

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Информационные системы и технологии»**

СОГЛАСОВАНО

Руководитель образовательной программы

_____/М.Х. Мальсагов
от «03» марта 2025г.

УТВЕРЖДАЮ

И.о. декана физико-математического
факультета

_____/Б.С.Кульбужев
от «14» марта 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

**Б1.В.ДВ.03.01 Разработка предметно-ориентированных программных средств. Защита
компьютерных сетей**

Направление подготовки

09.03.02 Информационные системы и технологии

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, очно-заочная

Магас, 2025г.

Цели и задачи освоения дисциплины «Разработка предметно-ориентированных программных средств, защита компьютерных сетей

»

Целью освоения дисциплины является формирование у студентов комплекса теоретических знаний и практических умений, необходимых для:

- разработки и применения предметно-ориентированных программных средств в сфере информационной безопасности, с учётом специфики защищаемых объектов и угроз;
- проектирования и реализации программных компонентов, обеспечивающих защиту компьютерных сетей от несанкционированного доступа, атак и вредоносных воздействий;
- анализа архитектуры программных и сетевых решений, а также внедрения специализированных средств защиты информации в локальных и распределённых сетях;
- формирования навыков выбора, настройки и интеграции прикладных решений для обеспечения комплексной защиты сетевой инфраструктуры организации.

- Код и - наименова ние профессион ально го - стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	Наименование	Урове нь квали фикац ии	Наименование	Код	Уровень (подуров ень) квалифи кации
06.026 Системный администратор информационно-коммуникационных систем	D	Обслуживание серверных операционных систем информационно-коммуникационной системы	6	Выполнение работ по выявлению и устранению нетипичных инцидентов, возникающих в серверных операционных системах информационно-коммуникационной системы	D/01.6	6
				Проведение анализа и определе- ние основных причин сложных проблем, возникающих на серверах и в серверных операционных системах	D/02.6	6

			Выполнение планирования резервного копирования, архивирования и восстановления конфигурации серверов и серверных операционных систем	D/03.6	6
			Планирование изменений параметров работы серверов и серверных операционных систем	D/04.6	6
			Выполнение обновления программного обеспечения серверных операционных систем	D/05.6	6
			Прогнозирование влияния внешних и внутренних воздействий на поведение серверных операционных систем	D/06.6	6
			Прогнозирование потребности в изменении объемов необходимых ресурсов для обеспечения бесперебойной работы серверов и серверных операционных систем	D/07.6	6
			Планирование и проведение работ по распределению нагрузки между имеющимися ресурсами, снятию нагрузки на серверы и серверные операционные системы перед проведением регламентных работ, восстановлению штатной схемы работы в случае сбоев	D/08.6	6
			Определение потребностей в приобретении специализированных средств контроля и тестирования серверов и серверных операционных систем	D/09.6	6

Место учебной дисциплины в структуре основной профессиональной образовательной программы

Дисциплина **«Разработка предметно-ориентированных программных средств. Защита компьютерных сетей»** относится к вариативной части профессионального цикла. Для её успешного освоения обучающемуся необходимы знания и навыки, полученные при изучении курсов **«Информатика»**, **«Языки программирования»**, **«Компьютерные сети»**, **«Операционные системы»**, **«Информационная безопасность»**.

Данная дисциплина является основой для последующего изучения специализированных курсов, связанных с практической реализацией средств защиты информации, построением безопасных программных решений и комплексной защитой компьютерных сетей.

В результате освоения дисциплины обучающийся должен:

Знать:

- основы построения предметно-ориентированных программных средств в контексте обеспечения информационной безопасности;
- принципы функционирования и архитектуру защищённых компьютерных сетей;
- основные угрозы информационной безопасности в сетевых системах и способы их программной нейтрализации;
- стандарты и регламенты в области защиты информации, включая применение криптографических и программных механизмов защиты.

Уметь:

- проектировать и разрабатывать программные решения, ориентированные на защиту информации в сетевых и распределённых системах;
- реализовывать модули аутентификации, контроля доступа и шифрования в прикладных программных средствах;
- проводить аудит безопасности сетевых приложений и выявлять потенциальные уязвимости;
- использовать программные инструменты для моделирования, анализа и мониторинга защищённых компьютерных сетей.

Владеть:

- практическими навыками разработки и внедрения прикладных программных решений, соответствующих требованиям информационной безопасности;
- средствами интеграции средств защиты информации в архитектуру информационной системы;
- методами программной реализации политик безопасности и управления доступом в компьютерных сетях.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

УК-1. Способен осуществлять поиск, критический анализ информации, применять системный подход для решения поставленных задач.	УК-1.1. Знать: методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа.
	УК-1.2. Уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач.
	УК-1.3. Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.
ПК-2. Способен выполнять работы по созданию (модификации) и сопровождению информационных систем.	ПК-2.1. Знать: процесс согласования и утверждения требований к типовой ИС; основные инженерно-технической поддержки подготовки коммерческого предложения заказчику на создание (модификацию) и ввод в эксплуатацию типовой ИС на этапе предконтрактных работ; модульное тестирование ИС (верификация); процесс интеграции ИС с существующими ИС заказчика; процесс планирования коммуникаций с заказчиком в рамках типовых регламентов организации; процесс проведения приемосдаточных испытаний (валидации) ИС в соответствии с установленными регламентами. ПК-2.2. Уметь: определить первоначальные требования заказчика к ИС и возможности их реализации в типовой ИС на этапе предконтрактных работ; исправлять дефекты и несоответствий в коде ИС и документации к ИС; идентифицировать конфигурацию ИС в соответствии с регламентами организации. ПК-2.3. Иметь навыки: интеграционного тестирования ИС; настройки оборудования, необходимого для работы ИС; адаптации

Структура и содержание дисциплины

«Разработка предметно-ориентированных программных средств, защита компьютерных сетей

»

Структура дисциплины (модуля) Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 часов.

	Всего	Порядковый номер семестра		
		4		
Общая трудоемкость дисциплины, в том числе:	72			
Курсовой проект (работа)				
Аудиторные занятия всего В том числе:		+		
Лекции	14	+		
Практические занятия, семинары		+		
Лабораторные работы	14			
Самостоятельная работа	44	+		
Вид итоговой аттестации:				
Зачет/дифф.зачет		+		
К.С.Р.				
Экзамен				
Общая трудоемкость дисциплины	72			

Наименование разделов и тем дисциплины и распределение учебных часов

№	Наименование разделов и тем	Объём часов	Лекции	Практические занятия	Самостоятельная работа
1	Введение в предметно-ориентированное программирование и основы защиты сетей	6	2	1	3
2	Архитектура и принципы функционирования компьютерных сетей	8	2	2	4
3	Угрозы и уязвимости в компьютерных сетях: анализ и классификация	8	2	2	4
4	Принципы построения предметно-ориентированных программных средств	8	2	2	4
5	Технологии и инструменты разработки ПО с элементами защиты	10	2	2	6
6	Средства защиты сетевого взаимодействия: шифрование, VPN, межсетевые экраны	10	2	2	6
7	Моделирование атак и разработка защитных программных модулей	8	1	2	5
8	Интеграция ПО защиты в инфраструктуру организации	6	1	1	4
9	Проектная деятельность: разработка предметно-ориентированного защищённого решения	8	0	2	6
	Итого	72	14	14	44

Содержание учебной дисциплины

Тема 1: Введение в предметно-ориентированное программирование и защиту компьютерных сетей

Содержание темы:

- **Понятие предметно-ориентированного программирования (ПОПС).**
- **Роль ПОПС в информационной безопасности.**
- **Классификация угроз в компьютерных сетях.**
- **Основные понятия: модели угроз, атакующие, защищаемые объекты.**

Формы и методы проведения занятий:

- **Лекция с презентацией.**
- **Обсуждение актуальных угроз и атак.**
- **Лабораторная работа №1:**

Анализ сетевого трафика с помощью Wireshark. Определение потенциальных угроз.

Тема 2: Архитектура и принципы построения компьютерных сетей

Содержание темы:

- **Основы архитектуры сетей: модели OSI и TCP/IP.**
- **Компоненты сетевой инфраструктуры.**
- **Протоколы канального, сетевого и транспортного уровней.**

Формы и методы проведения занятий:

- **Лекция с визуальными схемами.**
- **Практическое моделирование сетевых структур.**
- **Лабораторная работа №2:**

Настройка локальной сети в виртуальной среде (GNS3, Cisco Packet Tracer).

Тема 3: Угрозы и уязвимости в компьютерных сетях

Содержание темы:

- **Типовые атаки на компьютерные сети (DoS, MITM, ARP-spoofing и др.).**
- **Уязвимости программного обеспечения.**
- **Инструменты анализа безопасности.**

Формы и методы проведения занятий:

- **Лекция с демонстрацией сценариев атак.**
- **Обсуждение инцидентов информационной безопасности.**
- **Лабораторная работа №3:**

Моделирование сетевой атаки и её обнаружение средствами IDS/IPS (например, Snort).

