

Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное профессиональное
образовательное учреждение
«Белгородский индустриальный колледж»

**КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

в рамках основной профессиональной образовательной программы (ОПОП)
по специальности СПО
09.02.06 Сетевое и системное администрирование

2019 г.

Комплект контрольно-оценочных средств по профессиональному модулю разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее - СПО) по специальности **09.02.06 Сетевое и системное администрирование**.

Рассмотрено
цикловой комиссией
«Информатики и ПОВТ»
Протокол заседания № 1
От «30» августа 2019 г.
Председатель цикловой комиссии
_____/ Третьяк И.Ю./

Утверждаю
Зам. директора по УР
_____/ Н.В. Выручаева
«30» августа 2019 г.

Рассмотрено
цикловой комиссией
«Информатики и ПОВТ»
Протокол заседания №
От « » августа 2020 г.
Председатель цикловой комиссии
_____/ _____/

Рассмотрено
цикловой комиссией
«Информатики и ПОВТ»
Протокол заседания №
От « » августа 2021 г.
Председатель цикловой комиссии
_____/ _____/

Рассмотрено
цикловой комиссией
«Информатики и ПОВТ»
Протокол заседания №
От « » августа 2022 г.
Председатель цикловой комиссии
_____/ _____/

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:

преподаватель ОГАПОУ «Белгородский индустриальный колледж»
Герасимова С.А.

Экспертиза:

(внутренний рецензент) ОГАПОУ «Белгородский индустриальный колледж»,
преподаватель Ченская И.Б.

(внешний рецензент) ООО «Фортуна», генеральный директор Мочалов В.И.

Содержание

	стр.
Общие положения	4
1. Результаты освоения модуля, подлежащие проверке	4
2. Формы контроля и оценивания элементов профессионального модуля	10
3. Оценка освоения теоретического курса профессионального модуля	10
4. Оценка по учебной практике	16
5. Оценка по производственной практике (по профилю специальности)	17
6. Контрольно-оценочные материалы для экзамена (квалификационного)	19
7. Приложения	55

Общие положения

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности эксплуатация объектов сетевой инфраструктуры и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ОПОП в целом.

Формой аттестации по профессиональному модулю является экзамен (квалификационный), проводимый в виде защиты портфолио обучающегося. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

1. Результаты освоения модуля, подлежащие проверке

1.1. Профессиональные и общие компетенции

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Профессиональные компетенции		Показатели оценки результата
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	- установка, настройка и обслуживание составляющих компьютерных сетей
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.	- составление и соблюдение графика профилактических работ на объектах компьютерных сетей
ПК 3.3.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.	- грамотность и точность работы с конфигурациями объектов
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.	- планирование и реализация работ по восстановлению работоспособности компьютерной сети - установка, настройка и тестирование ПО для резервирования и восстановления информации
ПК 3.5.	Организовывать	- установка, настройка и

	инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.	тестирование ПО для проведения инвентаризации технических средств
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	- диагностика неисправности периферийного оборудования - определение устаревшего оборудования и ПО

Общие компетенции		Показатели оценки результата
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	<ul style="list-style-type: none"> - Распознавать сложные проблемы в знакомых ситуациях. - Выделять сложные составные части проблемы и описывать её причины и ресурсы, необходимые для её решения в целом. - Определять потребность в информации и предпринимать усилия для её поиска. - Выделять главные и альтернативные источники нужных ресурсов. - Разрабатывать детальный план действий и придерживаться его. - Качество результата, в целом, соответствует требованиям. - Оценивать результат своей работы, выделять в нём сильные и слабые стороны.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	<p>Планировать информационный поиск из широкого набора источников, необходимого для выполнения профессиональных задач</p> <p>Проводить анализ полученной информации, выделять в ней главные аспекты</p>

		Структурировать отобранную информацию в соответствии с параметрами поиска Интерпретировать полученную информацию в контексте профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.	- Использовать актуальную нормативно-правовую документацию по профессии (специальности) - Применять современную научно профессиональную терминологию - Определять траекторию профессионального развития и самообразования
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- Участвовать в деловом общении для эффективного решения деловых задач - Планировать профессиональную деятельность
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- Грамотно устно и письменно излагать свои мысли по профессиональной тематике на государственном языке - Проявлять толерантность в рабочем коллективе
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	- Понимать значимость своей профессии (специальности) - Демонстрировать поведение на основе общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- Соблюдать правила экологической безопасности при ведении профессиональной деятельности; - Обеспечивать ресурсосбережение на рабочем месте.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- Сохранять и укреплять здоровье посредством использования средств физической культуры - Поддерживать уровень физической подготовленности для успешной реализации профессиональной деятельности
ОК 9.	Использовать информационные технологии в профессиональной	- Применять средства информатизации и информационных

	деятельности	технологий для реализации профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.	- Применять в профессиональной деятельности инструкции на государственном и иностранном языке. - Вести общение на профессиональные темы
ОК 11.	Планировать предпринимательскую деятельность в профессиональной сфере	- Определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности - Составлять бизнес-план - Презентовать бизнес-идею - Определять источники финансирования - Применять грамотные кредитные продукты

1.2. «Иметь практический опыт – уметь – знать»

В результате изучения профессионального модуля обучающийся должен:

иметь практический опыт:

- 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.
- Внедрять технологии VPN.
- Настраивать IP-телефоны
- Поддерживать пользователей сети, настраивать аппаратное и программное обеспечение сетевой инфраструктуры.
- Выполнять профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
- Составлять план-график профилактических работ
- 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.
- 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
- Проводить инвентаризацию технических средств сетевой инфраструктуры.
- Проводить контроль качества выполнения ремонта.
- Проводить мониторинг работы оборудования после ремонта.
- Устранять неисправности в соответствии с полномочиями техника.
- Заменять расходные материалы.
- Мониторинг обновлений программно-аппаратных средств сетевой инфраструктуры;

уметь:

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети;
- эксплуатировать технические средства сетевой инфраструктуры;
- осуществлять диагностику и поиск неисправностей технических средств;
- выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
- тестировать кабели и коммуникационные устройства;

- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- правильно оформлять техническую документацию;
- наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;
- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.

Знать:

- архитектуру и функции систем управления сетями, стандарты систем управления;
- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
- средства мониторинга и анализа локальных сетей;
- 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 ИС, 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.

2. Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	Форма контроля и оценивания	
	Промежуточная аттестация	Текущий контроль
МДК.03.01. Эксплуатация объектов сетевой инфраструктуры	Экзамен	Тестирование. Оценка результатов выполнения лабораторных работ.
МДК.03.02. Безопасность компьютерных сетей	Дифференцированный зачет	Оценка результатов выполнения лабораторных работ.
Учебная практика УП.03	Дифференцированный зачет	Оценка выполнения работ на учебной практике. Защита отчетов по учебной практике.
Производственная практика (по профилю специальности) ПП.03	Дифференцированный зачет	Оценка выполнения работ на производственной практике (по профилю специальности). Защита отчетов по практике.
ПМ.03	Экзамен (квалификационный)	

3. Оценка освоения теоретического курса профессионального модуля

3.1. Задания для оценки освоения МДК.03.01. Эксплуатация объектов сетевой инфраструктуры и МДК.03.02 Безопасность компьютерных сетей

1. Настройте сетевой интерфейс для введения компьютера в domain.
2. Настройте сетевую карту, имя компьютера, рабочую группу по заданным параметрам
3. Продемонстрируйте устранение неполадок с помощью PathPing
4. Продемонстрируйте устранение неполадок с помощью Ping
5. Продемонстрируйте устранение неполадок с использованием Network Diagnostics Framework
6. Выполните трассировку сети средствами утилиты Netsh
7. Сохраните кадры в текстовый файл.
8. Запишите данные средствами сетевого монитора
9. Выполните установку сетевого монитора

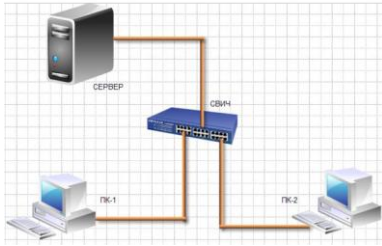
10. Используя оснастку Event Viewer, продемонстрируйте возможности работы с системными журналами.
11. Выполнить сканирование локальной сети с программой LanSurfer по заданным параметрам
12. Создайте профиль для сканирования Моё сканирование
13. Укажите диапазон адресов от 192.168.3.1 до 192.168.3.254
14. Просканируйте сеть
15. Используя возможности программы найдите файл MyTestXSetup.exe
16. Перейдите в папку содержащий данный файл.
17. Построить диаграмму сети с использованием программы EDraw Network Diagrammer



18. Построить диаграмму сети с использованием программы EDraw Network Diagrammer



19. Построить диаграмму сети с использованием программы EDraw Network Diagrammer



20. Построить схему сети с использованием программы 10-Strike LANState
21. Выполнить установку CommView Remote Agent и продемонстрировать возможности наблюдения трафика сети.
22. Выполнить настройку DNS Форвардера в WinRoute
23. Выполнить настройку DHCP-сервера в WinRoute
24. Выполнить базовую настройку политики трафика в WinRoute
25. Выполнить установку WinRoute
26. Создать группы BUN1 и BUN2 и распределить пользователей USER1 и USER12 по группам в domain соответственно.
27. Создать группы BUN1 и BUN2 средствами командной строки
28. Создать группы BUN1 и BUN2 в domain при помощи оснастки «Active Directory– пользователи и компьютеры»
29. Создать пароль для входа пользователю USER1 в domain
30. Создать пользователей средствами командной строки
31. Создать пользователя USER1 в domain на основании шаблонов.
32. Создать пользователя USER1 в domain при помощи оснастки «Active Directory– пользователи и компьютеры»

3.2. Вопросы к экзамену по МДК 03.01 Эксплуатация объектов сетевой инфраструктуры

1. Классификация информационных систем (ИС). Области применения ИС
2. Измерение числа коллизий в сети. Измерение числа ошибок на канальном уровне сети

3. Структурированная кабельная система. Сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.
4. Создание плана восстановления после аварии. Реализация восстановления.
5. Протоколы управления сетевым оборудованием. Протоколы SNMP, CMIP, TMN.
6. Основные сведения об инфраструктуре сети.
7. Измерение числа коллизий в сети. Измерение числа ошибок на канальном уровне сети
8. Протокол динамического конфигурирования сетевых параметров DHCP.
9. Основные сведения об инфраструктуре сети.
10. Мониторинг и анализ компьютерных сетей.
11. Статическая адресация в компьютерных сетях, протоколы.
12. Особенности сетевых сертификатов.
13. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети
14. Стандарты управления OSI
15. Виртуальные частные сети VPN. Понятие, особенности, настройка.
16. Анализаторы протоколов и сетевые анализаторы
17. Динамическая адресация в компьютерных сетях, протоколы.
18. Обслуживания сетевой инфраструктуры, восстановление работоспособности сети после сбоя
19. Активное и пассивное сетевое оборудование
20. Основные свойства сети. Расширяемость сети. Масштабируемость сети.
21. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети
22. Создание плана восстановления после аварии. Реализация восстановления.
23. Требования, предъявляемые к информационным системам.
24. Кабельные сканеры и тестеры

25. Типовая система технического профилактического обслуживания и ремонта объектов сетевой инфраструктуры.
26. Виды конфликтов при установке оборудования, способы их устранения
27. Этапы аудита. Методики аудита. Технические средства аудита.
28. Техническая и проектная документация
29. Классификация средств мониторинга и анализа сети.
30. Расширяемость и масштабируемость.

3.3 Вопросы к дифференцированному зачету по МДК. 03.02 Безопасность компьютерных сетей.

1. Информационная безопасность. Основные определения
2. Угрозы безопасности ИС, анализ угроз.
3. Уровни информационной безопасности
4. Типы и примеры атак.
5. Анализ защищенности и обнаружения атак
6. Обеспечение безопасности операционных систем
7. Способы защиты информации
8. Сетевая безопасность. Основные понятия
9. Методы обеспечения информационной безопасности
10. Межсетевые экраны. Основные компоненты использование и их особенности.
11. Сертификаты. Назначение, принцип работы, аутентификация. Назначение центра сертификации.
12. Политики безопасности. Локальная и групповая политики безопасности.
13. Групповые политики в Windows Server.
14. Построение систем защиты от угроз нарушения доступности
15. Принципы криптографической защиты информации. Криптографические алгоритмы.
16. Защита на сетевом уровне. Защита на канальном и сеансовом уровне.
17. Резервное копирование, как способ защиты информации.

18. Алгоритмы шифрования DES, AES, ГОСТ 28147-89
19. Симметричные алгоритмы шифрования
20. Асимметричные алгоритмы шифрования
21. Защита персональных данных
22. Аппаратно-программные средства защиты
23. Аудит сетевой инфраструктуры. Общие сведения об аудите, этапы аудита.
24. Этапы процесса управления рисками.
25. Объекты ActiveDirectory и политика безопасности применяемая к объектам ActiveDirectory
26. Формальные модели управления доступом, целостности.
27. Вирусы, их виды и защита от вирусов.
28. Программное обеспечение средств защиты информации
29. Технология аутентификации
30. Защита от несанкционированного доступа к информации

3.4 Примерная тематика курсовых работ (проектов) по МДК03.01.

Эксплуатация объектов сетевой инфраструктуры

1. Защита информационных процессов в компьютерных системах.
2. Выработка и реализация сетевой политики, настройка телекоммуникационного оборудования локальной вычислительной сети образовательного учреждения.
3. Выработка и реализация сетевой политики, настройка телекоммуникационного оборудования локальной вычислительной сети туристической компании.
4. Выработка и реализация сетевой политики, настройка телекоммуникационного оборудования локальной вычислительной сети страховой компании.

5. Выработка и реализация сетевой политики, настройка телекоммуникационного оборудования локальной вычислительной сети строительной компании
6. Выработка и реализация сетевой политики, настройка телекоммуникационного оборудования локальной вычислительной сети рекламной компании.
7. Обеспечение безопасности КС аптечной сети
8. Обеспечение безопасности структурированной КС учебного заведения
9. Обеспечение безопасности КС газовой компании
10. Обеспечение безопасности КС строительной компании
11. Обеспечение безопасности КС филиала нефтяной компании
12. Обеспечение безопасности КС бухгалтерии предприятия
13. Обеспечение безопасности КС торгового центра
14. Обеспечение безопасности КС транспортной компании
15. Обеспечение безопасности КС проектно-монтажной организации

4. Оценка по учебной практике

Дифференцированный зачет по учебной практике выставляется на основании данных аттестационного листа профессиональной деятельности студента на практике с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с требованиями.

Виды работ

- Настройка прав доступа.
- Оформление технической документации, правила оформления документов.
- Настройка аппаратного и программного обеспечения сети.

- Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.
- Программная диагностика неисправностей.
- Аппаратная диагностика неисправностей.
- Поиск неисправностей технических средств.
- Выполнение действий по устранению неисправностей.
- Использование активного, пассивного оборудования сети.
- Устранение паразитирующей нагрузки в сети.
- Построение физической карты локальной сети.

5. Оценка по производственной практике (по профилю специальности)

Дифференцированный зачет по производственной практике (по профилю специальности) выставляется на основании данных аттестационного листа профессиональной деятельности студента на практике с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с требованиями.

Виды работ

- Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.
- Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.
- Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.
- Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.

- Установка прав доступа и контроль использования сетевых ресурсов.
- Обеспечение своевременного копирования, архивирования и резервирования данных.
- Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.
- Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению.
- Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети.
- Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.
- Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.
- Документирование всех произведенных действий.

6. Контрольно-оценочные материалы для экзамена (квалификационного)

6.1 Задание для экзаменуемого

Инструкция

1. Получите индивидуальные задания.
2. Внимательно прочитайте задание.
3. Выполните задание.
4. Представьте в экспертную комиссию выполненные задания.

При выполнении задания вы можете воспользоваться учебно-методической литературой, Интернет-ресурсами, нормативно-правовыми документами согласно перечню:

Печатные издания

1. Назаров А.В., Мельников В.П., Куприянов А.И. Эксплуатация объектов сетевой инфраструктуры ОИЦ «Академия». 2014.

Электронные издания (электронные ресурсы, интернет-ресурсы)

1. Васин, Н. Н. Обеспечение безопасности сетей на маршрутизаторах и коммутаторах : методические указания по проведению лабораторных работ / Н. Н. Васин. — Самара : Поволжский государственный университет телекоммуникаций и информатики, 2014. — 24 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/71860.html>
2. Ложников, П. С. Обеспечение безопасности сетевой инфраструктуры на основе операционных систем Microsoft : практикум / П. С. Ложников, Е. М. Михайлов. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузское образование, 2017. — 264 с. — ISBN 978-5-4487-0080-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/67389.html>
3. Основы построения сетей пакетной коммутации / Васин Н. <http://www.intuit.ru/studies/courses/3645/887/info>
4. Сысоев, Э. В. Администрирование компьютерных сетей : учебное пособие / Э. В. Сысоев, А. В. Терехов, Е. В. Бурцева. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 79 с. — ISBN 978-5-8265-1802-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/85916.html>
5. www.elibrary.ru — научная электронная библиотека (НЭБ).

Дополнительные источники

1. Бубнов А.А. Основы информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2017. – 256 с.
2. Костров Б.В. Сети и системы передачи информации: учебник для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2019. – 288 с.

Вариант 1

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите функции маршрутизатора.
2. Дайте определение информационной безопасности в широком смысле.

Часть Б.

1. Опишите процесс настройки DNS сервера.
2. Опишите процесс установки программы Ethereum и подготовки к захвату.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 2

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите виды технических осмотров.
2. Перечислите основные действия по защите информации при эксплуатации вычислительных (компьютерных) систем.

Часть Б.

1. Настройте одноранговую локальную сеть.
2. Опишите пользовательский интерфейс программы Ethereum. Фильтр отображения пакетов. Поиск кадров

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 3

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Раскройте сущность трёх технологий масштабируемости.
2. Перечислите основные этапы изменения уровня безопасности.

Часть Б.

1. Настройте доступ к сетевым принтерам.
2. Опишите пользовательский интерфейс программы Ethereum. Поиск кадров

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 4

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Рассказать о методах технического обслуживания.
2. Классифицируйте угрозы ИБ по составу и последствиям.

Часть Б.

1. Настройте журналирование.
2. Опишите программу Ethereum. Выделение ключевых кадров. Сохранение данных захвата.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 5

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите способы резервирования кабельных систем.
2. Классифицируйте угрозы для ИС.

Часть Б.

1. Опишите процесс создания безопасной зоны Acronis.
2. Настройте программу Ethereal. Произведите печать информации, просмотр кадра в отдельном окне.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 6

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Объясните чем обусловлена надёжность ЛВС?
2. Перечислите источники угроз ИБ.

Часть Б.

1. Опишите процесс настройки DHCP сервера.
2. Проанализируйте протоколы Ethernet и ARP

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 7

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите способы переключения на резерв.
2. Классифицируйте угрозы ИБ по типу реализации.

Часть Б.

1. Опишите процесс настройки брандмауэра.
2. Проанализируйте протокол ICMP.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 8

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите типы резервного копирования.
2. Дайте определение информационной безопасности в узком смысле.

Часть Б.

1. Проанализируйте трафик сети на базе Lan2NET.
2. Проанализируйте протокол IP.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 9

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Опишите как осуществляется управление отказами в сети?
2. Классифицируйте угрозы ИБ по характеру возникновения.

Часть Б.

1. Разделите существующую сеть на подсети.
2. Проанализируйте протокол TCP

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 10

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите каковы цели профилактических проверок ОСИС?
2. Дайте определение безопасности данных.

Часть Б.

1. Настройте удалённый доступ к серверу.
2. Объясните принцип анализа рисков проверки политики информационной безопасности предприятия.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 11

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Дайте определение технического обслуживания.
2. Перечислите основные функции межсетевого экрана.

Часть Б.

1. Распишите алгоритм развёртывания служб Active Directory.
2. Перечислите этапы сетевой атаки. Исследование сетевой топологии.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 12

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. В чём сущность восстановительного метода ТО сетей?
2. Классифицируйте угрозы для ЭИС.

Часть Б.

1. Разрешить порт 1316 в брандмауэре.
2. Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 13

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Объясните в чём сущность восстановительного метода ТО сетей?
2. Перечислите основные подходы к защите сети.

Часть Б.

1. Опишите процесс добавления компьютера в домен.
2. Объясните как осуществляется реализации атак. Выявление атаки на протокол SMB.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 14

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Расскажите о централизованной системе управления сетью.
2. Классифицируйте угрозы ИБ.

Часть Б.

1. Объясните алгоритм настройки VPN.
2. Опишите стандарт криптографической защиты AES (Advanced Encryption Standart).

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 15

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите виды телекоммуникационных сетей.
2. Дайте определение шифрования данных.

Часть Б.

1. Объясните алгоритм настройки прокси сервера.
2. Опишите отечественный стандарт хэш-функции и цифровой подписи.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 16

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите какие виды контроля включает управление ТО?
2. Перечислите угрозы, связанные с преднамеренными ошибками.

Часть Б.

1. Опишите алгоритм действий при тестировании кабельных систем.
2. Перечислите компоненты межсетевое экрана. Пример реализации политики МЭ.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 17

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите какие системы называются открытыми?
2. Дайте определение биометрических систем.

Часть Б.

1. Запретите рабочей станции в доступе к серверу.
2. Объясните применение МЭ на основе двудомного узла.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 18

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Объясните, что такое IP-сеть?
2. Классифицируйте угрозы по месту возникновения, объекту воздействия, причине возникновения.

Часть Б.

1. Настройте ЛВС между тремя компьютерами.
2. Объясните применение МЭ на основе фильтрующего маршрутизатора.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 19

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Расскажите об архитектуре систем управления сетями.
2. Перечислите основные действия по управлению доступом.

Часть Б.

1. Ограничьте внешний трафик пользователю через панель управления Lan2NET.
2. Объясните применение МЭ на основе экранирующего узла.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 20

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Опишите схему взаимодействия Агент-Менеджер.
2. Перечислите последствия несанкционированного манипулирования информацией.

Часть Б.

1. Настройте подключение через ADSL модем.
2. Объясните применение технологии трансляции сетевых адресов. Задачи, решаемые VPN.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 21

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите какую информацию предоставляет администратору сети ЭС?
2. Классифицируйте функции защиты управления доступом.

Часть Б.

1. Опишите процесс настройки прямой зоны DNS сервера.
2. Объясните принцип туннелирования в VPN.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 22

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Объясните в чём состоит задача сбора статистики использования устройств сети?
2. Классифицируйте угрозы ИБ по характеру возникновения.

Часть Б.

1. Опишите процесс настройки обратной зоны DNS сервера.
2. Объясните принцип организации VPN средствами протокола PPTP.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 23

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Классифицируйте средства мониторинга сети?
2. Классифицируйте угрозы для ЭИС.

Часть Б.

1. Опишите процесс настройки маршрутизатора.
2. Объясните принцип организации VPN средствами СЗИ VipNet.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 24

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Дайте определение понятий «диагностика» и «тестирование сети».
2. Перечислите основные подходы к защите сети.

Часть Б.

1. Опишите процесс настройки беспроводной сети.
2. Объясните принцип организации VPN средствами СЗИ StrongNet.

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 25

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Изложите основные принципы локализации неисправностей сети.
2. Дайте определение биометрических систем.

Часть Б.

1. Объясните с помощью командной строки получить подробные сведения обо всех сетевых интерфейсах ПК.
2. Объясните принцип организации VPN средствами протокола SSL в Windows Server

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 26

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Для каких целей проводится входное и нагрузочное тестирование сети?
2. Перечислите последствия несанкционированного манипулирования информацией.

Часть Б.

1. Проверить реальную скорость интернета.
2. Объясните принцип организации сигнатурного анализа и обнаружения аномалий

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 27

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Объясните в чём состоит принцип локализации неисправностей «сверху вниз»?
2. Классифицируйте угрозы ИБ по составу и последствиям.

Часть Б.

1. Объясните алгоритм действий при потере соединения с интернетом.
2. Объясните принцип организации обнаружения аномалий в реальном времени и отложенный анализ

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 28

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Перечислите какие типы нагрузочных тестов вам известны?
2. Перечислите основные этапы изменения уровня безопасности.

Часть Б.

1. Опишите процесс создания резервной копии пользовательского каталога.
2. Объясните принцип организации локальных и сетевых систем обнаружения атак

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 29

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Дайте определение сетевых утилит.
2. Перечислите основные подходы к защите сети.

Часть Б.

1. Опишите процесс настройки доступа к сетевым принтерам.
2. Объясните принцип организации распределенных систем обнаружения атак

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

Вариант 30

Инструкция

1. Внимательно прочитайте задание.
2. Выполните задание части А. Вы можете воспользоваться учебно-методической литературой, имеющейся на специальном столе, Интернет-ресурсами.
3. После выполнения части А выполните задание части Б.

Максимальное время для выполнения заданий – 50 минут

Часть А.

1. Расскажите о функциях сетевых тест-программ.
2. Перечислите угрозы, связанные с преднамеренными ошибками.

Часть Б.

1. Опишите процесс настроить параметры сети IPv4.
2. Объясните принцип организации систем обнаружения атак Snort

КРИТЕРИИ

Обоснование выбора подходов и методов расчетов и анализа в соответствии с требованиями стандартов.

Соответствие проведенных расчетов в представленных заданиях с различными подходами и их последовательности требованиям принятых методик.

Составление и оформление материала задания в соответствии с действующими нормативно-правовыми актами.

Демонстрация последовательности выполнения работы по анализу представленных ситуаций.

Рефлексия выполненных действий, своевременное и точное нахождение ошибок, внесение соответствующих корректив.

Защита выполненных заданий, умение обосновать свои действия, аргументированность и доказательство приводимых аргументов.

6.2. Требования к портфолио

Тип портфолио смешанный.

1. **Титульный лист** (Приложение 1).

2. **Обязательные документы:**

– индивидуальные показатели успеваемости: выписки из экзаменационных ведомостей по МДК.03.01. Эксплуатация объектов сетевой инфраструктуры (Приложение 2);

– аттестационный лист по учебной практике (Приложение 3);

– дневник учебной практики (Приложение 4);

– аттестационный лист по производственной практике (по профилю специальности) (Приложение 5);

– дневник производственной практики (по профилю специальности) (Приложение 6);

– характеристика с производства.

3. **Дополнительные материалы:**

- результаты самостоятельной работы студента по МДК.03.01. Эксплуатация объектов сетевой инфраструктуры: рефераты, доклады, индивидуальные задания (выданные преподавателями);

- сведения об участии студента в олимпиадах и конкурсах профессионального мастерства, конференциях по профилю специальности (копии дипломов, грамот, свидетельств);

- сведения об участии студента в профориентационной работе и представлении колледжа (специальности) в школах города, района;

- документы о поощрении за участие в мероприятиях различного уровня (колледжных, областных, региональных, всероссийских, международных);

- грамоты, дипломы за спортивные и общественные достижения;

- приказы о поощрениях;

- сведения об участии в учебно-полевых сборах (для юношей).

Основные требования к портфолио

1. Требования к оформлению портфолио

Портфолио оформляется студентом в течение всего периода освоения программы профессионального модуля (в том числе в период практики) под руководством преподавателей МДК, руководителей учебной и производственной практик.

Студент имеет право включать в портфолио дополнительные разделы, материалы, элементы оформления (фотоматериалы, презентации и т.п.), отражающие его индивидуальность.

При оформлении портфолио должны соблюдаться следующие требования:

1. регулярность ведения;
2. достоверность представленных сведений;
3. аккуратность и эстетичность оформления;
4. целостность и эстетическая завершенность материалов;
5. наглядность.

