

Федеральное государственное бюджетное образовательное учреждение высшего
образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«22 » мая 2025 г., протокол № 9
Исполняющий обязанности
заведующего кафедрой



Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.В.ДВ.09.02 Сетевая безопасность

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
09.03.03 Прикладная информатика

профиль
Автоматизированные системы обработки информации и управления

Квалификация
бакалавр

Форма обучения
очная

Южно-Сахалинск
2025 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПКС-2	ПКС-2. Способен проводить формализацию предметной области с целью создания информационной системы	ПКС-2.1 - Знает требования к компьютерному программному обеспечению; виды технической спецификации на программные компоненты и их взаимодействие; методы проектирование компьютерного программного обеспечения ПКС-2.2 – Умеет применять требования к компьютерному программному обеспечению; разрабатывать технические спецификации на программные компоненты и их взаимодействие; применять методы проектирования компьютерного программного обеспечения; ПКС-2.3 – Владеет методами разработки требований к компьютерному программному обеспечению, технических спецификаций на программные компоненты, методами проектирования компьютерного программного обеспечения.
ПКС-3	ПКС-3 - Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС	ПКС-3.1 - Знает методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.2 - Умеет применять методы организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС; ПКС-3.3 - Владеет методами организации взаимодействия с заказчиком, планирования проекта, разработки, верификации и тестирования ИС.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Тема 1. Основы безопасности компьютерных сетей. Основные понятия и терминология, угрозы, уязвимости, атаки	ПКС-2, ПКС-3	Устный опрос по теме лекции
2.	Тема 2. Основы безопасности компьютерных сетей. Нормативно-правовое обеспечение информационной безопасности КС	ПКС-2, ПКС-3	Устный опрос по теме лекции .
3.	Тема 3 Основы безопасности компьютерных сетей. Классификация угроз и уязвимостей, банки угроз и уязвимостей, Банк данных угроз ФСТЭК, MITRE ATT&CK	ПКС-2, ПКС-3	Устный опрос по теме лекции

4.	Тема 4 Основы безопасности компьютерных сетей. Сетевые атаки, модель Cyber-Kill Chain	ПКС-2, ПКС-3	Устный опрос по теме лекции
5.	Тема 5 Средства обеспечения безопасности компьютерных сетей. Фильтрация сетевого трафика, межсетевые экраны, NGFW	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания
6.	Тема 6 Средства обеспечения безопасности компьютерных сетей. Технологии обнаружения сетевых атак, системы обнаружения и предотвращения вторжений	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания
7.	Тема 7. Средства обеспечения безопасности компьютерных сетей. Технологии построения защищенных каналов связи, средства построения виртуальных защищенных сетей	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания
8.	Тема 8. Средства обеспечения безопасности компьютерных сетей. Инструменты для исследования сети, снифферы и сканеры безопасности, инструменты мониторинга состояния сети	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания
9.	Тема 9 Средства обеспечения безопасности компьютерных сетей. Предотвращение утечек информации, DLP-системы	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания
10.	Тема 10 Средства обеспечения безопасности компьютерных сетей. Защита конечных устройств КС, технологии Endpoint Security, системы защиты конечных точек (Endpoint Protection Platform)	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания
11.	Тема 11. Современные тенденции в обеспечении безопасности компьютерных сетей Основы тестирования на проникновение, этапы проведения тестирования на проникновение, инструменты. XDR-системы	ПКС-2, ПКС-3	Устный опрос по теме лекции Выполнение практического задания

3. Оценочные средства

Тестирование является одним из средств формального контроля качества обучения – методе, основанном на стандартизированных заданиях, которые позволяют оценить знания, умения и навыки испытуемого

Требования к составлению тестового задания

Тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

– **закрытая** форма – является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов.

Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде.

Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

– **открытая** форма – вопрос представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие – части слова или буквы, условные обозначения, линии или изображения элементов схемы или графика.

Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

– **установление соответствия** – в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

– **установление последовательности** – предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Примерный тест

Вариант возможного итогового теста, проводимого на последнем занятии.

Компетенции, формируемые при изучении дисциплины:

ПКС-2. Способен проводить формализацию предметной области с целью создания информационной системы

ПКС-3 - Способен осуществлять организацию взаимодействия с заказчиком, планирования проекта ИС; руководить разработкой программного кода, верификацией и тестированием ИС

Вопрос 1. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей. Какое стандартное средство следует использовать для уменьшения риска такого рода атак?

