

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Выборнова Любовь Алексеевна

Должность: Ректор

Дата подписания: 29.09.2025 07:54:03

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»)

Колледж креативных индустрий и предпринимательства

УТВЕРЖДЕНО

на заседании ПЦК

по образовательной программе  
09.02.06 Сетевое и системное  
администрирование

Протокол от 22.11.2024 г. № 3

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств) для проведения промежуточной аттестации

### по междисциплинарному курсу

учебному предмету, дисциплине, междисциплинарному курсу, профессиональному модулю

### «Безопасность компьютерных сетей»

наименование учебного предмета, дисциплины, междисциплинарного курса, профессионального модуля

по образовательной программе среднего профессионального образования –

### программе подготовки специалистов среднего звена

программе подготовки специалистов среднего звена / программе подготовки квалифицированных рабочих, служащих

### Сетевое и системное администрирование

наименование образовательной программы

### 09.02.06 Сетевое и системное администрирование

шифр, наименование специальности / профессии

Составитель

Попов А.К., преподаватель Колледжа креативных  
индустрий и предпринимательства

ФИО, должность, структурное подразделение,  
ученая степень, ученое звание

Тольятти

2024

## 1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ (ДАЛЕЕ – ФОС)

### 1.1. Планируемые результаты обучения по междисциплинарному курсу

| Код компетенции | Наименование компетенции                                                             |
|-----------------|--------------------------------------------------------------------------------------|
| ПК 3.1          | Осуществлять проектирование сетевой инфраструктуры                                   |
| ПК 3.3          | Осуществлять защиту информации в сети с использованием программно-аппаратных средств |
| ПК 3.5          | Модернизировать сетевые устройства информационно-коммуникационных систем             |

### 1.2. Содержание междисциплинарного курса

| №  | Тема (раздел дисциплины)<br>(в соответствии с РПД)                   | Код компетенции        |
|----|----------------------------------------------------------------------|------------------------|
| 1. | Проблемы информационной безопасности компьютерных сетей              | ПК 3.1, ПК 3.3, ПК 3.5 |
| 2. | Криптографическая защита информации в компьютерных сетях             | ПК 3.1, ПК 3.3, ПК 3.5 |
| 3. | Идентификация, аутентификация и управление доступом                  | ПК 3.1, ПК 3.3, ПК 3.5 |
| 4. | Безопасность операционных систем                                     | ПК 3.1, ПК 3.3, ПК 3.5 |
| 5. | Современные подходы к обеспечению анонимности работы в сети Интернет | ПК 3.1, ПК 3.3, ПК 3.5 |
| 6. | Вредоносные программы и спам                                         | ПК 3.1, ПК 3.3, ПК 3.5 |

### 1.3. Система оценивания по междисциплинарному курсу

Междисциплинарный курс изучается в течение одного семестра. Форма промежуточной аттестации по дисциплине – дифференцированный зачет.

| Шкалы оценки уровня сформированности результатов обучения |                      | Шкала оценки уровня освоения дисциплины |                           |
|-----------------------------------------------------------|----------------------|-----------------------------------------|---------------------------|
| Уровневая шкала оценки компетенций                        | 100 бальная шкала, % | 100 бальная шкала, %                    | дифференцированная оценка |
| допороговый                                               | ниже 61              | ниже 61                                 | неудовлетворительно       |
| пороговый                                                 | 61-85,9              | 61-69,9                                 | удовлетворительно         |
|                                                           |                      | 70-85,9                                 | хорошо                    |
| повышенный                                                | 86-100               | 86-100                                  | отлично                   |

## 2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

### Вопросы для подготовки к дифференцированному зачету

| №                                                                | Содержание вопроса                                                                            |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>ПК 3.1 Осуществлять проектирование сетевой инфраструктуры</b> |                                                                                               |
| 1.                                                               | Какие этапы проектирования сетевой инфраструктуры необходимы для обеспечения её безопасности? |
| 2.                                                               | Как выбрать подходящие протоколы для безопасной передачи данных при проектировании сети?      |

| №                                                                                                  | Содержание вопроса                                                                                                                                 |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.                                                                                                 | Каковы основные принципы сегментации сети и как они влияют на безопасность инфраструктуры?                                                         |
| 4.                                                                                                 | Что такое модель "Zero Trust" и как она применяется при проектировании безопасной сетевой инфраструктуры?                                          |
| 5.                                                                                                 | Как выбрать и настроить устройства для защиты периметра сети (например, фаерволы, IDS/IPS)?                                                        |
| 6.                                                                                                 | Какова роль шифрования при проектировании безопасной сети и какие алгоритмы шифрования предпочтительны для разных типов трафика?                   |
| 7.                                                                                                 | Какие способы аутентификации пользователей и устройств наиболее эффективны при проектировании защищённых сетевых решений?                          |
| 8.                                                                                                 | Какие факторы необходимо учитывать при выборе и настройке VPN-сервисов для защиты удалённых пользователей и филиалов?                              |
| 9.                                                                                                 | Как обеспечить отказоустойчивость и высокую доступность сетевой инфраструктуры без ущерба для безопасности?                                        |
| 10.                                                                                                | Как проектировать защиту от DDoS-атак на уровне сетевой инфраструктуры?                                                                            |
| 11.                                                                                                | Какие риски безопасности следует учитывать при проектировании сетевых соединений между локальными сетями и облачными сервисами?                    |
| 12.                                                                                                | Какую роль играют ACL (списки управления доступом) в проектировании сетевой безопасности и как их правильно настроить?                             |
| 13.                                                                                                | Как учесть безопасность IoT-устройств при проектировании корпоративной сети?                                                                       |
| 14.                                                                                                | Какие методы защиты от несанкционированного доступа к сети следует применять в процессе проектирования беспроводных сетей?                         |
| 15.                                                                                                | Как мониторинг и анализ трафика помогают в проектировании безопасной сетевой инфраструктуры, и какие инструменты для этого используются?           |
| <b>ПК 3.3 Осуществлять защиту информации в сети с использованием программно-аппаратных средств</b> |                                                                                                                                                    |
| 16.                                                                                                | Какие программно-аппаратные средства используются для защиты информации в сети на уровне периметра?                                                |
| 17.                                                                                                | Какую роль в защите информации в сети играют фаерволы, и как они должны быть настроены для обеспечения максимальной безопасности?                  |
| 18.                                                                                                | Что такое IDS/IPS системы и как они помогают в защите информации в сети?                                                                           |
| 19.                                                                                                | Какую роль в защите данных в сети играет шифрование и какие алгоритмы шифрования предпочтительны для различных типов трафика?                      |
| 20.                                                                                                | Какие методы аутентификации и авторизации пользователей следует применять для повышения безопасности сети?                                         |
| 21.                                                                                                | Как защитить сетевые соединения от атак с использованием технологий виртуальных частных сетей (VPN)?                                               |
| 22.                                                                                                | Какие программно-аппаратные решения необходимы для защиты от атак "человек посередине" (Man-in-the-Middle)?                                        |
| 23.                                                                                                | Как эффективно использовать анти-DDoS устройства и системы для защиты сетевой инфраструктуры от распределённых атак отказа в обслуживании?         |
| 24.                                                                                                | Какие средства мониторинга и анализа трафика можно использовать для обнаружения вторжений и предотвращения угроз безопасности в сети?              |
| 25.                                                                                                | Как защитить беспроводные сети с использованием программно-аппаратных решений, таких как WPA3, и какие угрозы необходимо учитывать?                |
| 26.                                                                                                | Какие роли в защите информации в сети играют технологии управления доступом (например, ACL, VLAN)?                                                 |
| 27.                                                                                                | Какова роль хеш-функций и цифровых подписей в обеспечении целостности данных и предотвращении их подделки?                                         |
| 28.                                                                                                | Какие решения для защиты конечных устройств (антивирусы, EDR) следует использовать для защиты информации на рабочих станциях и серверах?           |
| 29.                                                                                                | Как настроить и использовать средства защиты для предотвращения утечек данных (DLP-системы) в сети?                                                |
| 30.                                                                                                | Какие аппаратные устройства защиты, такие как криптографические модули (HSM), используются для защиты ключей шифрования и других критичных данных? |
| <b>ПК 3.5 Модернизировать сетевые устройства информационно-коммуникационных систем</b>             |                                                                                                                                                    |

| №   | Содержание вопроса                                                                                                                                                  |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31. | Какие факторы следует учитывать при модернизации сетевых устройств для повышения уровня безопасности информационно-коммуникационных систем?                         |
| 32. | Как правильно выбрать и настроить новые фаерволы при модернизации сетевых устройств для защиты от современных угроз?                                                |
| 33. | Какие технологии могут быть использованы для модернизации маршрутизаторов и коммутаторов с целью повышения их безопасности?                                         |
| 34. | Как модернизировать устройства управления доступом (например, NAS, SAN) для улучшения защиты данных в сети?                                                         |
| 35. | Какие программно-аппаратные решения можно интегрировать в процесс модернизации сетевых устройств для защиты от DDoS-атак?                                           |
| 36. | Как улучшить защиту сети при модернизации беспроводных точек доступа с использованием современных стандартов безопасности (WPA3)?                                   |
| 37. | Как интеграция средств мониторинга и анализа в процесс модернизации сетевых устройств помогает повысить уровень безопасности сети?                                  |
| 38. | Какие новые криптографические протоколы следует внедрить при модернизации сетевых устройств для улучшения шифрования данных в передаче?                             |
| 39. | Каковы особенности модернизации средств защиты от вторжений (IDS/IPS) в сети с учетом новых угроз?                                                                  |
| 40. | Какие методы защиты можно добавить при модернизации межсетевых экранов для более эффективного фильтрации трафика и предотвращения несанкционированного доступа?     |
| 41. | Как модернизация серверов и рабочих станций может повлиять на безопасность сети и какие меры следует предпринять для защиты этих устройств?                         |
| 42. | Какие аппаратные средства, такие как криптографические модули (HSM), должны быть интегрированы в процессе модернизации для улучшения защиты данных?                 |
| 43. | Как выбрать и настроить более защищённые решения для виртуализации сетевых устройств при модернизации сетевой инфраструктуры?                                       |
| 44. | Как модернизация сетевых устройств помогает обеспечить отказоустойчивость и высокую доступность при атакующих угрозах?                                              |
| 45. | Какие средства защиты от утечек данных (DLP-системы) следует интегрировать при модернизации сетевых устройств для обеспечения контроля за передаваемой информацией? |