Тема 4: Проектирование предметно-ориентированных программных средств

Содержание темы:

- **Принципы ПОПС: анализ предметной области, формализация, шаблоны проектирования.**
- **Языки программирования и инструменты разработки.**
- **Требования безопасности при проектировании.**

Формы и методы проведения занятий:

- **Лекция с анализом шаблонов проектирования.**
- **Работа с UML-диаграммами.**
- **Лабораторная работа №4:**

Проектирование и реализация программного модуля аутентификации пользователей.

Тема 5: Программные средства защиты компьютерных сетей

Содержание темы:

- **Межсетевые экраны, NAT, VPN, антивирусные системы.**
- **Протоколы безопасности: SSL/TLS, IPsec, SSH.**
- **Настройка и тестирование защитных решений.**

Формы и методы проведения занятий:

- **Лекция с примерами из практики.**
- **Работа с конфигурационными файлами.**
- **Лабораторная работа №5:**

Настройка защищённого VPN-соединения между двумя узлами сети.

Тема 6: Защищённое программное взаимодействие в распределённых системах

Содержание темы:

- **Безопасные API и протоколы обмена (REST, JSON Web Token, OAuth).**
- **Методы защиты на уровне приложений.**
- **Примеры программных решений с защитой данных.**

Формы и методы проведения занятий:

- **Лекция с примерами реализации.**
- **Обсуждение принципов безопасного программирования.**
- **Лабораторная работа №6:**

Разработка защищённого REST API с авторизацией и шифрованием передаваемых данных.

Тема 7: Анализ практических решений по защите сетей

Содержание темы:

- Кейсы защищённых информационных систем.
- Анализ типичных ошибок при разработке.
- Интеграция защитных решений в инфраструктуру организации.

Формы и методы проведения занятий:

- Лекция с анализом кейсов.
- Семинар с разбором проектов.
- Лабораторная работа №7:

Анализ готового защищённого программного решения. Поиск и исправление уязвимостей.

Тема 8: Проектная деятельность

Содержание темы:

- Выбор темы и цели проекта.
- Этапы разработки предметно-ориентированного ПО с функциями сетевой безопасности.
- Презентация и защита результатов.

Формы и методы проведения занятий:

- Самостоятельная работа под руководством преподавателя.
- Консультации и код-ревью.
- Лабораторная работа №8:

Разработка и защита итогового проекта: программный модуль/система, реализующая защиту сетевого взаимодействия в заданной предметной области.

Экзаменационные вопросы по дисциплине «

Модуль 1. Введение и основы

1. Понятие предметно-ориентированного программирования: цели, задачи и особенности.
2. Основные угрозы информационной безопасности в компьютерных сетях.
3. Модели архитектуры компьютерных сетей: сравнение моделей OSI и TCP/IP.
4. Элементы и структура цифровых систем управления и автоматизации.
5. Принципы построения защищённых программно-аппаратных систем.

Модуль 2. Программирование и проектирование

6. Основы объектно-ориентированного и предметно-ориентированного подходов в программировании.
7. Этапы проектирования предметно-ориентированных программных средств.
8. Основные шаблоны проектирования ПО и их применение в системах безопасности.
9. Требования к безопасной архитектуре программного обеспечения.
10. Роль UML-диаграмм в разработке защищённых программных систем.

Модуль 3. Сетевые технологии и протоколы

11. Назначение и функции основных сетевых протоколов (IP, TCP, UDP, DNS, DHCP).
12. Классификация сетевых атак и методы их предотвращения.
13. Принцип работы и настройка VPN-соединений.
14. Особенности применения протоколов SSL/TLS и IPsec в системах безопасности.
15. Межсетевые экраны: виды, принципы работы и примеры настройки.

Модуль 4. Средства и методы защиты

16. Системы обнаружения и предотвращения вторжений (IDS/IPS): архитектура и применение.
17. Антивирусные технологии: методы обнаружения вредоносного ПО.
18. Принципы и методы криптографической защиты данных.
19. Программные средства защиты на прикладном уровне: токены, JWT, OAuth 2.0.
20. Методы контроля целостности программного обеспечения и данных.

Модуль 5. Практические аспекты

21. Особенности разработки безопасного REST API.
22. Применение анализа уязвимостей в процессе разработки программных систем.
23. Роль логирования и мониторинга в обеспечении безопасности ПО.
24. Защита клиент-серверных приложений: подходы и реализация.
25. Интеграция средств защиты в информационную инфраструктуру организации.

Модуль 6. Проектная деятельность

26. Этапы реализации проекта по разработке ПО с функциями защиты.
27. Основные ошибки при проектировании защищённых информационных систем.
28. Методы верификации и тестирования безопасности программных решений.
29. Примеры успешных программных решений в области защиты сетей.
30. Роль предметной области в формировании требований к системе безопасности.

**Перечень основной и дополнительной учебной литературы,
Необходимой для освоения дисциплины**

1. Угрюмов, Евгений Павлович. Цифровая схемотехника : учебное пособие / Е. П. Угрюмов. - 2-е изд., перераб. и доп. - СПб. : БХВ - Петербург, 2007. - 782 с
2. Зиятдинов, Сергей Ильич (проф.). Схемотехника телекоммуникационных устройств [Текст] : учебник / С. И. Зиятдинов, Т. А. Суетина, Н. В. Поваренкин. - М. : Академия, 2013. - 368 с
3. Шишмарев, В. Ю. Основы автоматического управления [Текст] : учебное пособие / В. Ю. Шишмарев. - М. : Академия, 2008. - 352 с
4. Технические средства автоматизации и управления: Учебное пособие / Шишов О.В. - М.:НИЦ ИНФРА-М, 2016. - 396 с

**Перечень ресурсов информационно-телекоммуникационной сети
«Интернет»**

1. <http://mexalib.com/view/2880> - Петров И.В. Программируемые контроллеры. Стандартные языки и приемы прикладного проектирования. 2004
2. <http://freecomputerbooks.com/AutomatingManufacturing-Systems-with-PLCs.html> <http://www.razym.ru/79485-programmiruemye-kontrollery-rukovodstvo-dlya.html> Э. Папп - Программируемые контроллеры: руководство для инженера. 200
3. <https://www.arduino.cc/>

Перечень информационных технологий

Для проведения лекционных и лабораторных занятий рекомендуется использовать программное обеспечение: операционная система Linux с ядром 3.2 и выше, обслуживающие программы и среды разработки программ по выбору преподавателей.

Электронная поддержка дисциплины

При изучении дисциплины для проработки всех тем и выполнения заданий по всем темам студенты могут использовать различные учебно-методические материалы, размещаемые в электронном виде преподавателями на файловом ftp- сервере, в хранилище полнотекстовых материалов, а также в электронной образовательной среде, которая предполагает также возможность обмена информацией с преподавателем для подготовки заданий. Доступ студентов к студенческому файловому серверу, хранилищу полнотекстовых материалов, электронной образовательной среде осуществляется с использованием с использованием учетных записей студентов.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02

«Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от «__19__» сентября 2017 г. No 926(ред.8.02.2021).

Программу составили: ассистент кафедры «Информационные системы и технологии» Евлоев И.Т.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол №6 от «03» марта 2025 года

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол №7 от «13» марта 2025 года

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Б1.В.ДВ.03.01 Разработка предметно-ориентированных программных средств.

Защита компьютерных сетей

Направление подготовки

09.03.02 Информационные системы и технологии

-

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, очно-заочно

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Типовой тест промежуточной аттестации

1. Что является основой предметно-ориентированного программирования?

- A) Упрощение синтаксиса языка программирования
- + B) Использование предметной области в моделировании
- C) Автоматическое тестирование
- D) Многозадачность и управление потоками

2. Что представляет собой модель OSI?

- A) Протокол передачи данных
- B) Аппаратный стандарт
- + C) Эталонная сетевая модель
- D) Программное обеспечение маршрутизатора

3. Какой протокол отвечает за установление защищённого соединения?

- A) FTP
- B) HTTP
- + C) TLS
- D) DNS

4. Что обеспечивает межсетевой экран (firewall)?

- + A) Контроль входящего и исходящего трафика
- B) Управление доступом к базам данных
- C) Шифрование пользовательских данных
- D) Мониторинг уровня заряда оборудования

5. Что из перечисленного относится к средствам аутентификации?

- A) VPN
- + B) Пароль
- C) SQL-запрос
- D) Сжатие данных

6. Какой метод защиты информации реализует принцип «шифруй всё»?

- A) Брандмауэр
- + B) Криптографическая защита
- C) RAID-массив
- D) IDS-система

7. Что такое IDS?

- + A) Система обнаружения вторжений
- B) Инструмент для разработки ПО
- C) Сетевой протокол передачи видео
- D) Сервис маршрутизации

8. Какой язык чаще всего используется для создания REST API?

- A) Pascal
- + B)
- C) SQL
- D) Verilog

9. Какой протокол используется для передачи IP-адресов в сети?

- A) SMTP
- B) HTTP
- + C) DHCP
- D) SSL

10. Что такое CSRF-атака?

- A) Атака на файловую систему
- + B) Подделка межсайтового запроса
- C) Перехват пароля

D) Вирус-шифровальщик

11. Что из ниже перечисленного является компонентом микроконтроллера?

+ A) АЦП (аналогово-цифровой преобразователь)

B) Коммутатор

C) Маршрутизатор

D) BIOS

12. Что такое SQL-инъекция?

A) Метод передачи данных через API

+ B) Метод внедрения вредоносных SQL-запросов

C) Способ генерации паролей

D) Средство аутентификации пользователей

13. Что делает протокол IPsec?

A) Обеспечивает адресацию в сети

+ B) Обеспечивает безопасную передачу данных по сети

C) Отвечает за потоковое видео

D) Сканирует вирусы на клиентском устройстве

14. Для чего используется токен в системах авторизации?

A) Для хранения конфигураций

+ B) Для подтверждения прав доступа пользователя

C) Для загрузки операционной системы

D) Для создания сетевых протоколов

15. Какой метод тестирования безопасности включает проверку на уязвимости вручную или с помощью сканеров?

A) Функциональное тестирование

B) Интеграционное тестирование

+ C) Анализ уязвимостей

D) Нагрузочное тестирование

Типовой вариант задания на контрольную работу

Вариант №__

Цель работы:

Проверка уровня усвоения теоретических положений и практических навыков в области разработки предметно-ориентированных программных средств, а также оценки и реализации базовых мер защиты компьютерных сетей.

ЗАДАНИЕ

Часть 1. Теоретическая (письменная)

Ответьте на следующие вопросы развернуто:

1. Раскройте понятие предметно-ориентированного программирования. Приведите примеры использования в прикладных системах.
2. Классификация и характеристики угроз информационной безопасности в локальных и корпоративных сетях.
3. Архитектура предметно-ориентированных программных средств: основные компоненты и принципы взаимодействия.
4. Методы защиты сетевых соединений на уровне транспортного и сетевого уровней модели OSI.

5. Опишите этапы проектирования и разработки простого предметно-ориентированного приложения для мониторинга сетевой активности.
-

Часть 2. Практическая

Выполните одно из заданий (на выбор преподавателя или по указанию обучающегося):

Задание 2.1.

Разработайте консольное приложение (или веб-интерфейс) на любом языке программирования (, JavaScript, C# и др.), реализующее:

- Сбор и отображение данных о текущих IP-соединениях на устройстве;
- Логирование активности в текстовый файл;
- Возможность фильтрации по порту/протоколу/адресам.

Задание 2.2.

Смоделируйте элементарную систему авторизации с применением токенов (JWT, OAuth 2.0 и др.):

- Создание пользователя;
- Выдача токена при входе;
- Проверка валидности токена при доступе к защищённому ресурсу.

Приложите схему или описание логики.

Задание 2.3.

Проведите анализ защищённости условной сети предприятия:

- Опишите сетевую архитектуру (можно на схеме);
- Перечислите потенциальные уязвимости и возможные точки входа злоумышленника;
- Предложите меры по защите (firewall, VPN, IDS/IPS и т.д.).

Оформление и требования:

- Теоретическая часть — в объеме **5–7 страниц**.
- Практическая часть — код, скриншоты или схемы (по необходимости), краткие пояснения к каждому этапу.
- Формат: .docx или .pdf, прилагаемые файлы (если есть): .py, .js, .html и т.д.
- Срок выполнения: по индивидуальному графику преподавателя.

Экзаменационные вопросы по дисциплине

Модуль 1. Введение и основы

1. Понятие предметно-ориентированного программирования: цели, задачи и особенности.
2. Основные угрозы информационной безопасности в компьютерных сетях.
3. Модели архитектуры компьютерных сетей: сравнение моделей OSI и TCP/IP.
4. Элементы и структура цифровых систем управления и автоматизации.
5. Принципы построения защищённых программно-аппаратных систем.

Модуль 2. Программирование и проектирование

11. Основы объектно-ориентированного и предметно-ориентированного подходов в программировании.
12. Этапы проектирования предметно-ориентированных программных средств.
13. Основные шаблоны проектирования ПО и их применение в системах безопасности.
14. Требования к безопасной архитектуре программного обеспечения.
15. Роль UML-диаграмм в разработке защищённых программных систем.

Модуль 3. Сетевые технологии и протоколы

16. Назначение и функции основных сетевых протоколов (IP, TCP, UDP, DNS, DHCP).
17. Классификация сетевых атак и методы их предотвращения.
18. Принцип работы и настройка VPN-соединений.
19. Особенности применения протоколов SSL/TLS и IPsec в системах безопасности.
20. Межсетевые экраны: виды, принципы работы и примеры настройки.

Модуль 4. Средства и методы защиты

21. Системы обнаружения и предотвращения вторжений (IDS/IPS): архитектура и применение.
22. Антивирусные технологии: методы обнаружения вредоносного ПО.
23. Принципы и методы криптографической защиты данных.
24. Программные средства защиты на прикладном уровне: токены, JWT, OAuth 2.0.
25. Методы контроля целостности программного обеспечения и данных.

Модуль 5. Практические аспекты

26. Особенности разработки безопасного REST API.
27. Применение анализа уязвимостей в процессе разработки программных систем.
28. Роль логирования и мониторинга в обеспечении безопасности ПО.
29. Защита клиент-серверных приложений: подходы и реализация.
30. Интеграция средств защиты в информационную инфраструктуру организации.

Модуль 6. Проектная деятельность

31. Этапы реализации проекта по разработке ПО с функциями защиты.
32. Основные ошибки при проектировании защищённых информационных систем.
33. Методы верификации и тестирования безопасности программных решений.
34. Примеры успешных программных решений в области защиты сетей.
35. Роль предметной области в формировании требований к системе безопасности.

Типовая лабораторная работа по дисциплине

Лабораторная работа №1

Тема: Разработка простого предметно-ориентированного приложения для сетевого мониторинга

Цель работы:

Освоение базовых принципов разработки программных средств, ориентированных на выполнение прикладной задачи мониторинга сетевой активности, а также реализация элементарных методов защиты информации.

Задачи лабораторной работы:

- Познакомиться с концепцией предметной области (сетевой мониторинг);
 - Разработать приложение, которое отслеживает активные сетевые подключения;
 - Реализовать логирование активности в файл;
 - Применить простейшие меры защиты (например, шифрование логов или ограничение доступа к интерфейсу).
-

Оборудование и ПО:

- Компьютер с ОС Windows/Linux;
 - Установленный интерпретатор 3.x или аналог;
 - Среда разработки (например, VS Code, PyCharm, Thonny);
 - Библиотеки: psutil, socket, cryptography (опционально).
-

Ход выполнения работы:

1. **Создание проекта.**
Инициализируйте рабочую директорию и создайте файл monitor.py.
2. **Получение данных о сетевых соединениях.**
Используя модуль psutil, получите список активных соединений:

```
import psutil
```

```
for conn in psutil.net_connections():
```

```
    print(f"PID: {conn.pid}, Status: {conn.status}, Laddr: {conn.laddr}, Raddr: {conn.raddr}")
```

3. **Формирование логов.**
Реализуйте запись данных в текстовый лог-файл с указанием времени:

```
from datetime import datetime
```

```
with open("log.txt", "a") as f:
    f.write(f"{datetime.now()}: {conn}\n")
```

4. Простейшая защита логов (по выбору):

- Ограничение доступа к файлу логов (через права доступа ОС);
- Или шифрование с использованием модуля cryptography.

5. Создание предметно-ориентированного интерфейса (минимальный CLI).

```
def show_connections():
    # отображение текущих соединений
    pass

def save_log():
    # логирование
    pass

while True:
    cmd = input("Введите команду (show, log, exit): ")
    if cmd == "show":
        show_connections()
    elif cmd == "log":
        save_log()
    elif cmd == "exit":
        break
```

Контрольные вопросы:

1. Что понимается под предметно-ориентированным программным обеспечением?
2. Какие библиотеки используются для работы с сетями и логированием?
3. Перечислите базовые угрозы безопасности в сетевых приложениях.
4. Как можно обеспечить безопасность лог-файлов?

Форма отчета:

- Титульный лист;
- Цель и задачи лабораторной;
- Описание предметной области;
- Снимки экрана интерфейса программы;
- Листинг кода (основных функций);
- Ответы на контрольные вопросы;
- Выводы.