- а) использовать систему обнаружения вторжений
- б) переименовать учетную запись администратора
- в) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации
- г) использовать мультифакторную аутентификацию

Правильный ответ: в)

Вопрос 2. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?

- а) система обнаружения вторжений
- б) персональный межсетевой экран
- в) трансляция сетевых адресов
- г) антивирусное программное обеспечение

Правильный ответ: в)

Вопрос 3. Какое из средств защиты используется для мониторинга сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности?

- а) межсетевой экран
- б) система анализа защищенности
- в) система предотвращения вторжений
- г) средство антивирусной защиты

Правильный ответ: в)

Вопрос 4. Как называется процесс защиты ресурсов сети от несанкционированного использования?

- а) охрана оборудования сети
- б) защита ядра безопасности
- в) контроль доступа
- г) защита периметра безопасности

Правильный ответ: в)

Вопрос 5. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?

- а) создать диапазон IP адресов
- б) создать параметр DHCP
- в) создать исключение для IP адреса

г) создать область DHCP

Правильный ответ: в)

Вопрос 6. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?

а) сетевой доступ

б) папка

в) каталог

г) домен

Правильный ответ: г)

Вопрос 7. Какой протокол используется для доступа к службе каталогов Active Directory?

а) ShareDiscovery

б) ADSL

в) LDAP

г) ICMP

Правильный ответ: в)

Вопрос 8. Как называется компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам?

а) хаб

б) рабочая станция

в) сервер

г) хост

Правильный ответ: в)

Вопрос 9. В каком методе передачи данные пересылаются в двух направлениях одновременно?

а) симплексный

б) синхронный

в) дуплексный

г) полудуплексный

Правильный ответ: в)

Вопрос 10. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?

а) синхронном

б) асинхронном

в) туннельном

г) транспортном

Правильный ответ: в)

Вопрос 11. Определите стандартный механизм, который следует использовать для уменьшения риска подбора паролей (брутфорс-атак), согласно записям в журнале аутентификации.

(Выберите один вариант ответа)

А) Использование системы обнаружения вторжений (IDS)

Б) Переименование учетной записи администратора

В) Включение блокировки учетных записей при определенном количестве неуспешных попыток входа

Г) Использование трансляции сетевых адресов (NAT)

Ответ: В

Вопрос 12. Назовите технологию, которая позволяет скрыть схему IP-адресации внутренней сети от внешних пользователей.

(Выберите один вариант ответа)

- А) Система обнаружения вторжений (IDS)
- Б) Персональный межсетевой экран
- В) Трансляция сетевых адресов (NAT)
- Г) Антивирусное программное обеспечение

Ответ: В

Вопрос 13. Установите соответствие между типом средства защиты информации и его основным назначением.

№	Средство защиты	Назначение
1	Межсетевой экран	А) Обнаружение и блокировка вредоносной активности в реальном времени
2	Система предотвращения вторжений (IPS)	Б) Фильтрация трафика на основе заданных правил
3	DLP-система	В) Выявление уязвимостей в информационных системах
4	Сканер безопасности	Г) Предотвращение утечек конфиденциальной информации

Ответ: 1-Б, 2-А, 3-Г, 4-В

Вопрос 14. Определите режим работы протокола IPsec, при котором шифруется весь исходный IP-пакет целиком и помещается в новый пакет.

(Выберите один вариант ответа)

- А) Транспортный режим
- Б) Туннельный режим
- В) Асинхронный режим
- Г) Симплексный режим

Ответ: Б

Вопрос 15. Назовите протокол, используемый для доступа к службе каталогов Active Directory.

(Выберите один вариант ответа)

- А) HTTP
- Б) FTP
- В) LDAP
- Г) SMTP

Ответ: В

Вопрос 16. Выберите из списка понятия, которые относятся к основам безопасности компьютерных сетей (три правильных ответа).

(Выберите несколько вариантов ответа)

- А) Угроза

- Б) Доменное имя
- В) Уязвимость
- Г) IP-адрес
- Д) Атака

Ответ: А, В, Д

Вопрос 17. Дополните предложение.

Процесс проверки подлинности пользователя называется _____, а процесс определения прав доступа к ресурсам — _____.

Ответ: аутентификация, авторизация

Вопрос 18. Назовите модель, которая описывает жизненный цикл кибератаки от разведки до достижения цели.

(Выберите один вариант ответа)

- А) Модель OSI
- Б) Модель TCP/IP
- В) Модель Cyber Kill Chain
- Г) Модель Белла — ЛаПадулы

Ответ: В

Вопрос 19. Определите, верно ли следующее утверждение: «Основная функция DLP-системы — это фильтрация сетевого трафика по портам и протоколам».

(Выберите один вариант ответа)

- А) Да, верно
- Б) Нет, это функция межсетевого экрана

Ответ: Б

Вопрос 20. Укажите действие, которое необходимо выполнить на DHCP-сервере, чтобы исключить выдачу конкретного IP-адреса клиентам.

(Выберите один вариант ответа)

- А) Создать новую область DHCP
- Б) Создать исключение (резервирование) для IP-адреса
- В) Перезапустить службу DHCP
- Г) Изменить маску подсети

Ответ: Б

Вопрос 21. Расположите этапы проведения тестирования на проникновение (пентеста) в правильной последовательности.

(Установите правильную последовательность)

- А) Эксплуатация уязвимостей
- Б) Разведка и сбор информации
- В) Анализ рисков и составление отчета
- Г) Закрепление в системе и очистка следов

Ответ: Б, А, Г, В

Вопрос 22. Определите, какое средство безопасности относится к классу Endpoint Protection Platform (EPP).

(Выберите один вариант ответа)

- А) Межсетевой экран уровня предприятия
- Б) Система защиты конечных точек (рабочих станций)
- В) SIEM-система
- Г) Криптографический шлюз

Ответ: Б

Вопрос 23. Назовите списки правил, определяющие разрешенные или запрещенные типы трафика на межсетевом экране.

(Краткий ответ)

Ответ: Политики безопасности / Списки доступа (ACL)

Вопрос 24. Определите организацию в РФ, которая ведет банк данных угроз информационной безопасности.

(Выберите один вариант ответа)

- А) MITRE
- Б) Минцифры России
- В) ФСТЭК России
- Г) Роскомнадзор

Ответ: В

Вопрос 25. Выберите два основных типа систем обнаружения вторжений (IDS) по способу мониторинга.

(Выберите несколько вариантов ответа)

- А) Сетевые (NIDS)
- Б) Сигнатурные
- В) Хостовые (HIDS)
- Г) Эвристические

Ответ: А, В

Вопрос 26. Назовите метод передачи данных, при котором информация передается в двух направлениях одновременно.

(Выберите один вариант ответа)

- А) Симплексный
- Б) Полудуплексный
- В) Дуплексный
- Г) Синхронный

Ответ: В

Вопрос 27. Определите зону сети (сегмент), которая обычно используется для размещения публичных серверов (веб, почта), доступных из Интернета.

(Краткий ответ)

Ответ: Демилитаризованная зона (DMZ)

Вопрос 28. Укажите основное назначение технологии VPN (Virtual Private Network).

(Выберите один вариант ответа)

- А) Увеличение скорости интернет-соединения
- Б) Создание защищенного канала связи поверх сети общего пользования
- В) Блокировка рекламных баннеров
- Г) Анонимизация трафика в Tor

Ответ: Б

Вопрос 29. Определите функцию, которая является отличительной для межсетевого экрана нового поколения (NGFW) по сравнению с классическим (Stateful Inspection).

(Выберите один вариант ответа)

- А) Анализ трафика на уровне приложений (прикладной уровень)
- Б) Фильтрация по IP-адресам
- В) Фильтрация по номерам портов
- Г) Ведение логов соединений

Ответ: А

Вопрос 30. Установите соответствие между названием сетевой атаки и ее описанием.

№	Атака	Описание
1	Перехват (Sniffing)	А) Атака на отказ в обслуживании, исчерпание ресурсов системы
2	DDoS	Б) Прослушивание сетевого трафика
3	Спуфинг (Spoofing)	В) Внедрение вредоносного кода в базы данных через пользовательский ввод
4	SQL-инъекция	Г) Подмена сетевого адреса (например, IP-адреса отправителя)

Ответ: 1-Б, 2-А, 3-Г, 4-В

Критерии оценки знаний при проведении тестирования

Отметка «**отлично**» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «**хорошо**» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «**удовлетворительно**» выставляется при условии правильного ответа не менее 50 %;

Отметка «**неудовлетворительно**» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации