**Министерство образования, науки и молодёжи Республики Крым**

**Государственное бюджетное профессиональное образовательное учреждение Республики Крым**

**«Чапаевский агротехнологический техникум им.ИН. Шатилова»**

УТВЕРЖДено

Директор ГБПОУ РК

«ЧАТ имени И.Н. Шатилова»

\_\_\_\_\_\_А.А. Булатова

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_202\_ г.

**Фонд оценочных средств**

**ПМ.03 Эксплуатация облачных сервисов**

по специальности

**09.02.06 Сетевое и системное администрирование**

Чапаевка, 202\_\_г

Фонд оценочных средств ПМ.03 разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования специальности: 09.02.06 Сетевое и системное администрирование, приказ Министерства просвещения РФ от 10 июля 2023 г. № 519,с учетом проекта примерной основной образовательной программы специальности: 09.02.06 Сетевое и системное администрирование, укрупненная группа специальностей 09.00.00 Информатика и вычислительная техника.

**Организация-разработчик:**

Государственное бюджетное профессиональное образовательное учреждение Республики Крым «Чапаевский агротехнологический техникум имени И.Н. Шатилова»

**Разработчик:** Халилов Руслан Алимович, преподаватель

Рассмотрено на заседании цикловой комиссии

Протокол № от « » 20 г.

Председатель МК / /

|  |  |
| --- | --- |
| **СОГЛАСОВАНО** | **СОГЛАСОВАНО** |
| *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*  Председатель Методического совета  ГБПОУ РК «ЧАТ имени И.Н. Шатилова» | \_\_\_\_\_\_\_\_\_\_\_\_\_  Директор « \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»  (*название предприятия)* |
| Протокол №\_\_\_\_\_ | «\_\_»\_\_\_\_\_\_\_\_\_\_\_\_202\_\_г. |
| «\_\_»\_\_\_\_\_\_\_202\_\_г. | М.П. |

**СОДЕРЖАНИЕ**

1. [Паспорт фонда оценочных средств 3](#_bookmark0)
   1. [Область применения фонда оценочных средств](#_bookmark1) 3
   2. [Результаты освоения дисциплины 3](#_bookmark2)
2. [Перечень оценочных средств](#_bookmark3) 3
3. [Оценочные средства текущего контроля и промежуточной аттестации 10](#_bookmark4)

# Паспорт фонда оценочных средств

# Область применения фонда оценочных средств

Фонд оценочных средств предназначен для оценки результатов освоения программного модуля ПМ.03 Эксплуатация облачных сервисов

# Результаты освоения дисциплины

В результате контроля оценки по дисциплине осуществляется комплексная проверка освоения следующих общих и профессиональных компетенций:

|  |  |
| --- | --- |
| **Код** | **Общие компетенции** |
| ОК 01 | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам |
| ОК 02 | Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности |
| ОК 03 | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях. |
| ОК 04 | Эффективно взаимодействовать и работать в коллективе и команде |
| ОК 05 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста |
| ОК 06 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения |
| ОК 07 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях |
| ОК 08 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности |
| ОК 09 | Пользоваться профессиональной документацией на государственном и иностранном языках |

|  |  |
| --- | --- |
| **Код** | **Профессиональные компетенции** |
| ПК 3.1. | Осуществлять развертывание облачной инфраструктуры |
| ПК 3.2. | Проводить документирование требований и технических возможностей облачных инфраструктур |
| ПК 3.3. | Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки |
| ПК 3.4. | Производить хранение и анализ данных |
| ПК 3.5. | Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов |
| ПК 3.6. | Проводить мониторинг системы в облачных сервисах |

# Перечень оценочных средств

|  |  |  |
| --- | --- | --- |
| **Виды деятельности** | **Код и наименование**  **компетенции** | **Показатели освоения компетенции** |
| ВД 3. Эксплуатация облачных сервисов | ПК 3.1. Осуществлять развертывание облачной инфраструктуры | Практический опыт:  Обслуживать облачную инфраструктуру, восстанавливать работоспособность сети после сбоя. Осуществлять удаленное администрирование и восстановление работоспособности облачной инфраструктуры. Поддерживать пользователей сети, настраивать аппаратное и программное обеспечение облачной инфраструктуры. Обеспечивать защиту облачных устройств. Внедрять механизмы облачной безопасности на втором уровне модели OSI. Внедрять механизмы облачной безопасности с помощью межсетевых экранов. Внедрять технологии VPN. Настраивать IP-телефоны. |
| Умения: Тестировать кабели и коммуникационные устройства. Описывать концепции облачной безопасности. Описывать современные технологии и архитектуры безопасности. Описывать характеристики и элементы конфигурации этапов VoIP звонка. |
|  |  | Знания: Архитектуру и функции систем управления сетями, стандарты систем управления. Задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией. Правила эксплуатации технических средств сетевой инфраструктуры. Методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных. Основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных. Средства мониторинга и анализа локальных сетей. Основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем. Принципы работы сети аналоговой телефонии. Назначение голосового шлюза, его компоненты и функции. Основные принципы технологии обеспечения QoS для голосового трафика. |
| ПК 3.2. Проводить документирование требований и технических возможностей облачных инфраструктур | Практический опыт: Поддерживать пользователей сети, настраивать аппаратное и программное обеспечение сетевой инфраструктуры. Выполнять профилактические работы на объектах облачной инфраструктуры и рабочих станциях. Составлять  план-график профилактических работ. |
| Умения: Наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных. Устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту. Выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств. Осуществлять диагностику и поиск неисправностей всех компонентов сети. Выполнять действия по  устранению неисправностей. |
| Знания: Задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией. Классификацию регламентов, порядок технических осмотров, проверок и профилактических работ. Расширение структуры  компьютерных сетей, методы и средства диагностики неисправностей технических средств |

|  |  |  |
| --- | --- | --- |
|  |  | и сетевой структуры. Методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных. Основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных. Средства мониторинга и анализа локальных сетей. Основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем. Принципы работы сети аналоговой телефонии. Назначение голосового шлюза, его компоненты и функции. Основные принципы технологии обеспечения QoS для голосового  трафика. |
| ПК 3.3. Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки | Практический опыт: Поддерживать пользователей сети, настраивать аппаратное и программное обеспечение сетевой инфраструктуры. Обеспечивать защиту сетевых устройств. Внедрять механизмы сетевой безопасности на втором уровне модели OSI. Внедрять механизмы сетевой безопасности с помощью межсетевых экранов. Внедрять технологии VPN. Настраивать IP-телефоны. Эксплуатировать технические средства сетевой инфраструктуры. Использовать схемы послеаварийного восстановления  работоспособности сети. |
| Умения: Описывать концепции сетевой безопасности. Описывать современные технологии и архитектуры безопасности. Описывать характеристики и элементы  конфигурации этапов VoIP звонка. |
| Знания: Задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией. Правила эксплуатации технических средств сетевой инфраструктуры. Основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных. Средства мониторинга и анализа локальных сетей. Основные требования к средствам и видам тестирования для определения  технологической безопасности информационных |

|  |  |  |
| --- | --- | --- |
|  |  | систем. Принципы работы сети традиционной телефонии. Назначение голосового шлюза, его компоненты и функции. Основные принципы технологии обеспечения QoS для голосового  трафика. |
| ПК 3.4. Производить хранение и анализ данных | Практический опыт: Организовывать бесперебойную работу системы по резервному копированию и восстановлению информации. Обслуживать сетевую инфраструктуру, восстанавливать работоспособность сети после сбоя. Осуществлять удаленное администрирование и восстановление работоспособности сетевой инфраструктуры. Поддерживать пользователей сети, настраивать аппаратное и программное обеспечение сетевой инфраструктуры. Обеспечивать защиту сетевых устройств. Внедрять механизмы сетевой безопасности на втором уровне модели OSI. Внедрять механизмы сетевой безопасности с  помощью межсетевых экранов. |
| Умения: Наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных. Устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту. Выполнять  действия по устранению неисправностей. |
| Знания: Задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией. Классификацию регламентов, порядок технических осмотров, проверок и профилактических работ. Расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры. Методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных. Основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных. Основные требования к средствам и видам тестирования для определения технологической безопасности информационных  систем. |
|  | ПК 3.5. Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов | Практический опыт: Проводить инвентаризацию технических средств сетевой инфраструктуры. Проводить контроль качества выполнения  ремонта. Проводить мониторинг работы |

|  |  |  |
| --- | --- | --- |
|  |  | оборудования после ремонта |
| Умения: Правильно оформлять техническую документацию. Осуществлять диагностику и поиск неисправностей всех компонентов сети. Выполнять действия по устранению неисправностей |
| Знания: Задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией. Классификацию регламентов, порядок технических осмотров, проверок и профилактических работ. Правила эксплуатации технических средств сетевой инфраструктуры. Расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры. Методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных. Основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз  данных. |

* 1. **К оценочным средствам текущего контроля** успеваемости относятся:
     + контрольные вопросы к темам практических занятий.
  2. **К оценочным средствам для промежуточной аттестации** относятся:
     + тестовые задания открытого и закрытого типа;
     + билеты для экзамена.
  3. **Критерии оценки результатов освоения дисциплины Критерии оценивания теоретических знаний:**

*«Отлично»* - ставится, если обучающийся:

а) точно формулирует ответы на поставленные в задании вопросы;

б) дает правильные формулировки понятий и терминов по изученной дисциплине;

в) демонстрирует понимание материала, что выражается в умении обосновать свой ответ;

г) свободно обобщает и дифференцирует признаки и понятия; д) правильно отвечает на дополнительные вопросы;

е) свободно владеет речью (демонстрирует связанность и последовательность в изложении) и т.п.

*«Хорошо»* - ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для отметки «отлично», но допускает единичные ошибки, которые сам же исправляет после замечания преподавателя.

*«Удовлетворительно»* - ставится, если обучающийся демонстрирует знание и понимание основных положений данной темы, но:

а) неточно и неуверенно воспроизводит ответы на поставленные в задании вопросы;

б) дает неточные формулировки понятий и терминов; в) затрудняется обосновать свой ответ;

г) затрудняется обобщить или дифференцировать признаки и понятия; д) затрудняется при ответах на дополнительные вопросы;

е) излагает материал недостаточно связанно и последовательно с частыми заминками и перерывами и т.п.

*«Неудовлетворительно»* - ставится, если обучающийся демонстрирует незнание или непонимание большей части соответствующего раздела.

**Критерии оценивания практических умений:**

*«Отлично»* ставится, если обучающийся:

а) умеет подтвердить на примерах свое умение по выполнению полученного практического задания;

б) умеет аргументировать свои действия при выполнении практического задания;

в) целесообразно использует теоретический материал для выполнения задания;

г) правильно использует необходимые приемы, методы, инструменты и другие ресурсы;

д) демонстрирует умение действовать в стандартных и нестандартных профессиональных ситуациях;

е) грамотное составление документов, относящихся к профессиональной деятельности и т.п.

*«Хорошо» -* ставится, если обучающийся демонстрирует практические умения, удовлетворяющие тем же требованиям, что и для отметки «отлично», но допускает единичные негрубые ошибки, которые сам же исправляет после замечания преподавателя.

*«Удовлетворительно»* - ставится, если обучающийся обнаруживает практические умения, но:

а) затрудняется привести примеры, подтверждающие его умения, использованные в процессе выполнения практического задания;

б) непоследовательно аргументирует свои действия, предпринятые им в процессе выполнения практического задания; аргументы, объясняющие его действия, предпринятые им в процессе выполнения практического задания;

в) нецелесообразно использует теоретический материал для составления плана выполнения практического задания;

г) излагает материал недостаточно связано и с последовательно с частыми заминками и перерывами;

д) испытывает затруднения в действиях при нестандартных профессиональных ситуациях и т.п.

*«Неудовлетворительно» -* ставится, если обучающийся допускает грубые нарушения алгоритма действия или ошибки, влекущие за собой возникновение отрицательных последствий для оборудования, окружающей среды и экипажа судна, или (и) отсутствие умения действовать в стандартных профессиональных ситуациях, или(и) демонстрирует незнание или непонимание большей части соответствующего раздела.

**Критерии оценивания по дисциплине в форме тестирования**:

«Отлично» - 81-100 % правильных ответов;

«Хорошо» - 61-80 % правильных ответов;

«Удовлетворительно» - 41-60% правильных ответов;

«Неудовлетворительно» - 0-40% правильных ответов.

1. **Оценочные средства текущего контроля и промежуточной аттестации Контрольные вопросы к практическим занятиям**

**Практическая работа 1-3. Протокол управления SNMP. Основные**

**характеристики протокола SNMP. Набор услуг (PDU) протокола SNMP**

Контрольные вопросы:

1. Протокол управления SNMP.
2. Основные характеристики протокола SNMP.
3. Набор услуг (PDU) протокола SNMP

**Практическая работа 4-6. Задачи управления: анализ производительности сети. Задачи управления: анализ надежности сети. Управление безопасностью в сети.**

Контрольные вопросы:

1. Задачи управления: анализ производительности сети.
2. Задачи управления: анализ надежности сети.
3. Управление безопасностью в сети.

**Практическая работа 7-9. Учет трафика в сети. Средства мониторинга компьютерных сетей. Средства анализа сети с помощью команд сетевой операционной системы**

Контрольные вопросы:

1. Учет трафика в сети.
2. Средства мониторинга компьютерных сетей.
3. Средства анализа сети с помощью команд сетевой операционной системы

**Практическая работа 10-12. Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры. Настройка аппаратных IP- телефонов. Настройка программных IP-телефонов, факсов**

Контрольные вопросы:

1. Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры.
2. Настройка аппаратных IP-телефонов.
3. Настройка программных IP-телефонов, факсов

**Практическая работа 13-14. Развертывание сети с использованием VLAN для IP- телефонии. Настройка шлюза. Установка, подключение и первоначальные настройки голосового маршрутизатора**

Контрольные вопросы:

1. Развертывание сети с использованием VLAN для IP-телефонии.
2. Настройка шлюза.
3. Установка, подключение и первоначальные настройки голосового маршрутизатора

**Практическая работа 15-17. Настройка таблицы пользователей в голосовом маршрутизаторе. Настройка групп в голосовом маршрутизаторе. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе**

Контрольные вопросы:

1. Настройка таблицы пользователей в голосовом маршрутизаторе.
2. Настройка групп в голосовом маршрутизаторе.
3. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе

**Практическая работа 18-19. Настройка голосовых сообщений в маршрутизаторе. Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk)**

Контрольные вопросы:

1. Настройка голосовых сообщений в маршрутизаторе.
2. Настройка программно-аппаратной IP-АТС.
3. Установка и настройка программной IP-АТС (например, Asterisk)

**Практическая работа 20-22. Тестирование кодеков. Исследование параметров качества обслуживания. Мониторинг и анализ соединений по различным протоколам. Мониторинг вызовов в программном коммутаторе**

Контрольные вопросы:

1. Тестирование кодеков.
2. Исследование параметров качества обслуживания.
3. Мониторинг и анализ соединений по различным протоколам.
4. Мониторинг вызовов в программном коммутаторе

**Практическая работа 23-25. Создание резервных копий баз данных. Диагностика и устранение неисправностей в системах IP-телефонии. Финальная комплексная практическая работа по эксплуатации систем IP-телефонии. Практические примеры применения стандартов в сопровождении ИС. Формирование отчётной документации по результатам выполнения работ.**

Контрольные вопросы:

1. Создание резервных копий баз данных.
2. Диагностика и устранение неисправностей в системах IP-телефонии.
3. Финальная комплексная практическая работа по эксплуатации систем IP-

телефонии.

1. Практические примеры применения стандартов в сопровождении ИС.
2. Формирование отчётной документации по результатам выполнения работ.

**Практическая работа 26-27. Выполнение регламентных работ по обновлению и техническому сопровождению ИС. Модификация и сопровождение ПО кода программного обеспечения.**

Контрольные вопросы:

1. Выполнение регламентных работ по обновлению и техническому сопровождению ИС.
2. Модификация и сопровождение ПО кода программного обеспечения.

**Практическая работа 28-29. Настройка ИС под конкретного пользователя согласно технической документации. Установка серверной части. Управляющие серверы (сетевые операционные системы), файловые серверы.**

Контрольные вопросы:

1. Настройка ИС под конкретного пользователя согласно технической документации.
2. Установка серверной части.
3. Управляющие серверы (сетевые операционные системы), файловые серверы.

**МДК 03.02 Безопасность компьютерных сетей**

**Практическая работа 1-2. Безопасность Сетевых устройств OSI. Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.**

Контрольные вопросы:

1. Безопасность Сетевых устройств OSI.
2. Безопасный доступ к устройствам.
3. Назначение административных ролей.
4. Мониторинг и управление устройствами.
5. Использование функция автоматизированной настройки безопасности.

**Практическая работа 3-4. Авторизация, аутентификация и учет доступа (ААА) Свойства ААА. Локальная ААА аутентификация. Server-based ААА** Контрольные вопросы:

1. Авторизация, аутентификация и учет доступа (ААА)
2. Свойства ААА.
3. Локальная ААА аутентификация.
4. Server-based ААА

**Практическая работа 5-6. Реализация технологий брандмауэра. ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах. IPS технологии.**

Контрольные вопросы:

1. Реализация технологий брандмауэра.
2. ACL.
3. Технология брандмауэра.
4. Контекстный контроль доступа (CBAC).
5. Политики брандмауэра, основанные на зонах.
6. IPS технологии.

**Практическая работа 7-9. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS. Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2).**

Контрольные вопросы:

1. IPS сигнатуры.
2. Реализация IPS.
3. Проверка и мониторинг IPS.
4. Безопасность локальной сети.
5. Обеспечение безопасности пользовательских компьютеров.
6. Соображения по безопасности второго уровня (Layer-2).

**Практическая работа 10-11. Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN. Социальная инженерия. Настройка политики безопасности брандмауэров. Настройка системы предотвращения вторжений (IPS). Настройка безопасности на втором уровне на коммутаторах. Исследование методов шифрования**

Контрольные вопросы:

1. Конфигурация безопасности второго уровня.
2. Безопасность беспроводных сетей, VoIP и SAN.
3. Социальная инженерия.
4. Настройка политики безопасности брандмауэров.
5. Настройка системы предотвращения вторжений (IPS).
6. Настройка безопасности на втором уровне на коммутаторах.
7. Исследование методов шифрования

**Практическая работа 12-13. Исследование методов шифрования. Конфиденциальность. Криптография открытых ключей.**

Контрольные вопросы:

1. Исследование методов шифрования.
2. Конфиденциальность.
3. Криптография открытых ключей.

**Практическая работа 14-15. Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность.**

**Тестирование сети на уязвимости. Непрерывность бизнеса**

Контрольные вопросы:

1. Принципы безопасности сетевого дизайна.
2. Безопасная архитектура.
3. Управление процессами и безопасность.
4. Тестирование сети на уязвимости.
5. Непрерывность бизнеса

**Практическая работа 16-17. Планирование восстановления аварийных ситуаций. Разработка регламентов компании и политик безопасности. Cisco ASA** Контрольные вопросы:

1. Планирование восстановления аварийных ситуаций.
2. Разработка регламентов компании и политик безопасности.
3. Cisco ASA

**Практическая работа 18-20. Планирование, создание и изменение учетных записей пользователей. Создание и администрирование групп пользователей. Планирование и установка разрешений NTFS для файлов. Настройка политики безопасности учетных записей.**

Контрольные вопросы:

1. Планирование, создание и изменение учетных записей пользователей.
2. Создание и администрирование групп пользователей.
3. Планирование и установка разрешений NTFS для файлов.
4. Настройка политики безопасности учетных записей.

**Задания открытого типа**

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ:

|  |  |
| --- | --- |
| ПК 3.1. | Осуществлять развертывание облачной инфраструктуры |
| ПК 3.2. | Проводить документирование требований и технических возможностей облачных инфраструктур |
| ПК 3.3. | Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки |
| ПК 3.4. | Производить хранение и анализ данных |
| ПК 3.5. | Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов |
| ПК 3.6. | Проводить мониторинг системы в облачных сервисах |

1. Вопрос: Какие основные функции выполняет протокол динамической конфигурации хоста (DHCP) в процессе настройки сетевого соединения?

Ответ: Основными функциями протокола DHCP являются:

* + Автоматическое назначение IP-адресов узлам сети. Протокол DHCP позволяет автоматически назначать IP-адреса сетевым устройствам, что упрощает настройку сетевых соединений и избавляет от необходимости ручной настройки каждого узла.
  + Обеспечение временной аренды IP-адресов. Протокол DHCP также предоставляет возможность временной аренды IP-адресов, что позволяет динамически изменять IP-адреса устройств без необходимости их перенастройки.
  + Поддержка нескольких классов адресов. DHCP может работать с различными классами IP-адресов (например, локальными и глобальными), предоставляя возможность гибкой настройки сетевых соединений.

1. Вопрос: Какие существуют методы контроля доступа к ресурсам сети и какова их роль в обеспечении безопасности сетевых инфраструктур?
2. Ответ: Методы контроля доступа к сетевым ресурсам включают в себя следующие подходы:
3. Идентификация и аутентификация пользователей: процесс подтверждения личности пользователя и его права на доступ к сетевым ресурсам. Этот метод обеспечивает защиту от несанкционированного доступа к конфиденциальной информации.
4. Разграничение доступа: процесс определения прав доступа пользователей к различным ресурсам сети.
5. Это позволяет ограничить доступ пользователей только к тем ресурсам, которые им действительно нужны для выполнения своих задач.
6. Шифрование данных: процесс преобразования данных в зашифрованный вид, который может быть расшифрован только авторизованными пользователями. Этот метод предотвращает чтение конфиденциальных данных неавторизованными лицами.
7. Использование межсетевых экранов (firewall) и систем обнаружения вторжений (IDS): эти системы обеспечивают защиту сети от внешних угроз, таких как хакерские атаки и вирусы.
8. Отслеживание и мониторинг активности пользователей: этот метод позволяет выявить подозрительную активность пользователей и предотвратить

возможные угрозы безопасности.

1. Все эти методы контроля доступа играют важную роль в обеспечении безопасности сетевой инфраструктуры, поскольку они позволяют

предотвратить несанкционированный доступ к конфиденциальной информации и защитить сеть от внешних и внутренних угроз.

1. Какой основной функцией обладает протокол DHCP при настройке сетевого соединения?

Ответ. Протокол DHCP обладает основной функцией автоматического назначения IP-адресов сетевым устройствам.

1. Какие существуют методы контроля доступа к ресурсам сети и какую роль они играют в обеспечении безопасности сетевых инфраструктур?

Ответ. Существуют такие методы контроля доступа как идентификация и аутентификация пользователей, разграничение доступа, шифрование данных,

использование межсетевых экранов и систем обнаружения вторжений, а также отслеживание и мониторинг активности пользователей. Все эти методы играют важную роль в обеспечении безопасности сети.

1. Какие основные функции выполняет протокол DHCP? (Автоматическое назначение IP-адресов узлам сети, Обеспечение временной аренды IP- адресов, Поддержка нескольких классов адресов.)
2. Что такое “разграничение доступа”? (Процесс определения прав доступа пользователей к различным ресурсам.)
3. Для чего используется шифрование данных? (Для предотвращения чтения конфиденциальных данных.)
4. Какую роль играют межсетевые экраны в сетевой инфраструктуре? (Защищают сеть от внешних угроз.)
5. С какой целью проводится отслеживание и мониторинг пользовательской активности? (Выявление подозрительной активности.)
6. Что подразумевается под “безопасностью сетевых инфраструктур”? (Защита от несанкционированного доступа, защита от внешних и внутренних угроз.)
7. В чем заключается работа специалиста по эксплуатации объектов сетевой инфраструктуры? (Настройка и обслуживание сетевого оборудования, обеспечение доступа к ресурсам, поддержка пользователей.)
8. Какие виды сетевого оборудования вы знаете? (Коммутаторы, маршрутизаторы, модемы, точки доступа, сетевые адаптеры, медиаконвертеры.)
9. Как осуществляется настройка сетевого оборудования?

22.(Через специализированное программное обеспечение или веб-интерфейс.)

1. Что входит в процесс обслуживания сетевого оборудования? (Мониторинг состояния, обновление прошивки, замена вышедших из строя компонентов.)
2. Какими навыками должен обладать специалист по сетевой инфраструктуре? (Знание сетевых технологий, навыки работы с оборудованием, знание основ безопасности сетей.)
3. Какие технологии беспроводных сетей вы знаете? (Wi-Fi, Bluetooth, ZigBee, LTE, 5G.)
4. Какие функции выполняет сервер в сетевой инфраструктуре? (Хранение и обработка данных, предоставление доступа к ресурсам.)
5. Что включает в себя работа с кабельными системами? (Прокладка кабеля, коммутация, диагностика неисправностей.)
6. Какие способы аутентификации пользователей вы знаете? (Пароль, биометрия, двухфакторная аутентификация.)
7. Какие виды атак на сетевые инфраструктуры вы знаете? (DoS-атаки, DDoS- атаки, SQL-инъекции, фишинговые атаки.)
8. Каким образом можно предотвратить сетевые атаки? (Использование антивирусного ПО, применение межсетевых экранов, обучение пользователей.)
9. Что значит “сбалансировать нагрузку на сетевое оборудование”? (Равномерное распределение трафика между устройствами.)

**Тестовые задания закрытого типа:**

* 1. Какой тип оптоволоконного кабеля требуется в соответствии со стандартом EIA/TIA-568B для горизонтальной кабельной системы?

а) 100-омный кабель с двумя витыми парами;

**б) двухволоконный многомодовый кабель 62.5/125 мкм; \***

в) 150-омный кабель с двумя витыми парами;

г) четырехволоконный многомодовый кабель 62.5/125 мкм.

* 1. Оборудование СКС чаще всего размещают:

а) за подвесным потолком в специальных конструкциях;

**б) в телекоммуникационных шкафах и стойках;\***

в) в кабельных слаботочных стояках;

д) на чердаке или подвале здания за специальной перегородкой.

* 1. Какие номера портов используются протоколом SNMP?

**а) 161,162; \***

б) 20,21;

в) 53,54;

г) 441,443.

* 1. Как следует перехватить поток трафика, чтобы наилучшим образом понять модель трафика в сети?

а) в периоды низкого уровня загруженности;

**б) в периоды максимальной загруженности;\***

в) только когда он проходит основной сегмент сети; г) когда трафик формируют пользователи.

* 1. Укажите небезопасный протокол прикладного уровня. а) HTTPS;

**б) Telnet;\***

в) ICMP; г) SSH.

* 1. К какому нарушению приводит модификация передаваемых данных? а) к нарушению конфиденциальности;

**б) к нарушению целостности; \***

в) к нарушению доступности; г) к нарушению аутентичности.

* 1. Укажите тип криптографического преобразования, наиболее широко используемого для проверки целостности передаваемых данных протоколами виртуальных частных сетей.

**а) ключевая хэш-функция;\***

б) бесключевая хэш-функция; в) симметричное шифрование; г) ассиметричное шифрование.

* 1. Алгоритм ГОСТ Р 34.12-2015 является:

а) алгоритмом вычисления функции хеширования;

б) блочным алгоритмом асимметричного шифрования;

**в) блочным алгоритмом симметричного шифрования; \***

г) алгоритмом формирования электронной подписи.

* 1. Укажите правильный порядок размещения правил межсетевого экранирования при реализации политики доступа к сетевым ресурсам?

а) от общих правил к частным правилам;

**б) от частных правил к общим правилам; \***

в) не имеет значения, правила размещаются в произвольном порядке.

* 1. Какой способ считается наиболее эффективным для минимизации последствий атакивируса-червя?

а) регулярная смена системных паролей;

б) настройка в сети сервиса аутентификации, авторизации и учета;

в) загрузка обновлений системы безопасности операционной системы и исправление всех уязвимых систем; \*

г) шифрование данных.

**Образец билетов для экзамена**

|  |  |
| --- | --- |
| ГБПОУ РК «Чапаевский агротехнологический техникум имени И.Н. Шатилова»  **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №\_**1\_  ПМ 03. Эксплуатация объектов сетевой инфраструктуры | |
| (наименование дисциплины или дисциплин - при проведении комплексного экзамена) | |
| 1. Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы 2. Объясните алгоритм настройки VPN | |
| 3. Опишите процесс настройки маршрутизато | ора |
| Преподаватель |  |
| подпись | Инициалы, фамилия |
| Председатель ЦК |  |
| подпись | Инициалы, фамилия |

|  |  |
| --- | --- |
| ГБПОУ РК «Чапаевский агротехнологический техникум имени И.Н. Шатилова»  **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №\_**2\_  ПМ 03. Эксплуатация объектов сетевой инфраструктуры | |
| (наименование дисциплины или дисциплин - при проведении комплексного экзамена) | |
| 1. Опишите процесс настройки беспроводной | сети. |
| 2. Перечислите типы резервного копирования |  |
| 3 Классифицируйте угрозы ИБ по составу и последствиям | |
| Преподаватель |  |
| подпись | Инициалы, фамилия |
| Председатель ЦК |  |
| подпись | Инициалы, фамилия |