**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 РУТ (МИИТ)
Тимониным В.С.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Защита информации в системах передачи информации

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 РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2026

1. Общие сведения о дисциплине (модуле).

Цель: Формирование у обучающихся системных теоретических знаний, практических умений и профессиональных компетенций в области обеспечения информационной безопасности в системах передачи данных, а также подготовка специалистов, способных анализировать угрозы, проектировать, внедрять и эксплуатировать комплексные средства защиты информации в телекоммуникационных системах и сетях связи в соответствии с требованиями специальности 10.05.01 «Компьютерная безопасность».

Задача: Освоить комплекс теоретических знаний и практических компетенций для анализа угроз, проектирования, внедрения и аудита средств защиты информации в телекоммуникационных системах с соблюдением требований регуляторов (ФСТЭК, ФСБ России), включая оценку рисков, мониторинг, реагирование на инциденты и разработку соответствующей нормативно-технической документации.

2. Планируемые результаты обучения по дисциплине (модулю).

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

**ОПК-5** - Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;

**ПК-4** - Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах.

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

**Знать:**

- Классификацию и характеристики инструментальных средств разработки (компиляторы, отладчики, IDE, системы контроля версий);
- Критерии выбора языков программирования, фреймворков и архитектурных решений в зависимости от постановки профессиональной задачи;
- Нормативно-правовую базу и стандарты в области информационной безопасности (ФЗ-152, ГОСТ Р 57580, ISO/IEC 27001, NIST);

- Принципы построения и компоненты политик информационной безопасности на организационном и техническом уровнях;

**Уметь:**

- Применять методы структурного и объектно-ориентированного программирования для решения прикладных задач;
- Проводить сравнительный анализ инструментов программирования и обосновывать выбор технологического стека;
- Разрабатывать и внедрять частные политики ИБ (парольная политика, политика доступа, реагирования на инциденты) в соответствии с требованиями организации;
- Настраивать и администрировать средства защиты: межсетевые экраны, SIEM-системы, DLP, антивирусные комплексы;

**Владеть:**

- Навыками проектирования архитектуры программных модулей и выбора рациональных способов организации данных;
- Инструментами автоматизации сборки, тестирования и развёртывания программных решений;
- Методиками анализа защищённости и проведения тестов на проникновение (в рамках регламента);
- Навыками моделирования угроз и оценки рисков с применением стандартных фреймворков (STRIDE, OCTAVE, FAIR);

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): | 80 | 80 |
| В том числе: | | |
| Занятия лекционного типа | 48 | 48 |
| 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 100 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 | Понятие информационной безопасности в СПИ<br>Рассматриваемые вопросы:<br>- Введение в базовые принципы ИБ: конфиденциальность, целостность, доступность.<br>- Обзор уровней обеспечения безопасности — от законодательного до программно-технического.<br>- Знакомство с международными стандартами (ISO 27001, «Оранжевая книга», «Общие критерии»). |
| 2 | Нормативно-правовая база РФ<br>Рассматриваемые вопросы:<br>- Обзор ключевых федеральных законов в области защиты информации.<br>- Требования ФСТЭК России к аттестации объектов информатизации.<br>- Особенности регулирования для гостайны, персональных данных и критической информационной инфраструктуры. |
| 3 | Моделирование угроз и анализ рисков<br>Рассматриваемые вопросы:<br>- Методологии выявления и оценки угроз (FAIR, OCTAVE, ГОСТ Р 57580).<br>- Построение модели нарушителя и карты угроз для интернет/интранет-сетей.<br>- Практические подходы к количественной и качественной оценке рисков. |
| 4 | Классификация информационных систем<br>Рассматриваемые вопросы:<br>- Критерии отнесения ИС к уровням защищенности в зависимости от типа обрабатываемых данных и актуальных угроз.<br>- Требования к защите для различных классов систем согласно российским нормативным документам. |
| 5 | Криптографические методы защиты<br>Рассматриваемые вопросы:<br>- Принципы симметричного и асимметричного шифрования.<br>- Механизмы электронной подписи и хеширования. |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | - Протоколы безопасного обмена ключами (Diffie-Hellman, IKE).<br>- Обзор российских криптоалгоритмов (ГОСТ). |
| 6 | Идентификация и аутентификация<br>Рассматриваемые вопросы:<br>- Методы подтверждения личности: пароли, биометрия, аппаратные токены, смарт-карты.<br>- Многофакторная аутентификация.<br>- Сетевые протоколы аутентификации: RADIUS, TACACS+, Kerberos. |
| 7 | Управление доступом и аудит<br>Рассматриваемые вопросы:<br>- Модели разграничения прав: дискреционная (DAC), мандатная (MAC), ролевая (RBAC).<br>- Принципы организации аудита.<br>- Сбор и анализ логов: syslog, SIEM-системы, корреляция событий безопасности. |
| 8 | Защита носителей и контроль ПО<br>Рассматриваемые вопросы:<br>- Политики работы со съемными носителями.<br>- Механизмы Application Control («белые списки»).<br>- Изоляция исполняемой среды: sandboxing, ограничение прав приложений, предотвращение выполнения неавторизованного кода. |
| 9 | Безопасность маршрутизации и коммутации<br>Рассматриваемые вопросы:<br>- Уязвимости протоколов динамической маршрутизации (BGP, OSPF, IS-IS).<br>- Методы защиты: аутентификация соседних устройств, фильтрация анонсов маршрутов, защита плоскости управления (CoPP). |
| 10 | Защита ЛВС на канальном уровне<br>Рассматриваемые вопросы:<br>- Атаки типа ARP-spoofing, MAC-flooding, манипуляции STP.<br>- Средства противодействия: Port Security, DHCP Snooping, Dynamic ARP Inspection, механизмы защиты от петель (BPDU Guard, Loop Guard). |
| 11 | Межсетевые экраны и фильтрация трафика<br>Рассматриваемые вопросы:<br>- Архитектуры МЭ: от пакетных фильтров до NGFW.<br>- Настройка ACL, stateful-инспекция, анализ приложений.<br>- Организация периметра безопасности и демилитаризованной зоны (DMZ). |
| 12 | Виртуальные частные сети (VPN)<br>Рассматриваемые вопросы:<br>- Сравнение протоколов: IPsec, GRE, OpenVPN, WireGuard.<br>- Принципы туннелирования и шифрования.<br>- Сценарии развертывания: сайт-сайт и удаленный доступ.<br>- Управление ключами и сессиями. |
| 13 | Защита беспроводных сетей<br>Рассматриваемые вопросы:<br>- Специфические угрозы Wi-Fi и Bluetooth.<br>- Эволюция протоколов безопасности: WPA2 > WPA3.<br>- Аутентификация через 802.1X.<br>- Сегментация трафика, обнаружение и блокировка несанкционированных точек доступа (Rogue AP). |
| 14 | IDS/IPS и антивирусная защита<br>Рассматриваемые вопросы:<br>- Принципы обнаружения атак: сигнатурный и поведенческий анализ. |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | - Сетевые и хостовые архитектуры IDS/IPS.<br>- Интеграция систем предотвращения вторжений с межсетевыми экранами и антивирусами. |
| 15 | Безопасность технологий MPLS<br>Рассматриваемые вопросы:<br>- Архитектура MPLS и векторы атак.<br>- Методы изоляции трафика через VRF.<br>- Защита от подмены меток и атак на плоскость управления.<br>- Использование криптографических механизмов в MPLS-сетях. |
| 16 | Криптозащита каналов и технических средств<br>Рассматриваемые вопросы:<br>- Аппаратное шифрование: HSM-модули, криптошлюзы.<br>- Защита от утечек по ПЭМИН: экранирование, заземление, фильтрация.<br>- Требования к защите оконечных устройств и линий связи. |
| 17 | Обеспечение доступности<br>Рассматриваемые вопросы:<br>- Методы противодействия DDoS-атакам: фильтрация, rate limiting, облачная защита.<br>- Резервирование оборудования и каналов (HSRP, VRRP).<br>- Кластеризация, балансировка нагрузки, стратегии резервного копирования. |
| 18 | Обеспечение целостности<br>Рассматриваемые вопросы:<br>- Контроль целостности через хеширование и контрольные суммы.<br>- Механизмы доверенной загрузки (Secure Boot, TPM).<br>- Защита критичных файлов и конфигураций от несанкционированных изменений. |
| 19 | ИБ на железнодорожном транспорте<br>Рассматриваемые вопросы:<br>- Особенности защиты АСУ ТП и диспетчерских систем (SCADA).<br>- Требования к системам высокоскоростного и беспилотного транспорта.<br>- Отраслевые стандарты и регуляторные требования. |
| 20 | Безопасность облачных сервисов<br>Рассматриваемые вопросы:<br>- Модели развертывания (IaaS, PaaS, SaaS) и разделение ответственности.<br>- Защита данных в публичных и приватных облаках.<br>- Использование CASB для контроля доступа и мониторинга активности. |
| 21 | Защита виртуализации и контейнеров<br>Рассматриваемые вопросы:<br>- Угрозы гипервизорам и средства их изоляции.<br>- Безопасность Docker-контейнеров и оркестрации Kubernetes: политики безопасности, сканирование образов, сетевые политики в микросервисах. |
| 22 | Контроль и анализ защищенности<br>Рассматриваемые вопросы:<br>- Методы оценки эффективности СЗИ: внутренний/внешний аудит, пентесты, сканирование уязвимостей.<br>- Анализ конфигураций на соответствие стандартам (CIS Benchmarks). |
| 23 | Планирование мероприятий по защите<br>Рассматриваемые вопросы:<br>- Разработка Плана защиты информации на этапах ЖЦ объекта информатизации.<br>- Оценка стоимости владения СЗИ, бюджетирование, выбор и обоснование защитных мер. |
| 24 | Реагирование на инциденты ИБ<br>Рассматриваемые вопросы:<br>- Организация группы CSIRT/SOC. Жизненный цикл инцидента: обнаружение > локализация > |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | устранение > восстановление.<br>- Основы цифровой криминалистики (форензики) и сбора доказательств. |

## 4.2. Занятия семинарского типа.

### Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | Настройка операционной системы Cisco IOS<br>В результате выполнения работы студент умеет выполнять базовую настройку Cisco IOS, настраивать пароли привилегированных режимов, конфигурировать локальные учётные записи и обеспечивать безопасное удалённое управление через SSH с отключением небезопасных протоколов (Telnet). |
| 2 | Защита инфраструктуры маршрутизации<br>В результате выполнения работы студент умеет настраивать аутентификацию протоколов динамической маршрутизации OSPF и EIGRP с использованием MD5/SHA, применять пассивные интерфейсы и фильтрацию маршрутов для предотвращения несанкционированного внедрения ложных маршрутов. |
| 3 | Защита инфраструктуры коммутации<br>В результате выполнения работы студент умеет настраивать Port Security для ограничения доступа по MAC-адресам, активировать BPDU Guard и Root Guard для защиты топологии STP от несанкционированных изменений и атак типа rogue switch. |
| 4 | Защита ЛВС от петель на канальном уровне<br>В результате выполнения работы студент умеет настраивать и верифицировать протоколы STP/RSTP, применять Loop Guard и BPDU Filter для предотвращения петель коммутации и обеспечения стабильности топологии второго уровня. |
| 5 | Защита ЛВС от атак канального уровня<br>В результате выполнения работы студент умеет настраивать DHCP Snooping для фильтрации недоверенных DHCP-серверов, активировать Dynamic ARP Inspection (DAI) для предотвращения ARP-spoofing атак и связывать эти механизмы в единую систему защиты коммутатора. |
| 6 | Построение маршрутизируемой ЛВС<br>В результате выполнения работы студент умеет создавать и назначать VLAN, настраивать магистральные порты (802.1Q), реализовывать межсегментную маршрутизацию методами «роутер-на-палке» и Layer 3 switching с применением ACL для контроля межсегментного трафика. |
| 7 | Настройка списков доступа (ACL)<br>В результате выполнения работы студент умеет разрабатывать и применять стандартные, расширенные и именованные списки доступа для фильтрации трафика по адресам, портам и протоколам, размещать ACL в правильной топологической позиции и верифицировать их работу через логи и счётчики. |
| 8 | Организация VPN на сетевом оборудовании<br>В результате выполнения работы студент умеет настраивать туннели GRE для инкапсуляции трафика, конфигурировать IPsec VPN в режимах tunnel/transport с использованием IKEv1/IKEv2, управлять криптографическими параметрами (ESP, AH, преобразователи) и проверять работоспособность защищённых каналов. |
| 9 | Защита периметра сети<br>В результате выполнения работы студент умеет проектировать демилитаризованную зону (DMZ), настраивать правила межсетевого экранирования на основе зональной модели (zone-based firewall), реализовывать NAT/PAT и контролировать трафик между доверенными, недоверенными и публичными сегментами сети. |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 10 | Криптографическая защита каналов передачи данных<br>В результате выполнения работы студент умеет настраивать шифрование трафика на интерфейсах маршрутизаторов с использованием IPsec, управлять ключами шифрования, настраивать политики безопасности (crypto maps) и обеспечивать конфиденциальность данных в точках межсетевого взаимодействия. |
| 11 | Защита беспроводной ЛВС<br>В результате выполнения работы студент умеет настраивать WPA2-Enterprise с использованием RADIUS-аутентификации, внедрять 802.1X для контроля доступа устройств, применять фильтрацию по MAC-адресам и верифицировать защищённость беспроводной инфраструктуры от несанкционированного подключения. |
| 12 | Сбор предварительной информации о сети<br>В результате выполнения работы студент умеет проводить пассивную и активную разведку с использованием nmap, Wireshark и tcpdump, анализировать заголовки пакетов, выявлять открытые сервисы и потенциальные векторы атак на основе собранной информации о сетевой топологии. |
| 13 | Идентификация узлов и портов сетевых служб<br>В результате выполнения работы студент умеет выполнять сканирование портов и сервисов, извлекать баннеры приложений, определять версии ПО и операционных систем, классифицировать уязвимости на основе полученных данных и формировать отчёт о потенциальных точках входа для атакующего. |
| 14 | Настройка систем мониторинга и аудита событий безопасности<br>В результате выполнения работы студент умеет настраивать централизованный сбор логов через syslog, конфигурировать SNMPv3 с шифрованием, интегрировать сетевые устройства с системами мониторинга (Zabbix) и SIEM-платформами для оперативного обнаружения инцидентов безопасности. |
| 15 | Обеспечение безопасности диспетчерских систем (SCADA)<br>В результате выполнения работы студент умеет выполнять сегментацию промышленных сетей, настраивать белые списки приложений и устройств, изолировать критические контроллеры от корпоративного сегмента и применять специализированные правила фильтрации для протоколов промышленной автоматизации (Modbus, DNP3). |
| 16 | Разработка фрагмента политики безопасности для корпоративной сети транспортного предприятия<br>В результате выполнения работы студент умеет анализировать бизнес-требования и угрозы для транспортной инфраструктуры, формулировать правила контроля доступа, сегментации и мониторинга, оформлять нормативный документ в соответствии с лучшими практиками (ISO 27001, NIST) и обосновывать выбранные меры защиты с учётом специфики отрасли. |

## 4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | Изучение дополнительной литературы. |
| 2 | Подготовка к практическим занятиям. |
| 3 | Выполнение курсового проекта. |
| 4 | Подготовка к промежуточной аттестации. |
| 5 | Подготовка к текущему контролю. |

## 4.4. Примерный перечень тем курсовых проектов

1. Разработка модели угроз и нарушителя для корпоративной сети предприятия с выходом в интернет и использованием VPN для филиалов.

2. Проектирование системы защиты информации для сегмента сети, обрабатывающего конфиденциальную информацию

3. Анализ уязвимостей и выбор средств защиты для гибридной сети (проводной + беспроводной сегмент) с использованием WPA3 и NAC.

4. Разработка политики безопасности и системы защиты для интранет-портала организации

5. Проектирование системы защиты каналов передачи данных между центральным офисом и филиалами на основе технологий VPN

6. Обеспечение безопасности межсетевого взаимодействия при подключении удаленных филиалов и мобильных сотрудников

7. Разработка мер защиты от атак канального и сетевого уровня в корпоративной ЛВС

8.Проектирование системы мониторинга, регистрации событий и анализа защищенности на базе SIEM-решения для транспортного предприятия.

9. Защита инфраструктуры маршрутизации и MPLS-сети провайдера связи

10. Обеспечение информационной безопасности диспетчерской системы управления движением поездов

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

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Защита информации Груздева Л. М. Учебное пособие М.: Российский университет транспорта, - 144 с. - ISBN 978-5-7876-0326-2 , 2019 | https://reader.lanbook.com/book/188703 |
| 2 | Техническая защита информации Раков А. С., Маслов О. Н., Губарева О. Ю., Почепцов А. О., Гуреев В. О. Учебное пособие Поволжский государственный университет телекоммуникаций и информатики, - 96 с. , 2020 | https://reader.lanbook.com/book/255575 |

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/).

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

Work 9,

Интегрированная среда разработки программного обеспечения для эиуляции сетевого оборудования OmniGraffle;

Среда разработки программного обеспечения HTML5 и PHP.

Построения программных и аппаратных средств защиты информации в телекоммуникационных сетях (iOS15 Cisco и выше) с поддержкой MPLS;

Программные продукты Mac OS server, XSan.

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:

Курсовой проект в 10 семестре.

Экзамен в 10 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры "Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах" Института железнодорожного транспорта В.М. Алексеев

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин