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
09.04.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в сетях

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность (профиль): Компьютерные сети и технологии

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цели освоения дисциплины «Защита информации в сетях»:

- формирование у обучающихся способности понимать сущность и значение информации в развитии современного информационного общества;

- сознавать опасности и угрозы, возникающие в этом процессе;

- соблюдать основные требования информационной безопасности в сетевых технологиях, в том числе защиты государственной тайны;

- формирование у обучающихся способности анализировать и выбирать методы и средства обеспечения защиты информации в сетях.

Студенты должны научиться использовать сочетание различных технологий, протоколов и сетевого оборудования.

Основными задачами дисциплины являются:

- ознакомление основными видами сетевого оборудования;

- изучение методов и средств контроля эффективности защиты информации от утечки по сетям;

- изучение способов и средств защиты информации, обрабатываемой сетевыми технологиями;

- изучение основных принципов и подходов к защите информации в разнотипных сетях и системах.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способность проектировать распределенные информационные системы, их компоненты и протоколы их взаимодействия;

ПК-3 - Способностью формировать технические задания и участвовать в разработке аппаратных и (или) программных средств вычислительной техники.

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

Знать:

- цели, задачи, принципы и основные направления обеспечения информационной безопасности компьютерных сетей;

- методологическую базу в создание систем защиты информации;

- перспективные направления развития средств и методов защиты информации в сетях;

- технические концепции построения различных сетей и систем.

Уметь:

- рассчитывать и выбирать основные параметры аппаратуры сетевого оборудования, исходя из требований к качеству;
- эксплуатировать оборудование сетей;
- осуществлять выбор оборудования и программного обеспечения для построения защищенных сетей связи;
- осуществлять мониторинг сетей.

Владеть:

- навыками расчета и выбора основных параметров сетевого оборудования, исходя из требований к качеству;
- навыками эксплуатации оборудования сетей;
- навыками анализа качества и оценки систем и отдельных методов средств защиты информации в сети;
- навыками интеграции телекоммуникационных сетей связи в сетевую инфраструктуру предприятия, учитывая все аспекты обеспечения ее безопасности;
- принципами мониторинга телекоммуникационных 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	Семестр №3
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	Основы информационной безопасности Рассматриваемые вопросы: - Основные понятия. - Терминология. - Задачи программно-аппаратной защиты информации и основные принципы её построения.
2	Нормативная база Рассматриваемые вопросы: - Нормативно-правое регулирование в области информационной безопасности. - Законы РФ. - Государственные стандарты в области информационной безопасности. - Распоряжение Правительства РФ от 2 декабря 2021 г. № 3427-р Об утверждении стратегического направления в области цифровой трансформации.
3	Защита от несанкционированного доступа Рассматриваемые вопросы: - Классификация методов НСД. - Формирование требований к системе информационной безопасности. - Методы защиты данных от несанкционированного доступа (НСД).
4	Угрозы безопасности автоматизированных систем Рассматриваемые вопросы: - Классификация угроз информационной безопасности (ИБ) автоматизированных систем (АС). - Источники угроз НСД. - Каналы утечки информации в АС. - Классификация каналов утечки информации в АС.
5	Применение организационных методов для защиты информации Рассматриваемые вопросы: - Организационные методы защиты информации. - Организационные формы информационной безопасности на предприятии. - Политика безопасности компании. - Положительные и отрицательные стимулы.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Обучение персонала.
6	Применение технических средств защиты информации Рассматриваемые вопросы: - Защита от НСД на примере развертывания СЗИ Secret Net и АПМДЗ «Соболь». - Назначение и особенности СЗИ от НСД Secret Net. - Реализуемые функции защиты СЗИ от НСД Secret Net.
7	Информационная безопасность при межсетевом взаимодействии Рассматриваемые вопросы: - Средства защиты информации в локальных вычислительных сетях при межсетевом взаимодействии. - Требования к межсетевым экранам. - Правила межсетевого экранирования.
8	Вредоносное программное обеспечение Рассматриваемые вопросы: - Программно-математическое воздействие. - Понятие программно-математического воздействия и вредоносной программы. - Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации.
9	Защита от вредоносного программного обеспечения Рассматриваемые вопросы: - Организация антивирусной защиты. - Уровни защиты от компьютерных вирусов. - Политика безопасности компьютерной системы. - Характеристика антивирусных программ.
10	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа Рассматриваемые вопросы: - Защита целостности информации при хранении. - Защита целостности информации при обработке. - Защита целостности информации при транспортировке. - Защита от угрозы нарушения целостности информации на уровне содержания. - Построение систем защиты от угрозы отказа доступа к информации. - Защита семантического анализа и актуальности информации.
11	Политика и модели безопасности Рассматриваемые вопросы: - Субъектно-объектные модели разграничения доступа. - Аксиомы политики безопасности. - Политика и модели дискреционного доступа. - Парольные системы разграничения доступа. - Политика и модели мандатного доступа. - Политика и модели тематического разграничения доступа. - Ролевая модель безопасности.
12	Безопасность сетевых конфигураций Рассматриваемые вопросы: - Рекомендации X.800. - Функции безопасности, характерные для распределенных систем. - Интерпретация «Оранжевой книги» для сетевых конфигураций. - Понятие сетевой надежной вычислительной базы.

№ п/п	Тематика лекционных занятий / краткое содержание
13	Криптографические методы защиты информации Рассматриваемые вопросы: - Классификация методов криптографического закрытия информации. - Распределение ключей. - Криптография, цифровые сертификаты, PKI. - Электронная подпись.
14	Классические криптографические алгоритмы шифрования Рассматриваемые вопросы: - Шифрование простой одноалфавитной подстановкой. - Многоалфавитная простая подстановка. - Многоалфавитная монофоническая подстановка подстановка. - Простая перестановка. - Перестановка, усложненная по таблице.
15	Классические криптографические алгоритмы кодирования Рассматриваемые вопросы: - Классификация методов кодирования. - Смысловое кодирование. - Кодирование по специальным таблицам. - Символьное кодирование. - Кодирование по кодовому алфавиту.
16	Современные криптографические алгоритмы Рассматриваемые вопросы: - Симметричные и асимметричные криптоалгоритмы. - Симметричные криптоалгоритмы DES, 3DES и AES. - Асимметричные криптоалгоритмы на примере RSA.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Защита документов MS Office В результате выполнения лабораторной работы студент изучит методы защиты документов MS Office, правила создания сложных паролей.
2	Работа с программой вскрытия паролей AZPR. В результате выполнения лабораторной работы студент изучит возможности защиты архива паролем, научиться использовать программу вскрытия паролей Advanced ZIP Password Recovery.
3	Исследование и настройка межсетевого экрана В результате выполнения лабораторной работы студент изучит: - механизмы работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера; - практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана Outpost.
4	Резервное копирование программ, системных параметров и файлов В результате выполнения лабораторной работы студент изучит возможности резервного копирования в ОС Windows.
5	Использование методов замены для шифрования данных В результате выполнения лабораторной работы студент изучит классические шифры замены,

№ п/п	Наименование лабораторных работ / краткое содержание
	научиться зашифровывать тексты с помощью шифров замены.
6	Использование методов перестановки для шифрования данных В результате выполнения лабораторной работы студент изучит классические шифры перестановки, научиться зашифровывать тексты с помощью шифров перестановки, познакомиться с основами криптоанализа.
7	Методы криптоанализа классических шифров В результате выполнения лабораторной работы студент изучит основные шифры перестановки и методы криптоанализа.
8	Шифрование с помощью аналитических преобразований 2В результате выполнения лабораторной работы студент изучит методы алгебры матриц при шифровании сообщений.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Выполнение курсового проекта.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

1. Настройка системы защиты информации от несанкционированного доступа «DALLAS LOCK»

2. Настройка системы защиты информации от несанкционированного доступа «SECRET NET»

3. Настройка средств защиты информации от несанкционированного доступа в ос сн «astra linux».

4. Настройка средства антивирусной защиты «kaspersky endpoint security для «WINDOWS».

5. Анализ рынка средств усиления парольной защиты

6. Реализация добавочных механизмов усиления парольной защиты

7. Разработка политики информационной безопасности для государственной организации

8. Разработка политики информационной безопасности для организации оборонно-промышленного комплекса

9. Архитектура корпоративной системы защиты информации машиностроительного предприятия

10. Анализ современных способов разграничения доступа

11. Анализ защищённости внутренней инфраструктуры сети государственной организации

12. Анализ защищённости внутренней инфраструктуры сети коммерческой организации

13. Применения инструментальных средств анализа защищённости внутренней инфраструктуры сети

14. Анализ рынка программно-аппаратных средств защиты информации от несанкционированного доступа

15. Технико-экономическая оценка комплексирования средств защиты информации на примере коммерческой организации

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

№ п/п	Библиографическое описание	Место доступа
1	Защита программ и данных: учебно-метод. пособие для специалистов напр. Компьютерная безопасность / В. М. Алексеев; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 24 с.	URL: http://library.miit.ru/bookscatalog/metod/DC-436.pdf. (дата обращения 23.03.2024) Текст : непосредственный
2	Разработка корпоративной сети на основе MPLS. Защита информации: учебно-метод. пособие по курс. работе для специалистов напр. Компьютерная безопасность / В. М. Алексеев; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 22 с.	URL: http://library.miit.ru/bookscatalog/metod/DC-437.pdf(дата обращения 23.03.2024) Текст : непосредственный.004 А-47
3	Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Криптографическая 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.	URL: http://library.miit.ru/bookscatalog/metod/03-42764.pdf (дата обращения 25.03.2024) Текст : непосредственный. 004 Г60
4	Обеспечение информационной безопасности, проектирования, создания, модернизации объектов информации на	URL: http://library.miit.ru/bookscatalog/metod/DC-741.pdf(дата обращения 23.03.2024) Текст

	базе компьютерных систем в защищенном исполнении: учебно-метод. пособие к курс. работе для студ. спец. Компьютерная безопасность / А. А. Привалов; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2018. - 48 с.	: непосредственный.004 П-75
5	Защищенные беспроводные и мобильные коммуникации: Учеб. пособие для студ., обуч. по магистерской программе Безопасность и защита инф-ции напр. Информатика и выч. тех.; МИИТ. Центр компетентности Защита и безопасность информации / В.П. Соловьев, Д.В. Иванов, Н.Н. Пуцко; Ред. В.П. Соловьев. - М.: МИИТ, 2007. - 121 с.	URL: http://library.miit.ru/miitpublishing/04-35015.pdf(дата обращения 23.03.2024) Текст : непосредственный. 681.3 С-25

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/

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

- Microsoft Windows
- Microsoft Office

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

Для проведения аудиторных занятий и самостоятельной работы требуются:

• Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET

• Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской

• Компьютерный класс с кондиционером. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET

Для проведения практических занятий:

• компьютерный класс; кондиционер; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0

• 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.

9. Форма промежуточной аттестации:

Курсовой проект в 3 семестре.

Экзамен 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
«Вычислительные системы, сети и
информационная безопасность» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова