

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ))



Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в сетях

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

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: 4196

Подписал: заведующий кафедрой Желенков Борис
Владимирович

Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Защита информации в сетях» являются формирование компетенций по основным разделам теоретических и практических основ по организации защиты информации в сетях, дать необходимые знания по уязвимостям в компьютерных сетях, формированию модели угроз и модели нарушителя, навыки по практическому использованию средств анализа трафика и мониторинга инцидентов защиты в сетях, включая использование возможностей ограничения доступа к защищаемым ресурсам.

Слушатель получает систематизированные теоретические и практические знания в области обеспечения защиты информации в сетях, должен научиться определять возможные уязвимости, использовать современные обеспечения безопасности, в том числе, предоставляемые сетевым оборудованием для уменьшения уязвимости компьютерных сетей.

Основными задачами дисциплины являются:

- изучение принципов структурной и архитектурной организации современных средств обеспечения защиты информации в сетях;
формирование модели угроз и модели нарушителя;
- рассмотрение и анализ перспектив развития средств защиты информации в сетях;
- изучение средств мониторинга сетевых событий с точки зрения обеспечения безопасности;
- изучение направлений атак и уязвимостей в компьютерных сетях;
- конфигурирование средств для оповещения и выявления инцидентов защиты;
- анализ трафика с целью выявления угроз защиты информации в сетях;
- обработка инцидентов защиты компьютерных сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

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:

- методы проведения исследований при построении модели угроз и модели нарушителя, а так же средства защиты информации в сети;
- методы оценки эффективности функционирования, оценки затрат и рисков при формировании политики защиты.

Уметь:

- формировать отчеты по проведению исследований при построении модели угроз и модели нарушителя;
- анализировать направления развития информационных (телекоммуникационных) технологий с точки зрения возникновения угроз информационной безопасности

Владеть:

- навыками выбора инструментальных средств разработки и обеспечения защиты информации в сетях;
- навыками выбора средств создания и ведения репозитория, учета инцидентов информационной безопасности, сборки и непрерывной интеграции, базы знаний;
- навыками подготовки научных докладов и статей на основании полученных отчетов по проведению исследований при построении модели угроз и модели нарушителя;
- навыками формирования политики безопасности объектов защиты.

3. Объем дисциплины (модуля).**3.1. Общая трудоемкость дисциплины (модуля).**

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 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 №1
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 152 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	Компьютерная сеть. Классификация сетей. - Рассматриваются основные направления действия системы защиты информации в сети и принципы ее организации.
2	Принципы построения архитектуры сети, варианты схем и резервирование. - Рассматриваются вопросы защиты информации в сети и принципы ее организации с точки зрения топологии.
3	Определение надежности сети. Понятие SLA. - Рассматриваются вопросы защиты в сетях предприятия среднего и крупного бизнеса .
4	Коммутация каналов, сообщений, пакетов . - Рассматриваются вопросы защиты информации в сетях предприятия, определяются направления действия политики защиты. - Рассматривается комплексный структурированный подход защиты информации крупного предприятия.
5	Кросс-коммутационная матрица IP сетевого и транспортного оборудования. - Рассматриваются компоненты системы безопасности сети.
6	Атаки на коммуникационные протоколы сети . - Рассматриваются компоненты системы и сегментирование сети критерия защиты информации и их совместное использование.
7	Способы атаки на протоколы HTTP и HTTPS. - Рассматривается вопрос выявления границ потенциального влияния.
8	Определение требований безопасности коммуникационных протоколов сети крупной компании. - Рассматриваются способы обеспечения требований защиты.

№ п/п	Тематика лекционных занятий / краткое содержание
9	Определение необходимости полосы канала при построение связности объектов ЦОД-ЦОД. - Рассматривается вопрос принципы подхода к определению полосы пропускания.
10	Способы прогнозирования увеличения полосы пропускания при жизненном цикле решения (построение, эксплуатация, масштабирование). - Рассматриваются вопросы правильных подходов к архитектуре технических решений.
11	Обеспечение безопасности транспортного уровня . Рассматриваются вопросы: - Выявление уязвимостей, системы обнаружения вторжений, сканеры безопасности, DOS-атаки. -Способы обеспечения работы сети при DDOS. - Определение аппаратного шифратора и механизмов принципов его работы.
12	Обеспечение логирования и сборов логов любого сетевого оборудования. - Рассматривается вопрос хранения логов в горизонте один год .
13	Использование защищенных систем логирования PAM. - Рассматривается вопрос компонентов системы защиты.
14	Оценка возможности использования Linux-систем взамен Windows Server. -Рассматривается вопрос перехода на Linux-подобные системы.
15	Способы обеспечения надежной работы сети при атаках типа DDOS. - Рассматривается способы работы сети при длительных атаках.
16	Маршрутизация в виртуальных частных сетях с архитектурой клиент-сервер. Рассматриваются вопросы: - Принцип построения туннельного интерфейса. - Remote-accessVPN. - CiscoAnyConnect. - Использование Cisco ASA в качестве VPN-сервера. - Сравнение ФПСУ-IP клиента и CiscoAnyConnect . - Определение требований к серверному оборудованию ФПСУ.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Анализ сетевого трафика В результате выполнения работы студент получит практические навыки по анализу, передаваемой по сети, информации.
2	Определение критериев анализа и параметров подлежащих анализу и контролю В результате выполнения работы студент получит практические навыки по определению критериев подлежащих анализу и контролю.
3	Способы определения SLA для систем В результате выполнения работы студент получит практические навыки по определению критериев данного параметра и его расчетов.
4	Способы построения канально-пакетной сети В результате выполнения работы студент получит практические навыки по моделированию сети по определенным критериям определению.
5	Моделирование использования сети с матрицей кросс-коммутации В результате выполнения работы студент получит практические навыки по моделированию сети.

№ п/п	Наименование лабораторных работ / краткое содержание
6	Эмуляция реализации атаки на коммуникационных протоколах сети В результате выполнения работы студент получит практические навыки по приему и моделированию угроз.
7	Эмуляция реализации атаки на протоколы HTTP и HTTPS В результате выполнения работы студент получит практические навыки по приему и моделированию угроз, и способ защиты сети.
8	Исследование и анализ методологии по защите протоколов крупной компании В результате выполнения работы студент получит практические навыки по защите протоколов крупной компании.
9	Эмуляция полосы пропускания канала В результате выполнения работы студент получит практические навыки по пониманию принципов организованной полосы пропускания и QOS.
10	Анализ требований к увеличению полосы пропускания В результате выполнения работы студент получит практические навыки по прогнозированию полосы пропускания.
11	DDOS и способы защиты В результате выполнения работы студент получит практические навыки по приемам борьбы и понимание механизмов DDOS.
12	Понятие уязвимости софта и способы тестирования В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью софта и освоит навык понимания принципа обеспечения защиты сети.
13	Использование ПАМ и способы аутентификации в нем В результате выполнения работы студент получит практические навыки по работе с ПО ПАМ .
14	Установка ПО Linux(Server) Red Hat или Ubuntu(Server) В результате выполнения работы студент получит практические навыки по установке и администрированию ПО Linux(Server).
15	Моделирование угроз и определение рисков в случае DDOS В результате выполнения работы студент получит практические навыки по приемам моделирования угроз для обеспечения защиты сети.
16	ФПСУ-IP (Remote-accessVPN) В результате выполнения работы студент получит практические навыки по настройке Remote-accessVPN для российского ФПСУ-IP (Remote-accessVPN).

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых работ

1. Безопасность для сети LAN, комплексный подход защиты сети.

2. Криптошлюзы. Виды, цели и условия применения.
3. Сравнение разных криптошлюзов и их функционала. Принцип работы.
4. Механизм построения шифрования для различных криптошлюзов. Пример типовой конфигурации.
5. Архитектура предприятия для использования защиты периметра с шифрованием.
6. Различные виды шифрования используемые для защиты сети.
7. Определение модели угроз внешнего периметра и способы защиты сети.
8. Определение внутренних угроз и обеспечение безопасности периметра и способы защиты сети.
9. Установка OS Linux взамен Windows Server на базе дистрибутивов Red Hat и Ubuntu.
10. Преимущество и недостатки кросс-коммутационного оборудования над сетевым IP-оборудованием и DWDM транспортным оборудованием.
11. Построение сети с использованием коммутации каналов.
12. Полоса пропускания как критерий надежной эксплуатации.

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

№ п/п	Библиографическое описание	Место доступа
1	Краковский, Ю. М. Методы и средства защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 272 с. — ISBN 978-5-507-52958-2. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/463013 (дата обращения: 06.11.2025)
2	В. В. Сафронов, С. Л. Кенин, М. П. Иванкин, В. В. Ключников. Защита информации в вычислительных сетях : учебно-методическое пособие /— Воронеж : ВГУ, 2021. — 42 с. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/455111 (дата обращения: 06.11.2025)
3	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва :	https://e.lanbook.com/book/110336 (дата обращения: 06.11.2025)

	ТУСУР, 2015. — 284 с. — Текст : электронный // Лань : электронно-библиотечная система.	
--	--	--

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

- Научно-техническая библиотека РУТ(МИИТ) <http://library.miit.ru/>
- Официальный сайт по поддержке решений ФПСУ <https://www.fpsu.ru/>
- Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности - <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-2003-god>
- ГОСТ Р ИСО/МЭК 15408-1-2012 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ - <https://docs.cntd.ru/document/1200101777>
- 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).

- ОС Windows
- Microsoft Office
- Интернет-браузер (Yandex и др.)

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

- Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):
 - компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, доска.
 - Аудитория подключена к сети «Интернет».
 - Программно-аппаратный комплекс СОТСБИ.

9. Форма промежуточной аттестации:

Курсовая работа в 1 семестре.

Экзамен в 1 семестре.

10. Оценочные материалы.

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

Авторы:

Д.Н. Данилюк

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова