МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

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: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- ознакомление с основными типами угроз и атак;
- изучение механизмов защиты административного интерфейса и разграничения прав доступа;
- изучение технологии и принципов AAA;
- изучение способов защиты информации в сетях;
- изучение принципов построения виртуальных частных сетей.

Основные задачи дисциплины (модуля) следующие:

- поиска и проверки новых технических и программных решений по совершенствованию систем и средств информационной безопасности;
- разработки планов, программ и методик проведения исследований уровня защищенности объектов информатизации, анализ их результатов.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

ОПК-3 - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

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

Знать:

- Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основы системного администрирования.
- Устройство и функционирование современных информационных систем и автоматизированных систем.
- Современные стандарты информационного взаимодействия систем и протоколы безопасности.
- Программные средства и платформы инфраструктуры информационных технологий организаций.

- Методики тестирования систем защиты информации автоматизированных систем.

- Структуру и содержание эксплуатационной документации на системы защиты информации.

- Нормативно-правовую базу и методологию разработки планов мероприятий по защите информации.

- Критерии и методики анализа эффективности систем защиты информации.

- Принципы организации и этапы создания системы защиты информации процессов проектирования, создания и модернизации.

Уметь:

- Разрабатывать проектные решения по защите информации в автоматизированных системах.

- Проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации.

- Разрабатывать архитектуру системы защиты информации автоматизированной системы.

- Проводить тестирование систем защиты информации автоматизированных систем.

- Разрабатывать эксплуатационную документацию на системы защиты информации.

- Разрабатывать план мероприятий по защите информации в объектах информатизации.

- Проводить анализ эффективности систем защиты информации в объектах информатизации.

- Участвовать в создании системы защиты информации процессов проектирования, создания и модернизации.

- Разрабатывать проекты нормативных правовых актов и методических документов в области защиты информации.

Владеть:

- Навыками разработки проектной документации и технических заданий на создание систем защиты информации.

- Методами сравнительного анализа и критериями выбора средств защиты информации.

- Навыками проектирования архитектуры защиты автоматизированных систем.

- Навыками проведения тестирования и оценки эффективности систем защиты информации.

- Навыками разработки эксплуатационной и организационно-распорядительной документации.

- Навыками планирования мероприятий по защите информации на объектах информатизации.

- Навыками анализа входных данных и определения базовых элементов конфигурации информационных систем.

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 №10
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 116 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 и нормативное регулирование защиты информации Рассматриваемые вопросы: - цель обеспечения информационной безопасности; - виды контроля безопасности. - конфиденциальность, целостность и доступность; - принципы внедрения систем информационной безопасности; - классификация угроз информационной безопасности; - виды средств защиты информации; - примеры средств защиты информации. - виды защиты информации; - способы защиты информации; - техника защиты информации; - способы оценки соответствия требованиям защиты информации; - эффективность защиты информации.
2	Политика информационной безопасности и кадровая работа Рассматриваемые вопросы: - цели политики защиты; - задачи политики защиты; - основные требования к политике защиты; - содержание политики защиты. - организация работы по контролю состояния защиты конфиденциальной информации; - организация работы с персоналом предприятия, допущенного к конфиденциальной информации.
3	Угрозы информационной безопасности и вредоносное ПО Рассматриваемые вопросы: - виды угроз информационной безопасности; - источники угроз информационной безопасности. - классификация компьютерных вирусов; - методы защиты от компьютерных вирусов; - вредоносное воздействие компьютерных вирусов.
4	Противодействие опасным воздействиям и современные вызовы ИБ Рассматриваемые вопросы: - реализация сценариев угроз информационной безопасности; - несанкционированный доступ; - непосредственные и непрямые угрозы информационной безопасности; - методы организации защиты информации. - основные инструменты реализации угроз; - ключевые цели информационной инфраструктуры для злоумышленников; - угрозы информационной безопасности и меры защиты.
5	Сетевая безопасность и межсетевое экранирование Рассматриваемые вопросы: - направления защиты сети; - уязвимые места, через которые может быть выполнен несанкционированный доступ к сетевому оборудованию; - требования для защиты административного интерфейса сетевого оборудования; - настройка контекстных списков доступа. - принципы сетевой защиты на базе межсетевых экранов; - формирование политики межсетевого взаимодействия; - политика доступа к сетевым сервисам; - политика работы межсетевого экрана;

№ п/п	Тематика лекционных занятий / краткое содержание
	- выполняемые функции и составные элементы анализа; - основные схемы подключения межсетевых экранов.
6	Построение и защита виртуальных частных сетей (VPN) Рассматриваемые вопросы: - необходимость виртуальной частной сети; - реализация виртуальных частных сетей; - протоколы виртуальных частных сетей.
7	Идентификация, аутентификация и управление правами доступа Рассматриваемые вопросы: - необходимость; - примеры протоколов; - основные решения; - настройка удаленного доступа для администрирования сетевого оборудования. - основные понятия и определения; - сфера применения; - основные принципы управления правами доступа; - модель разграничения доступа; - правила именования групп доступа пользователей; - процессы управления доступом к файловым информационным ресурсам.
8	Интеграция систем информационной и физической безопасности Рассматриваемые вопросы: - достоинства интеграции систем защиты информации от несанкционированного доступа с контролем доступа и видеонаблюдением; - объединение систем на нескольких уровнях; - схема информационных потоков; - пример сценария.
9	Криптографическая защита и электронная цифровая подпись Рассматриваемые вопросы: - средства криптографической защиты информации; - принципы шифрования; - применение криптографии и средств криптографической защиты информации. - принцип использования электронной цифровой подписи; - алгоритмы электронной цифровой подписи; - особенности применения электронной цифровой подписи.
10	Защита ключевой информации и аппаратные токены Рассматриваемые вопросы: - безопасность средств хранения ключевой информации; - виды носителей ключевой информации; - контроль среды доступа к носителю ключевой информации; - «идеальный токен»: принципы функционирования.
11	Доверенная вычислительная среда Рассматриваемые вопросы: - доверенная загрузка; - условия обеспечения доверенной загрузки операционной системы; - доверенная вычислительная система; - условия доверенности компьютера и доверенного сетевого соединения; - доверенный сеанс связи; - особенности построения защищённых распределенных информационных систем.
12	Централизованное управление средствами защиты информации Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- назначение и основные элементы; - функции системы; - функции системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа; - состав ролей системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа.
13	Защита информационных систем персональных данных Рассматриваемые вопросы: - требования регуляторов по защите персональных данных и требования к информационной системе персональных данных для различных уровней защиты; - сетевая инфраструктура информационной системы персональных данных и меры ее защиты; - оптимизация сетевой инфраструктуры; - средства защиты информации от несанкционированного доступа.
14	Безопасность веб-приложений Рассматриваемые вопросы: - угрозы информационной безопасности при использовании Web-сервера; - методы и средства защиты информационной безопасности для Web-приложений; - угрозы и уязвимости информационной безопасности, возникающие в Web-среде; - меры по ликвидации угроз и уязвимостей информационной безопасности, возникающих в Web-среде.
15	Защита критической информационной инфраструктуре Рассматриваемые вопросы: - принадлежность объекта информатизации к критической информационной инфраструктуре; - возможности средств защиты сетевого взаимодействия между объектами в критической информационной инфраструктуре; - аппаратная защита данных в объектах критической информационной инфраструктуры; - требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
16	Информационная безопасность автоматизированных систем управления технологическими процессами Рассматриваемые вопросы: - факторы, влияющие на информационную безопасность современных АСУ ТП; - особенности обследования и аудита; - цели и концепции информационной безопасности в АСУ ТП; - основные этапы реализации 187-ФЗ от 26.07.2017 г.; - средства обеспечения безопасности объектов критической информационной инфраструктуры; - угрозы информационной безопасности и механизмы их предупреждения.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Анализ угроз безопасности в локальных и корпоративных сетях В результате работы на практическом занятии студент отрабатывает навык выявления и классификации угроз, анализа уязвимостей сетевой инфраструктуры.
2	Разработка политики информационной безопасности организации В результате работы студент получает навык разработки основных разделов политики ИБ, включая цели, задачи и требования к защите информации.

№ п/п	Тематика практических занятий/краткое содержание
3	Организация работы с персоналом, допущенным к конфиденциальной информации В результате работы студент изучает методы организации контроля и работы с персоналом в рамках политики защиты информации.
4	Управление правами доступа к корпоративным информационным ресурсам В результате работы студент получает навык настройки прав доступа к файлам и папкам, реализации модели разграничения доступа.
5	Настройка средств защиты административного интерфейса сетевого оборудования В результате работы студент осваивает настройку удаленного доступа для администрирования сетевого оборудования и контекстных списков доступа.
6	Реализация политики межсетевого экранирования В результате работы студент изучает принципы сетевой защиты на базе межсетевых экранов, формирование политик доступа к сетевым сервисам.
7	Построение виртуальных частных сетей (VPN) В результате работы студент получает навык настройки VPN-соединений с использованием различных протоколов (IPSec, OpenVPN).
8	Обеспечение безопасности Web-приложений В результате работы студент анализирует угрозы для Web-серверов и осваивает методы и средства защиты Web-приложений.
9	Применение средств криптографической защиты информации и электронной подписи В результате работы студент изучает принципы шифрования и практического применения ЭЦП для обеспечения целостности и аутентификации.
10	Тестирование систем защиты информации В результате работы студент осваивает методики и инструментальные средства тестирования систем защиты информации на проникновение и уязвимости.
11	Анализ эффективности системы защиты информации В результате работы студент проводит оценку эффективности выбранных мер и средств защиты, анализирует результаты мониторинга.
12	Разработка эксплуатационной и организационно-распорядительной документации В результате работы студент получает навык разработки инструкций, регламентов и планов мероприятий по защите информации для объекта информатизации.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом и изучение литературы по дисциплине
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Основы безопасности прикладных информационных технологий и систем Криулин А.А., Нефедов В.С., Смирнов С.И. Учебное пособие М.: МИРЭА - Российский технологиччский университет, - 136 с. , 2020	https://reader.lanbook.com/book/167606#2
2	Модели безопасности компьютерных систем Богульская Н.А. Учебное пособие Красноярск: Сиб. федер. ун-т, - 206 с., - ISBN 978-5-7638-4008-7 , 2019	https://reader.lanbook.com/book/157578#3

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

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/).

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 Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Компьютер должен быть обеспечен лицензионными программными продуктами: Foxit Reader/Acrobat Reader Microsoft Office (Power Point) Установлен мультимедийный курс лекций.

Компьютер должен быть обеспечен лицензионными программными продуктами: Foxit Reader/Acrobat Reader Microsoft Office (Word). На рабочие места должны быть установлены программные разработки кафедры «Вычислительные системы и сети»: Обучающая система «netlab»

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.

Для проведения практических занятий:

компьютеры с предустановленным Microsoft Windows не ниже Windows XP и процессором не ниже Pentium 4.

- маршрутизаторы Cisco;
- коммутаторы Cisco;
- соединительные кабели различных типов

9. Форма промежуточной аттестации:

Экзамен в 10 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, доцент, к.н. кафедры «Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах» Института железнодорожного транспорта — С.Е. Иконников

Согласовано:

Заведующий кафедрой ИУиИБ — Л.А. Баранов

Председатель учебно-методической комиссии — Н.А. Андриянова