Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:32:53
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса»
(ФГБОУ ВО «ПВГУС»)

УТВЕРЖДЕНО

на заседании Высшей школы интеллектуальных систем и кибертехнологий

Протокол от 06.09.2024 г. № 2

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(фонд оценочных средств)
для проведения промежуточной аттестации по дисциплине

«Сети и системы передачи информации»
наименование дисциплины

по образовательной программе высшего образования – программе **бакалавриата**

«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»
наименование образовательной программы

10.03.01 «Информационная безопасность»
шифр, наименование направления подготовки / специальности

Составители Коновалова Анжелика Денисовна, старший преподаватель, Высшая школа интеллектуальных систем и кибертехнологий
Курцев Евгений Александрович, ассистент, Высшая школа интеллектуальных систем и кибертехнологий
ФИО, должность, структурное подразделение, ученая степень, ученое звание

Тольятти
2025

1. Паспорт фонда оценочных средств (далее – ФОС)

1.1. Планируемые результаты обучения по дисциплине

Код компетенции	Наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИОПК-2.1. Применяет информационно-коммуникационные технологии, в том числе отечественного производства, для решения задач профессиональной деятельности
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИОПК-9.1. Знает основные характеристики, достоинства и недостатки средств криптографической и технической защиты информации в автоматизированных системах. ИОПК-9.2. Применяет средства криптографической и технической защиты информации от утечки.

В результате изучения дисциплины обучающийся должен:

владеть: навыками разработки логической схемы сети, настройки типовых сетевых функций и поиска неисправностей с использованием программных средств; навыками анализа защищенности сетевого взаимодействия и проверки действия базовых мер криптографической и технической защиты.

уметь: выполнять адресацию, базовую настройку сетевых узлов и сервисов, анализировать трафик и применять диагностические средства; применять сегментацию, фильтрацию, защищенные протоколы и средства контроля трафика для снижения сетевых рисков.

знать: принципы построения сетей и систем передачи информации, модели сетевого взаимодействия, назначение протоколов, оборудования и программных средств; основные угрозы при передаче информации и характеристики криптографических и технических средств защиты сетевого взаимодействия.

1.2. Содержание дисциплины

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
1.	Основы сетей и модели передачи информации	ОПК-2 ОПК-9
2.	Физический и канальный уровни передачи данных	ОПК-2 ОПК-9
3.	Сетевая адресация и протоколы межсетевого уровня	ОПК-2 ОПК-9
4.	Коммутация и виртуальные локальные сети	ОПК-2 ОПК-9
5.	Маршрутизация в IP-сетях	ОПК-2 ОПК-9
6.	Транспортные и прикладные сетевые протоколы	ОПК-2 ОПК-9
7.	Беспроводные сети и качество передачи информации	ОПК-2 ОПК-9

№	Тема (раздел дисциплины) (в соответствии с РПД)	Код компетенции
8.	Проектирование, диагностика и базовая защита сети	ОПК-2 ОПК-9

1.3. Система оценивания по дисциплине

Дисциплина изучается в течение одного семестра.

Форма промежуточной аттестации по дисциплине - экзамен.

Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
		70-85,9	«хорошо» / 4	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

2. Перечень оценочных материалов для проведения промежуточной аттестации

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения лабораторных и практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

Перечень вопросов и заданий для подготовки к экзамену

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности

1. Назначение и классификация компьютерных сетей.
2. Основные компоненты системы передачи информации.
3. Уровни и функции эталонной модели OSI.
4. Структура модели TCP/IP и ее соответствие модели OSI.
5. Инкапсуляция и деинкапсуляция сетевых данных.
6. Физические среды передачи данных и их характеристики.
7. Полоса пропускания, задержка, джиттер и потери пакетов.
8. Назначение и структура Ethernet-кадра.
9. MAC-адресация и доставка кадров в локальной сети.
10. Принцип работы сетевого коммутатора.
11. Таблица MAC-адресов и процесс обучения коммутатора.
12. Виртуальные локальные сети VLAN и транковые соединения.
13. Назначение протоколов предотвращения петель коммутации.
14. Структура IPv4-адреса и назначение маски подсети.
15. Методы разбиения сети на подсети.
16. Особенности адресации IPv6.
17. Назначение протоколов ARP и NDP.
18. Назначение и типы сообщений ICMP.

19. Структура таблицы маршрутизации.
20. Статическая и динамическая маршрутизация.
21. Метрики маршрутов и выбор наилучшего пути.
22. Сравнение транспортных протоколов TCP и UDP.
23. Порты и сокеты в сетевом взаимодействии.
24. Установление и завершение TCP-соединения.
25. Назначение и принцип работы DNS.
26. Назначение и принцип работы DHCP.
27. Клиент-серверная и одноранговая модели взаимодействия.
28. Архитектура и режимы работы беспроводных сетей IEEE 802.11.
29. Назначение механизмов качества обслуживания QoS.
30. Основные средства и команды диагностики компьютерной сети.

ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности

1. Основные угрозы безопасности при передаче информации по сети.
2. Угрозы перехвата и анализа сетевого трафика.
3. Подмена сетевых узлов и атаки посредника.
4. Атаки отказа в обслуживании в компьютерных сетях.
5. Роль криптографической защиты в сетевом взаимодействии.
6. Роль технических средств защиты информации в компьютерной сети.
7. Назначение защищенных сетевых протоколов.
8. Протокол TLS и обеспечиваемые им свойства безопасности.
9. Назначение IPsec и основные режимы его работы.
10. Виртуальные частные сети и схемы их применения.
11. Аутентификация сторон сетевого взаимодействия.
12. Контроль целостности сетевых сообщений.
13. Сегментация сети как мера защиты информации.
14. Списки контроля доступа и принципы их построения.
15. Назначение и типы межсетевых экранов.
16. Возможности и ограничения NAT в обеспечении безопасности.
17. Сетевые системы обнаружения и предотвращения вторжений.
18. Источники данных для мониторинга сетевой безопасности.
19. Анализ сетевого трафика средствами Wireshark.
20. Защита беспроводной сети с использованием WPA2 и WPA3.
21. Безопасная настройка сетевых служб.
22. Защищенное администрирование с использованием SSH.
23. Применение SNMPv3 для безопасного мониторинга сети.
24. Сертификаты и управление ключами в защищенных соединениях.
25. Журналирование событий сетевого оборудования и средств защиты.
26. Безопасная базовая конфигурация сетевого устройства.
27. Контроль доступа устройств и пользователей к сети.
28. Резервное копирование конфигурации сетевого оборудования.
29. Критерии оценки эффективности мер сетевой защиты.
30. Принципы многоуровневой защиты компьютерной сети.