**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 магистратуры
по направлению подготовки
11.04.02 Инфокоммуникационные технологии и системы связи,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Технологии кибербезопасности в инфокоммуникационных системах

Направление подготовки: 11.04.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль): Инфокоммуникационные и нейросетевые технологии передачи и анализа больших данных

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины является формирование у обучающихся компетенций в соответствии с требованиями образовательного стандарта и в формировании у студентов глубоких знаний и практических навыков для защиты информационных систем от киберугроз и обеспечения их безопасности в условиях современных вызовов.

Задачи дисциплины включают изучение основных принципов и методов защиты информации от киберугроз, а также анализ современных технологий и инструментов для обеспечения безопасности сетей и систем. Студенты должны освоить навыки оценки рисков и разработки стратегий защиты, а также научиться применять полученные знания на практике через решение реальных кейсов в области инфокоммуникаций. Кроме того, важной задачей является формирование критического мышления и способности к адаптации к быстро меняющимся условиям в области кибербезопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

**ОПК-3** - Способен приобретать, обрабатывать и использовать новую информацию в своей предметной области, предлагать новые идеи и подходы к решению задач своей профессиональной деятельности;

**ПК-1** - Способен применять в профессиональной деятельности стандарты, нормативные документы, правовые основы безопасности и конфиденциальности при работе с данными, разработке и внедрении IoT-решений.

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

**Знать:**

- теоретические основы кибербезопасности, включая основные принципы защиты информации, типы киберугроз и уязвимостей, а также современные стандарты и нормативные документы в области информационной безопасности.

**Уметь:**

- проводить комплексный анализ рисков, выявлять уязвимости в системах и разрабатывать эффективные стратегии защиты информации, а также проектировать и внедрять системы безопасности, адаптированные под

конкретные условия и требования организаций, оценивая эффективность применяемых мер защиты

**Владеть:**

- навыками работы с современными инструментами и технологиями кибербезопасности, включая анализ логов, мониторинг сетевого трафика и реагирование на инциденты.

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 №3 |
| Контактная работа при проведении учебных занятий (всего): | 24 | 24 |
| В том числе: | | |
| Занятия лекционного типа | 8 | 8 |
| 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 84 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 | Архитектура инфокоммуникационных систем<br>Рассматриваемые вопросы:<br>Основные компоненты и их взаимодействие<br>Протоколы передачи данных и их безопасность<br>Модели и стандарты безопасности в инфокоммуникациях |
| 2 | Киберугрозы в инфокоммуникационных системах.<br>Рассматриваемые вопросы:<br>Типы угроз и их влияние на системы<br>Методы анализа уязвимостей в инфокоммуникационных системах<br>Примеры атак на инфокоммуникационные системы и их последствия |
| 3 | Средства защиты инфокоммуникационных систем.<br>Рассматриваемые вопросы:<br>Защита сетевой инфраструктуры: фаерволы и VPN<br>Шифрование данных в инфокоммуникационных системах<br>Аутентификация и контроль доступа к системам |
| 4 | Управление рисками в инфокоммуникационных системах<br>Рассматриваемые вопросы:<br>Идентификация и оценка рисков в инфокоммуникациях<br>Разработка и внедрение стратегий управления рисками<br>Мониторинг и оценка эффективности мер защиты |

## 4.2. Занятия семинарского типа.

### Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | Анализ сетевого трафика<br>Рассматриваемые вопросы:<br>Использование Wireshark для захвата и анализа трафика<br>Определение аномалий и подозрительных пакетов<br>Анализ протоколов и выявление уязвимостей |
| 2 | Настройка фаерволов и VPN.<br>Рассматриваемые вопросы:<br>Конфигурация программного и аппаратного фаервола<br>Настройка VPN для безопасного доступа к сети<br>Тестирование безопасности фаервола и VPN-соединения. |
| 3 | Шифрование данных.<br>Рассматриваемые вопросы:<br>Основы симметричного и асимметричного шифрования<br>Практическое использование OpenSSL для шифрования файлов<br>Реализация TLS/SSL для безопасной передачи данных |
| 4 | Тестирование на проникновение.<br>Рассматриваемые вопросы:<br>Основы методологии тестирования на проникновение<br>Использование инструментов, таких как Metasploit и Burp Suite<br>Проведение теста на проникновение в контролируемой среде |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 5 | Управление инцидентами.<br>Рассматриваемые вопросы:<br>Разработка плана реагирования на инциденты<br>Симуляция инцидента и реагирование на него<br>Проведение пост-инцидентного анализа и составление отчета |
| 6 | Мониторинг и управление событиями безопасности<br>Рассматриваемые вопросы:<br>Настройка SIEM-системы для сбора и анализа логов<br>Создание правил для автоматического реагирования на события<br>Анализ отчетов и выявление угроз в реальном времени |
| 7 | Защита персональных данных<br>Рассматриваемые вопросы:<br>Практика применения принципов минимизации данных<br>Реализация мер по защите персональных данных в системах<br>Оценка уязвимостей в системах хранения и обработки данных |
| 8 | Этические аспекты кибербезопасности<br>Рассматриваемые вопросы:<br>Обсуждение кейсов и ситуаций, связанных с этикой в кибербезопасности<br>Разработка кодекса поведения для специалистов по безопасности<br>Ролевые игры для понимания ответственности и последствий действий в киберпространстве |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | Самостоятельное изучение и конспектирование отдельных тем учебной литературы, связынных с разделами дисциплины |
| 2 | Работа с лекционным материалом |
| 3 | Подготовка к практическим занятиям |
| 4 | Подготовка к текущему контролю |
| 5 | Подготовка к промежуточной аттестации. |

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

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Администрирование и кибербезопасность информационных систем : учебное пособие / В. П. Часовских, Г. А. Акчурина, В. Г. Лабунец [и др.]. — Екатеринбург : УрГЭУ, 2022. — 173 с. | https://e.lanbook.com/book/417746 |
| 2 | Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт- | https://e.lanbook.com/book/438971 |

| | | |
|---|---|---|
| | Петербург : Лань, 2025. — 280 с. — ISBN 978-5-507-50467-1. | |
| 3 | Баланов, А. Н. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 680 с. — ISBN 978-5-507-52709-0. | https://e.lanbook.com/book/457463 |

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

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

Единая коллекция цифровых образовательных ресурсов (http://window, edu.ru);

Научно-техническая библиотека РУТ (МИИТ) (http/library.miit.ru);

Поисковые системы «Яндекс» для доступа к тематическим информационным ресурсам;

Электронно-библиотечная система издательства «Лань» – http://e.lanbook.com/;

Электронно-библиотечная система ibooks.ru – http://ibooks.ru/;

Электронно-библиотечная система «УМЦ» – http://www.umczdt.ru/;

Электронно-библиотечная система «BOOK.ru» – http://www.book.ru/;

Электронно-библиотечная система «ZNANIUM.COM» – http://www.znanium.com/

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

1. Операционная система windows microsoft office 2003 и выше;

2. Браузер Internet Explorer 8.0 и выше с установленным Adobe Flash player версии 10.3 и выше;

3. Adobe acrobat.

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.

10. Оценочные материалы.

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

Авторы:

| | |
|---|---|
| доцент, к.н. кафедры «Системы управления транспортной инфраструктурой» | И.М. Губенко |

Согласовано:

| | |
|---|---|
| Заместитель директора | Б.В. Игольников |
| Руководитель образовательной программы | А.С. Киселёва |
| Председатель учебно-методической комиссии | Д.В. Паринов |