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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защищенные беспроводные сети

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

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-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности ;

ПК-3 - Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты.

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

Знать:

-показатели качества работы беспроводных сетей;

-стандарты современных и перспективных систем мобильной связи и беспроводного Интернета;

-требования и стандарты по обеспечению безопасности сетей беспроводного доступа.

Уметь:

- выявлять уязвимости беспроводных сетей, анализировать угрозы и предотвращать атаки на беспроводные сети;

-проводить оценку безопасности беспроводных сетей.

Владеть:

-навыками разработки защищенных беспроводных сетей.

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. №2
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 132 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	Правовые и организационные методы защиты информации Рассматриваемые вопросы: - методы и средства защиты компьютерной информации; - законодательные меры защиты информации (нормативные правовые акты РФ в области защиты информации); - виды защиты информации; - стандарты (оценочные стандарты и технические спецификации); - организации-разработчики стандартов.
2	Угрозы безопасности информации Рассматриваемые вопросы: - характеристики угроз, служб и механизмов безопасности (виды, взаимосвязь между службами и реализующими их механизмами); - классификация угроз (пути их реализации; комплекс требований к системе компьютерной безопасности); - способы несанкционированного доступа; - основные способы и каналы утечки информации; - преодоление программных средств защиты.
3	Стандарты и нормативные документы оценки информационной безопасности Рассматриваемые вопросы: - Международные: рекомендации X.800, Общие критерии оценки безопасности информационных технологий, ISO/IEC 27000:2018 и другие; - Федеральные стандарты, критерии, ГОСТы, руководящие и нормативные документы; - защита автоматизированных систем и средств вычислительной техники: классификация, требования по защите информации от НСД, классы защищенности; - стандарты безопасности в сети Internet: МЭ, протоколы защищенной передачи информации.
4	Аппаратно-программные средства защиты информации Рассматриваемые вопросы: - основные средства защиты компьютерной информации и их функции (Zecurion Zgate; Secret Disk; КриптоПро CSP; другие разработки); - криптопроцессоры; - уровни защиты информации; - защита от изменения потока сообщений и прерывания передачи, защита от навязывания ложных сообщений в каналы связи; - способы защиты сетей (сетевые атаки и методы противодействия, связь между характеристиками развития вирусной атаки и сетевой структурой); - межсетевые экраны.
5	Безопасность программного обеспечения, технических средств вычислительных систем и сетей Рассматриваемые вопросы: - методы и средства анализа безопасности программного обеспечения; - анализ безопасности технических средств компьютерных систем; - подходы к оценке информационной безопасности в сетях; - типы сетевых атак; - методы противодействия атакам; - защита от несанкционированного доступа (основные принципы системы AAA, методы аутентификации); - управление доступом к ресурсам (задачи, требования и модели доступа).
6	Криптографические ключи Рассматриваемые вопросы: - управление криптографическими ключами (виды ключей, процедуры управления ключами);

№ п/п	Тематика лекционных занятий / краткое содержание
	- генерация ключей; - хранение ключей; - распределение ключей
7	Симметричные и ассиметричные криптосистемы Рассматриваемые вопросы: - стандарты шифрования данных (алгоритм шифрования данных DES, Triple DES, AES, алгоритм Ривеста); - Российский стандарт крипто- и имитозащиты сообщений; - концепция криптосистемы с открытым ключом; - криптосистема шифрования данных RSA, схемы шифрования Полига-Хеллмана, Эль Гамаля, комбинированный метод шифрования.
8	Электронная подпись Рассматриваемые вопросы: - проблема аутентификации данных; - однонаправленные хэш-функции (использование в ЭП, стандарты хэш-функций); - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - подписи с дополнительными функциональными свойствами (слепая ЭП, быстрая, неоспоримая).
9	Проектирование и анализ систем обеспечения информационной безопасности Рассматриваемые вопросы: - принципы построения систем защиты информации; - основы политики безопасности (понятие политики безопасности, реализация политики безопасности, модели безопасности); - аудит безопасности, анализ рисков, разработка Концепции обеспечения ИБ; - архитектура системы защиты; - разработка организационной и функциональной структуры системы защиты; - подготовка ТЗ; - проектирование (разработка технического проекта), разработка политик, процедур, регламентов и т.п.; - разработка рабочего проекта, анализ и выбор программных и технических средства защиты информации; - организационные этапы.
10	Квантовая криптография Рассматриваемые вопросы: - основные понятия и определения; - квантовые сети, суть квантовой передачи данных; - квантовая телепортация и экспериментальная реализация; - виды ошибок при передаче информации; - протоколы подготовки и измерения, протоколы основанные на запутанности.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	АНАЛИЗ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В результате выполнения лабораторной работы студент получит знания о наиболее востребованных инженерно-технических средствах защиты информации.
2	РЕКОМЕНДАЦИИ X.800 ДЛЯ РАСПРЕДЕЛЕННЫХ СИСТЕМ В результате выполнения лабораторной работы студент получит навыки применения рекомендаций

№ п/п	Наименование лабораторных работ / краткое содержание
	X.800.
3	ПОЛОЖЕНИЯ ISO 15408 («COMMON CRITERIA»). Студент получит навыки применения «Common Criteria» при формировании политики безопасности и системы оценок эффективности, а также при проведении комплексных испытаний защищенности объекта информатизации.
4	МЕЖСЕТЕВЫЕ ЭКРАНЫ В результате работы студент получит навыки применения МЭ.
5	ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ И СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В результате выполнения лабораторной работы студент получит навыки применения Руководящих документов
6	ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ В результате выполнения лабораторной работы будут зашифрованы и расшифрованы сообщения.
7	ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ Результатом работы является отлаженная программа, реализующая предложенный студентом алгоритм шифрования.
8	ЭЛЕКТРОННАЯ ПОДПИСЬ И ФУНКЦИЯ ХЭШИРОВАНИЯ Студент получит навыки применения соответствующих стандартов, будет знать процессы формирования и проверки ЭП, особенности использования функции хэширования в схемах ЭП.
9	РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАШИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ В результате выполнения лабораторной работы студент получит навыки по разработки системы защиты информации.

4.3. Самостоятельная работа обучающихся.

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

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

№ п/п	Библиографическое описание	Место доступа
1	Вострецова Е.В. Основы информационной	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf(дата обращения: 29.01.2022). - Текст: электронный.

	безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	
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 978-5-534-13221-2.	Образовательная платформа Юрайт [сайт].URL: https://urait.ru/bcode/497433 (дата обращения: 10.10.2022) - Текст: электронный
3	Голиков, А. М. Защита информации в инфокоммуникационных 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. (дата обращения: 04.10.2022)	Лань: электронно-библиотечная система.https://e.lanbook.com/book/206279.Режим доступа:для авториз.пользователей.Текст: электронный
5	Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Криптографическая	Библиотека РУТ http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf (дата обращения 03.03.2023). - Текст: непосредственный.

	защита компьютерной информации: метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М.: МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - ISBN 978-5-9904834-1-5	

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/).

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.

Специализированное программное обеспечение не требуется.

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных

форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

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.

В случае проведении занятии с применением электронного обучения и дистанционных образовательных технологии необходимо наличие компьютернои техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет во 2 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. Клычева