**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)

## Защита информации

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Вычислительные системы и сети

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Защита информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Основными задачами дисциплины являются:

- освоение студентами базовых методов и средств защиты информации (организационных, технических, программных);
- ознакомление с законодательством и стандартами в этой области;
- студенты должны изучить теоретические основы компьютерной безопасности и уметь применять теорию на практике.

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-7** - Способен участвовать в настройке и наладке программно-аппаратных комплексов;

**ПК-5** - Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.

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

**Знать:**

- виды защиты информации, основные понятия и определения;
- стандарты и нормативные документы оценки информационной безопасности (ИБ) программного обеспечения и средств вычислительной техники;
- типы атак и методы противодействия атакам;
- службы и механизмы безопасности;
- методы шифрования;
- алгоритмы симметричных и ассиметричных криптосистем;
- информационный процесс управления криптографическими ключами;
- виды и алгоритмы электронной подписи (ЭП);

- концепцию построения систем защиты информации;
- основы квантовой криптографии.

**Уметь:**

- применять на практике методы противодействия атакам, методы и средства защиты информации от несанкционированного доступа (НСД);
- определять технические каналы утечки информации и способы их закрытия;
- использовать стандарты и нормативные документы при анализе ИБ и/или при построении системы защиты;
- использовать на практике службы и механизмы безопасности;
- структурировать угрозы ИБ, определять модель угроз и модель нарушителя;
- разрабатывать архитектуру и определять состав системы обеспечения информационной безопасности.

**Владеть:**

- навыками оценки вероятности возникновения угроз ИБ и проведения анализа рисков реализации угроз;
- навыками формирования политики безопасности;
- основами проектирования систем защиты информации;
- навыками применения инженерно-технических, программно-аппаратных и криптографических средств защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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): | 80 | 80 |
| В том числе: | | |

| | | |
|---|---|---|
| Занятия лекционного типа | 48 | 48 |
| 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 100 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 | 1 Правовые и организационные методы защиты информации.<br>Рассматриваемые вопросы:<br>- методы и средства защиты компьютерной информации;<br>- законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации);<br>- виды защиты информации;<br>- стандарты (оценочные стандарты и технические спецификации);<br>- организации-разработчики стандартов.<br><br>2 Угрозы безопасности информации.<br>Рассматриваемые вопросы:<br>- характеристики угроз, служб и механизмов безопасности (виды, взаимосвязь между службами и реализующими их механизмами);<br>- классификация угроз (пути их реализации; комплекс требований к системе компьютерной безопасности);<br>- способы несанкционированного доступа;<br>- основные способы и каналы утечки информации;<br>- преодоление программных средств защиты.<br><br>3 Стандарты и нормативные документы оценки информационной безопасности.<br>Рассматриваемые вопросы:<br>- Международные: рекомендации X.800, Общие критерии оценки безопасности информационных технологий, ISO/IEC 27000:2018 и другие; |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | - Федеральные стандарты, критерии, ГОСТы, руководящие и нормативные документы;<br>- защита автоматизированных систем и средств вычислительной техники: классификация, требования по защите информации от НСД, классы защищенности;<br>- стандарты безопасности в сети Internet: МЭ, протоколы защищенной передачи информации.<br><br>4 Аппаратно-программные средства защиты информации.<br>Рассматриваемые вопросы:<br>- основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки);<br>- криптопроцессоры;<br>- уровни защиты информации;<br>- защита от изменения потока сообщений и прерывания передачи, защита от навязывания ложных сообщений в каналы связи;<br>- способы защиты сетей (сетевые атаки и методы противодействия, связь между характеристиками развития вирусной атаки и сетевой структурой);<br>- межсетевые экраны.<br><br>5 Безопасность программного обеспечения, технических средств вычислительных систем и сетей.<br>Рассматриваемые вопросы:<br>- методы и средства анализа безопасности программного обеспечения;<br>- анализ безопасности технических средств компьютерных систем;<br>- подходы к оценке информационной безопасности в сетях;<br>- типы сетевых атак;<br>- методы противодействия атакам<br><br>6 Криптографические ключи.<br>Рассматриваемые вопросы:<br>- управление криптографическими ключами (виды ключей, процедуры управления ключами);<br>- генерация ключей;<br>- хранение ключей;<br>- распределение ключей.<br><br>7 Симметричные и ассиметричные криптосистемы.<br>Рассматриваемые вопросы:<br>- стандарты шифрования данных (алгоритм шифрования данных DES, Triple DES, AES, алгоритм Ривеста);<br>- Российский стандарт крипто- и имитозащиты сообщений;<br>- концепция криптосистемы с открытым ключом;<br>- криптосистема шифрования данных RSA, схемы шифрования Полига-Хеллмана, Эль Гамаля, комбинированный метод шифрования.<br><br>8 Электронная подпись.<br>Рассматриваемые вопросы:<br>- проблема аутентификации данных;<br>- однонаправленные хэш-функции (использование в ЭП, стандарты хэш-функций);<br>- алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП);<br>- подписи с дополнительными функциональными свойствами (слепая ЭП, быстрая, неоспоримая).<br><br>9 Проектирование и анализ систем обеспечения информационной безопасности.<br>Рассматриваемые вопросы:<br>- принципы построения систем защиты информации;<br>- основы политики безопасности (понятие политики безопасности, реализация политики безопасности, |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | модели безопасности);<br>- аудит безопасности, анализ рисков, разработка Концепции обеспечения ИБ;<br>- архитектура системы защиты;<br>- разработка организационной и функциональной структуры системы защиты;<br>- подготовка ТЗ;<br>- проектирование (разработка технического проекта), разработка политик, процедур, регламентов и т.п.;<br>- разработка рабочего проекта, анализ и выбор программных и технических средства защиты информации;<br>- организационные этапы.<br><br>10 Квантовая криптография.<br>Рассматриваемые вопросы:<br>- основные понятия и определения;<br>- квантовые сети, суть квантовой передачи данных;<br>- квантовая телепортация и экспериментальная реализация;<br>- виды ошибок при передаче информации;<br>- протоколы подготовки и измерения, протоколы основанные на запутанности. |

## 4.2. Занятия семинарского типа.

## Лабораторные работы

| № п/п | Наименование лабораторных работ / краткое содержание |
|---|---|
| 1 | 1. АНАЛИЗ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.<br>В результате выполнения лабораторной работы студент получит знания о наиболее востребованных инженерно-технических средствах защиты информации.<br><br>2. РЕКОМЕНДАЦИИ X.800 ДЛЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ.<br>В результате выполнения лабораторной работы студент получит навыки применения рекомендаций X.800.<br><br>3. ПОЛОЖЕНИЯ ISO 15408 («COMMON CRITERIA»).<br>Студент получит навыки применения «Common Criteria» при формировании политики безопасности и системы оценок эффективности, а также при проведении комплексных испытаний защищенности объекта информатизации.<br><br>4. МЕЖСЕТЕВЫЕ ЭКРАНЫ.<br>В результате работы студент получит навыки применения МЭ.<br><br>5. ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ.<br>В результате выполнения лабораторной работы студент получит навыки применения Руководящих документов.<br><br>6. ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ.<br>В результате выполнения лабораторной работы будут зашифрованы и расшифрованы сообщения.<br><br>7. СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ.<br>Результат выполнения лабораторной работы – отчет с описанием криптографических алгоритмов, программа работы алгоритмов. |

| № п/п | Наименование лабораторных работ / краткое содержание |
|---|---|
| | 8. ЭЛЕКТРОННАЯ ПОДПИСЬ И ФУНКЦИЯ ХЭШИРОВАНИЯ.<br>Студент получит навыки применения соответствующих стандартов, будет знать процессы формирования и проверки ЭП, особенности использования функции хэширования в схемах ЭП.<br><br>9. РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАШИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ.<br>В результате выполнения лабораторной работы студентом будет подготовлен отчет с описанием этапов разработки системы защиты информации.<br><br>10. АЛГОРИТМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ.<br>В результате выполнения лабораторной работы студентом будет подготовлен отчет об особенностях двух основных категорий протоколов. |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | Изучение дополнительной литературы |
| 2 | Работа с лекционным материалом. |
| 3 | Подготовка к лабораторным занятиям. |
| 4 | Выполнение курсового проекта. |
| 5 | Подготовка к промежуточной аттестации. |
| 6 | Подготовка к текущему контролю. |

4.4. Примерный перечень тем курсовых проектов

Система контроля доступа локальной сети.

Система контроля доступа локальной сети.

1. Разработка системы защиты коммерческой информации предприятия.

2. Система защиты сети на два офисных здания и отдельный центр обработки данных (проводная сеть).

3. Система защиты для локальной беспроводной сети, объединяющей центральный офис, два филиала и ЦОД.

4. Система защиты для локальной сети, объединяющая центральный офис и 2 филиала.

5. Система защиты для локальной беспроводной сети, объединяющая центральный офис, филиал и 5 удаленных рабочих мест.

5. Защита компьютерной система, состоящей из 2- небольших кластеров и офиса с выходом в Интернет.

6. Защита локальной оптической сети на 5 офисных зданий.

7. Система защиты локальной беспроводной сети, объединяющая

центральный офис и 2 удаленных рабочих места.

8. Система защиты двух объединенных центров обработки данных и 2-х офисов.

9. Защита локальной производственной сети, включающей в свой состав несколько роботов.

10. Система защиты проводной локальной сети, объединяющая центральный офис и 1 филиал и ЦОД.

11.Система защиты локальной проводной сети, объединяющая центральный офис, 2 филиала и 3 удаленных рабочих места.

12. Разработка защищенной сети с применением технологий VPN.

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

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8. | https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf(дата обращения: 16.02.2024). - Текст:электронный. |
| 2 | Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN | https://book-pc.ru/bezopasnost/1882-programmno-apparatnye-sredstva-zaschity-informacii.html(дата обращения: 16.02.2024). - Текст:электронный. |

| | | |
|---|---|---|
| | 978-5-534-13221-2. | |
| 3 | Голиков, А. М. Защита информации в инфокоммуникационн ых системах и сетях: учебное пособие / А. М. Голиков. — Москва: ТУСУР, 2015. — 284 с. // Лань: электронно-библиотечная система. | https://e.lanbook.com/book/110336 (дата обращения: 04.10.2022). — Режим доступа: для авториз. пользователей. — Текст: электронный |
| 4 | Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с. — ISBN 978-5-8114-4067-2. Текст: электронный | https://www.litres.ru/book/s-a-nesterov/osnovy-informacionnoy-bezopasnosti-66007377/(дата обращения: 16.02.2024). — Режим доступа: для авториз. пользователей. Текст: электронный. |
| 5 | Лось, А. Б., Нестеренко, А. Ю., Рожков, М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2019. — 473 с. — (Серия: Бакалавр. Академический курс). - ISBN 978-5-534-12474-3. | https://azon.market/image/catalog/v_1/product/pdf/378/3777079.pdf( дата обращения: 18.03.2023). — Режим доступа: для авториз. пользователей.—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/

Поисковые системы: Yandex, Google, Mail.

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/).

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.

Специализированное программное обеспечение не требуется.

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:

- рабочие место преподавателя с персональным компьютером, подключённым к INTERNET;
- специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской;
- рабочие места студентов в компьютерном классе, подключённые к сети INTERNET.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

Курсовой проект в 5 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, доцент, д.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» И.Е. Сафонова

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова