br>- Способы перепрограммирования информационных систем (психологические и технические аспекты).<br>- Проблема начала информационной войны.<br>- Обобщенный алгоритм (типовая стратегия) информационной войны.<br>- Основные аспекты и последствия информационной войны. |
| 5 | Организационно-правовые основы защиты информации. Классификация автоматизированных систем<br>Рассматриваемые вопросы:<br>- Документы Гостехкомиссии (ФСТЭК) при Президенте Российской Федерации.<br>- Концепции защиты автоматизированных систем (АС) и средств вычислительной техники (СВТ).<br>- Классификация автоматизированных систем и информационных систем по уровню защищенности.<br>- Требования к информационным системам по обеспечению безопасности информации. |
| 6 | Система защиты информации от несанкционированного доступа (НСД)<br>Рассматриваемые вопросы:<br>- Основные направления защиты от НСД и способы НСД.<br>- Принципы защиты информации от НСД.<br>- Структура системы защиты информации от НСД: назначение и функции элементов.<br>- Политика безопасности как основа построения системы защиты. |
| 7 | Модели управления доступом<br>Рассматриваемые вопросы:<br>- Правила разграничения доступа.<br>- Дискреционная (DAC) и мандатная (MAC) модели управления доступом.<br>- Ролевая модель управления доступом (RBAC).<br>- Атрибутные модели управления доступом (ABAC). |
| 8 | Основы криптографической защиты информации<br>Рассматриваемые вопросы:<br>- Основные понятия криптографии: шифрование, дешифрование, ключ.<br>- Предмет и задачи криптографии. Историческая справка.<br>- Требования к криптографическим системам.<br>- Симметричное и асимметричное шифрование (базовые понятия).<br>- Примеры простейших шифров. |
| 9 | Идентификация и аутентификация<br>Рассматриваемые вопросы:<br>- Понятия идентификации, аутентификации и авторизации.<br>- Классификация систем аутентификации (по факторам: знание, владение, неотъемлемые характеристики).<br>- Методы аутентификации: парольная, биометрическая, аппаратная (токены, смарт-карты).<br>- Сертификаты и цифровые подписи как средства подтверждения подлинности. |
| 10 | Разграничение и контроль доступа<br>Рассматриваемые вопросы: |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | - Разграничение доступа по виду информации, по способам обработки (чтение, запись, исполнение).<br>- Контекстное управление доступом (по времени, по терминалам).<br>- Разделение привилегий и контроль целостности.<br>- Аудит и мониторинг событий доступа. |
| 11 | Сетевые методы защиты. Межсетевые экраны<br>Рассматриваемые вопросы:<br>- Технология межсетевых экранов (МЭ) как защита корпоративных сетей от внешних угроз.<br>- Функции МЭ: фильтрация трафика, трансляция адресов, посредничество.<br>- Политика безопасности и ее реализация на МЭ.<br>- Типы межсетевых экранов (фильтрующие, прокси-серверы, stateful inspection). |
| 12 | Защищенные каналы связи. Виртуальные частные сети (VPN)<br>Рассматриваемые вопросы:<br>- Основные понятия и функции виртуальных частных сетей (VPN).<br>- Варианты построения защищенных каналов (узел-узел, удаленный доступ).<br>- Протоколы туннелирования (PPTP, L2TP, IPsec).<br>- Средства обеспечения безопасности VPN: шифрование, аутентификация, проверка целостности. |
| 13 | Обнаружение и предотвращение вторжений (IDS/IPS)<br>Рассматриваемые вопросы:<br>- Краткая история развития средств обнаружения атак.<br>- Основные понятия: событие, атака, вторжение, сигнатура, аномалия.<br>- Классификация систем обнаружения вторжений (IDS) и предотвращения вторжений (IPS).<br>- Методы обнаружения: сигнатурный анализ и поведенческий анализ (обнаружение аномалий). |
| 14 | Вредоносное программное обеспечение и методы антивирусной защиты<br>Рассматриваемые вопросы:<br>- Вирусы как угроза информационной безопасности.<br>- Классификация вредоносного ПО (вирусы, черви, трояны, программы-вымогатели).<br>- Средства антивирусной защиты: сигнатурный и эвристический анализ.<br>- Комплексные системы защиты конечных точек (EDR). |
| 15 | Стандартизация в области информационной безопасности<br>Рассматриваемые вопросы:<br>- Характеристика систем стандартизации в области защиты информации (международные, национальные, отраслевые).<br>- Информационная безопасность распределенных систем.<br>- Европейские критерии безопасности информационных технологий (ITSEC) и их эволюция.<br>- Обзор современных стандартов (Common Criteria/ISO 15408, семейство стандартов ISO 27xxx). |
| 16 | Комплексный подход к обеспечению информационной безопасности<br>Рассматриваемые вопросы:<br>- Взаимосвязь правовых, организационных и технических мер защиты.<br>- Политика информационной безопасности организации как документ.<br>- Современные тенденции в области угроз и защиты (кибервойны, атаки на критическую инфраструктуру).<br>- Роль человеческого фактора в обеспечении ИБ. |

4.2. Занятия семинарского типа.

Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | Основы информационной безопасности и информационная инфраструктура РФ<br>В результате выполнения задания студент умеет: классифицировать виды информации и методы её защиты, применять понятийный аппарат информационной безопасности и анализировать элементы информационной инфраструктуры государства. |
| 2 | Угрозы информационной безопасности, информационно-технологическое оружие и информационная война<br>В результате выполнения задания студент умеет: классифицировать источники и виды угроз ИБ, анализировать формы применения информационно-технологического оружия и оценивать возможные последствия информационной войны. |
| 3 | Утечки информации и формальная постановка задачи безопасности компьютерных систем<br>В результате выполнения задания студент умеет: выявлять причины и каналы утечки/искажения информации и формализовать задачу обеспечения безопасности компьютерной системы. |
| 4 | Модели организации кибернетической безопасности и модели управления доступом<br>В результате выполнения задания студент умеет: применять дискреционную и ролевую модели доступа, анализировать защищённость систем с использованием модели Лендвера–Маклина и выбирать модель организации кибербезопасности. |
| 5 | Оценка защищённости, средства обеспечения ИБ и разграничение доступа в БД<br>В результате выполнения задания студент умеет: оценивать защищённость компьютерных систем, выбирать методы и программно-аппаратные средства обеспечения ИБ и строить систему разграничения доступа в базе данных на основе ролевой модели. |
| 6 | Криптографическая защита, аутентификация, электронная подпись и VPN<br>В результате выполнения задания студент умеет: реализовывать простейший шифр, классифицировать системы аутентификации, применять электронную подпись для контроля целостности и выбирать варианты построения защищённых VPN-каналов. |
| 7 | Антивирусные комплексы и профилактика «троянских программ»<br>В результате выполнения задания студент умеет: работать с антивирусными комплексами, восстанавливать заражённые файлы и применять меры профилактики проникновения «троянских программ». |
| 8 | Стандарты обеспечения ИБ и документы по оценке защищённости автоматизированных систем в РФ<br>В результате выполнения задания студент умеет: анализировать архитектуру стандартов обеспечения ИБ организации и применять документы РФ по оценке защищённости автоматизированных систем. |

## 4.3. Самостоятельная работа обучающихся.

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

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

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Основы информационной безопасности Нестеров С. А. Учебник Издательство "Лань", - 3-е изд., стер. - 324 с. - ISBN 978-5--507-490777-6 , 2024 | https://reader.lanbook.com/book/370967 |
| 2 | Криптографическая защита информации Кунин Н. Т. Практикум Изд. МИРЭА - Российский технологический университет. - 66 с. - ISBN 978-5-7339-2447-2 , 2025 | https://reader.lanbook.com/book/493382 |
| 3 | Защита информации Груздева Л. М. Учебное пособие Изд. Российский университет транспорта, - 144 с. - ISBN 978-5-7876-0326-2 , 2019 | https://reader.lanbook.com/book/188703 |

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 издательства «Лань» (http://e.lanbook.com/).

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.

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.

10. Оценочные материалы.

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

Авторы:

А.С. Иконников

Согласовано:

Заведующий кафедрой ИУиИБ Л.А. Баранов

Председатель учебно-методической комиссии Н.А. Андриянова