Портфолио оформляется на **электронном и бумажном носителях**.

Требования к **электронным носителям**: диски CD в конвертах, на которых указываются:

1. вид документа (портфолио),
2. полное наименование колледжа (ОГАПОУ «Белгородский индустриальный колледж»),
3. специальность (09.02.06 Сетевое и системное администрирование),
4. группа,
5. фамилия, имя и отчество студента.

Требования к **бумажным носителям**:

1. текстовые документы представляются в форматах Word 2007(doc.) или pdf;
2. параметры текстового редактора:
 - поля: верхнее, нижнее – 2 см, левое – 3 см, правое – 1,5 см;

- шрифт TimesNewRoman;
 - размер шрифта – 14,
 - межстрочный интервал – одинарный,
 - выравнивание – по ширине,
 - красная строка – 1,25 см;
3. в текстах не допускается сокращение названий и наименований;
 4. все страницы нумеруются (нумерация начинается с титульного листа, номер на титульном листе не ставится);
 5. портфолио формируется в одной папке-накопителе с файлами.

Требования к анализу портфолио

Анализ портфолио производится экспертной группой после окончания изучения всех элементов профессиональных модулей (МДК.03.01. Эксплуатация объектов сетевой инфраструктуры, МДК.03.02 Безопасность компьютерных сетей, учебной и производственной практик).

Результаты анализа портфолио записываются в бланк и представляются при защите портфолио.

2. Требования к презентации и защите портфолио

Условия выполнения задания (защиты портфолио)

Максимальное время защиты портфолио: 20 минут.

При подготовке материалов портфолио, презентации к защите портфолио студенту предоставляются все необходимые условия: учебно-методические пособия, компьютер, принтер, доступ к источникам информации (ресурсы библиотеки, учебных кабинетов, лабораторий, мастерских, Интернет и т.п.).

При защите портфолио студент может воспользоваться компьютером, мультимедийным проектором, интерактивной доской и другим необходимым оборудованием.

Защита портфолио осуществляется в устной форме с демонстрацией презентации, выполненной в среде PowerPoint. В презентации должны быть продублированы документы портфолио (возможен вариант перечисления достижений, документов, фрагменты работ).

При защите портфолио студент демонстрирует умение предоставлять на основе сбалансированных формализованных показателей структурированную и систематизированную информацию о собственном профессиональном развитии, личных достижениях в образовательной деятельности; отвечает на вопросы членов комиссии по существу представленных документов.

Оценка портфолио

Коды проверяемых компетенций (ОК)	Показатели оценки результата	Оценка
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Характеристика классного руководителя группы. Характеристики и отзывы руководителей практик, работодателей. Грамоты и дипломы участие в мероприятиях колледжа. Документы, подтверждающие дополнительное образование	
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности		
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.		
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.		
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.		
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.		
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.		
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.		
ОК 9. Использовать информационные технологии в профессиональной деятельности		
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.		
ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере		

Областное государственное автономное профессиональное
образовательное учреждение
«Белгородский индустриальный колледж»

ПОРТФОЛИО
результатов учебной деятельности при изучении
профессионального модуля

ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ
ИНФРАСТРУКТУРЫ

в рамках основной профессиональной образовательной программы
по специальности СПО

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Студента группы _____
(Ф.И.О.)

Преподаватели:

МДК 03.01. Эксплуатация объектов
сетевой инфраструктуры

(Ф.И.О.)

МДК 03.02. Безопасность
компьютерных сетей

(Ф.И.О.)

Руководитель учебной практики

(Ф.И.О.)

Руководитель производственной практики
(по профилю специальности)

(Ф.И.О.)

Белгород, 201_

СОДЕРЖАНИЕ

1	Титульный лист	
2	Индивидуальные показатели успеваемости	
3	Бланк анализа портфолио	
4	Аттестационный лист по МДК04.01. Технология выполнения работ по профессии «Оператор станков с программным управлением»	
5	Оценочная ведомость по профессиональному модулю	
6	Дневник производственной практики (по профилю специальности)	
7	Дневник учебной практики	
8	Производственная характеристика	
9	Участие в олимпиадах, конкурсах профессионального мастерства по профилю специальности	
10	Учебно-исследовательская, проектная деятельность студента по профилю специальности	
11	Спортивные и иные достижения студента, свидетельствующие об освоении общих и профессиональных компетенций	
12	Другое	

Оценочная ведомость по профессиональному модулю

ПМ.03 Эксплуатация объектов сетевой инфраструктуры

ФИО _____
 обучающийся на _____ курсе по специальности 09.02.06 Сетевое и системное администрирование

освоил(а) программу Профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры

в объеме _____ часа(ов). С «___» _____ 201 г. по «___» _____ 201__г

Результаты промежуточной аттестации по элементам профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры.

Элемент модуля (код и наименование МДК, код практик)	Формы промежуточной аттестации	Оценка
МДК 03.01. Эксплуатация объектов сетевой инфраструктуры	Экзамен	
МДК 03.02. Безопасность компьютерных сетей	Дифференцированный зачет	
Учебная практика УП03	Дифференцированный зачет	
Производственная практика (по профилю специальности) ПП03	Дифференцированный зачет	
Коды проверяемых компетенций		Оценка (освоил/ не освоил)
ПК 3.1 Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.		
ПК 3.2 Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.		
ПК 3.3 Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.		
ПК 3.4 Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.		
ПК 3.5 Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.		
ПК 3.6 Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и		

программные средства сетевой инфраструктуры.	
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	
ОК 9. Использовать информационные технологии в профессиональной деятельности	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	
ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере	

Вид профессиональной деятельности _____, оценка _____

Дата « » 201 г.

Подписи членов экзаменационной комиссии:

<u>ОГАПОУ «БИК»</u> (место работы)	<u>преподаватель</u> (занимаемая должность)	_____ / _____ (Ф.И.О.)
---------------------------------------	--	---------------------------

<u>ОГАПОУ «БИК»</u> (место работы)	<u>зав.отделением</u> (занимаемая должность)	_____ / _____ (Ф.И.О.)
---------------------------------------	---	---------------------------

Эксперт от работодателя:

_____ / _____ (место работы)	_____ / _____ (занимаемая должность)	_____ / _____ (Ф.И.О.)
---------------------------------	---	---------------------------

Индивидуальные показатели успеваемости

1. ФИО студента _____
2. Группа _____
3. Специальность 09.02.06 Сетевое и системное администрирование

Элемент модуля	Результаты промежуточной аттестации		
	Форма промежуточной аттестации	Оценка	Ф.И.О. преподавателя
МДК03.01. Эксплуатация объектов сетевой инфраструктуры	Э (экзамен)		
Курсовое проектирование	ДЗ (диф.зачет)		
МДК 03.02 Безопасность компьютерных сетей	ДЗ (диф.зачет)		
Учебная практика УП.03	ДЗ (диф.зачет)		
Производственная практика (по профилю специальности) ПП.03	ДЗ (диф.зачет)		

Менеджер модуля ПМ.03
Эксплуатация объектов сетевой
инфраструктуры

С.А. Герасимова

Заведующий отделением

**Бланк
анализа портфолио**

№ п/п	Элемент портфолио	Наличие (да/нет)	Соответствие требованиям к оформлению портфолио <i>(соответствует полностью/ частично, не соответствует)</i>
1.	Титульный лист		
2.	Индивидуальные показатели успеваемости		
3.	Бланк анализа портфолио		
4.	Оценочная ведомость по профессиональному модулю		
5.	Дневник производственной практики		
6.	Дневник учебной практики		
7.	Производственная характеристика		
	Дополнительные материалы		
8.	Сведения об участии студента в олимпиадах и конкурсах профессионального мастерства, конференциях по профилю специальности		
9.	Сведения об участии студента в профориентационной работе		
10.	Документы о поощрении за участие в мероприятиях различного уровня		
11.	<i>Другое</i>		

Менеджер модуля

«_____» _____ 201__ г.

(подпись)

С.А. Герасимова

(Ф.И.О.)

**1. Участие в олимпиадах, конкурсах
профессионального мастерства по профилю специальности**

№ п/п	Компетенция	Название олимпиады	Место и время проведения	Примечание (наличие грамоты, диплома и т.п.)
1.				

Классный руководитель

(подпись)

(Ф.И.О.)

**2. Учебно-исследовательская, проектная
деятельность студента по профилю специальности**

№ п/п	Компетенция	Название мероприятия	Дата проведения	Тема выступления	Наличие публикации (название, выходные данные)
1.					

Классный руководитель

_____ (подпись)

_____ (Ф.И.О.)

3. Спортивные и иные достижения студента, свидетельствующие об освоении общих и профессиональных компетенций

№ п/п	Компетенция	Вид спорта	Участие в соревнованиях	Дата соревнований	Примечание (отметка о наличии сертификата, грамоты, диплома и т.п.)
1.					

Руководитель физ.воспитания

_____ (подпись)

С.И. Толстых
(Ф.И.О.)

Аттестационный лист по учебной практике

ФИО студента _____

Группа _____

Специальность 09.02.06 Сетевое и системное администрирование

Место проведения практики (организация), наименование, юридический адрес

Время проведения практики _____

Виды и объем работ, выполненные студентом во время практики:

№ п/п	Вид работ	Количество часов	Качество выполнения работ: «5» (отлично), «4» (хорошо), «3» (удовл.), «2» (неудовл.)
1.	Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.	2	
2.	Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	2	
3.	Полоса пропускания, паразитная нагрузка.	2	
4.	Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров,	4	
5.	Наращивание длины сегментов сети; замена существующей аппаратуры.	2	
6.	Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.	2	
7.	Техническая и проектная документация. Паспорт технических устройств.	2	
8.	Физическая карта всей сети; логическая топология компьютерной сети.	4	
9.	Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.	2	
10.	Проверка объектов сетевой инфраструктуры и профилактические работы	4	
11.	Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	2	
12.	Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.	4	

13.	Протокол SNMP, его характеристики, формат сообщений, набор услуг.	2	
14.	Задачи управления: анализ производительности и надежности сети.	2	
15.	Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	4	
16.	Эксплуатация систем IP-телефонии. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323. Установка и поддержка соединения H.323.	2	
17.	Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP.	4	
18.	Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами.	2	
19.	Управление программным коммутатором. Маршрутизация. Группы соединительных линий.	2	
20.	Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	4	
21.	Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.	2	
22.	Фундаментальные принципы безопасной сети Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	2	
23.	Безопасность Сетевых устройств OSI Безопасный доступ к устройствам. Назначение административных ролей.	4	
24.	Авторизация, аутентификация и учет доступа (AAA) Свойства AAA. Локальная AAA аутентификация. Server-based AAA	2	
25.	Реализация технологий брандмауэра ACL.	2	
26.	Реализация технологий предотвращения вторжения IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	4	
27.	Безопасность локальной сети	2	
28.	Криптографические системы Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность.	4	
29.	Реализация технологий VPN	2	

30.	Управление безопасной сетью Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости.	4	
31.	Cisco ASA	4	
32.	Социальная инженерия	2	
33.	Исследование сетевых атак и инструментов проверки защиты сети	2	
34.	Настройка безопасного доступа к маршрутизатору	2	
35.	Обеспечение административного доступа AAA и сервера Radius	2	
36.	Настройка политики безопасности брандмауэров	4	
37.	Настройка системы предотвращения вторжений (IPS)	2	
38.	Настройка безопасности на втором уровне на коммутаторах	2	
39.	Настройка Site-to-SiteVPN используя интерфейс командной строки	2	
40.	Исследование методов шифрования	4	
			«5» (отлично), «4» (хорошо), «3» (удовл.), «2» (неудовл.)

Руководитель
учебной практики

_____ (подпись)

_____ (Ф.И.О.)

«___» _____ 201__ г.

Областное государственное автономное профессиональное образовательное
учреждение
«Белгородский индустриальный колледж»

ДНЕВНИК

УП. 03 УЧЕБНОЙ ПРАКТИКИ

ПМ .03 Эксплуатация объектов сетевой инфраструктуры
для специальности
09.02.06 Сетевое и системное администрирование

Ф.И.О (практиканта)

студента группы _____

семестр _____ с _____ 201 года по _____ 201 года
(время прохождения практики)

Место проведения практики _____

Программа учебной практики по ПМ.03
выполнена _____
(указать полностью или не полностью)

За время прохождения практики пропустил _____ дней

Практика была _____
(указать оплачиваемая или не оплачиваемая, при возможности указывается
примерная сумма заработка)

_____/_____/

МП

подпись руководителя практики от предприятия

_____/_____/

МП

подпись руководителя практики ООП

**Содержание и виды ежедневных работ
по учебной практике**

Дата	Наименование работ	Оценка работы

Наставник _____ / _____ /
(подпись)

Куратор _____ / _____ /
(подпись)

Аттестационный лист по производственной практики (по профилю специальности)

ФИО студента _____

Группа _____

Специальность 09.02.06 Сетевое и системное администрирование

Место проведения практики (организация), наименование, юридический адрес

Время проведения практики _____

Виды и объем работ, выполненные студентом во время практики:

№ п/п	Вид работ	Количество часов	Качество выполнения работ: «5» (отлично), «4» (хорошо), «3» (удовл.), «2» (неудовл.)
1.	Вводное практическое занятие; знакомство с высокотехнологичным оборудованием	2	
2.	Правила оказания первой медицинской помощи. Инструктаж по охране труда.	2	
3.	Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.	2	
4.	Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	2	
5.	Полоса пропускания, паразитная нагрузка.	2	
6.	Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров,	4	
7.	Наращивание длины сегментов сети; замена существующей аппаратуры.	2	
8.	Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.	2	
9.	Техническая и проектная документация. Паспорт технических устройств.	2	
10.	Физическая карта всей сети; логическая топология компьютерной сети.	4	
11.	Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.	2	
12.	Проверка объектов сетевой инфраструктуры и профилактические работы	4	
13.	Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	2	

14.	Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.	4	
15.	Протокол SNMP, его характеристики, формат сообщений, набор услуг.	2	
16.	Задачи управления: анализ производительности и надежности сети.	2	
17.	Оконцовка кабеля витая пара	2	
18.	Заделка кабеля витая пара в розетку	2	
19.	Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену	4	
20.	Тестирование кабеля	2	
21.	Поддержка пользователей сети.	4	
22.	Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)	4	
23.	Выполнение действий по устранению неисправностей	2	
24.	Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	2	
25.	Оформление технической документации, правила оформления документов	2	
26.	Протокол управления SNMP	4	
27.	Основные характеристики протокола SNMP	2	
28.	Набор услуг (PDU) протокола SNMP	2	
29.	Формат сообщений SNMP	2	
30.	Задачи управления: анализ производительности сети	4	
31.	Задачи управления: анализ надежности сети	2	
32.	Управление безопасностью в сети.	4	
33.	Учет трафика в сети	2	
34.	Средства мониторинга компьютерных сетей	4	
35.	Средства анализа сети с помощью команд сетевой операционной системы	2	
36.	Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	4	

37.	Эксплуатация систем IP-телефонии. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323. Установка и поддержка соединения H.323.	2	
38.	Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP.	4	
39.	Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами.	2	
40.	Управление программным коммутатором. Маршрутизация. Группы соединительных линий.	2	
41.	Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	4	
42.	Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы	2	
43.	Настройка аппаратных IP-телефонов	4	
44.	Настройка программных IP-телефонов, факсов	4	
45.	Развертывание сети с использованием VLAN для IP-телефонии	2	
46.	Настройка шлюза	2	
47.	Установка, подключение и первоначальные настройки голосового маршрутизатора	2	
48.	Настройка таблицы пользователей в голосовом маршрутизаторе	4	
49.	Настройка групп в голосовом маршрутизаторе	2	
50.	Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе	2	
51.	Настройка голосовых сообщений в маршрутизаторе	4	
52.	Настройка программно-аппаратной IP-АТС	4	
53.	Установка и настройка программной IP-АТС (например, Asterisk)	2	
54.	Тестирование кодеков. Исследование параметров качества обслуживания	2	
55.	Мониторинг и анализ соединений по различным протоколам	2	
56.	Мониторинг вызовов в программном коммутаторе	4	

57.	Создание резервных копий баз данных	2	
58.	Диагностика и устранение неисправностей в системах IP-телефонии	4	
59.	Фундаментальные принципы безопасной сети Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	2	
60.	Безопасность Сетевых устройств OSI Безопасный доступ к устройствам. Назначение административных ролей.	2	
61.	Авторизация, аутентификация и учет доступа (AAA) Свойства AAA. Локальная AAA аутентификация. Server-based AAA	2	
62.	Реализация технологий брандмауэра ACL.	4	
63.	Реализация технологий предотвращения вторжения IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	4	
64.	Безопасность локальной сети	2	
65.	Криптографические системы Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность.	4	
66.	Реализация технологий VPN	2	
67.	Управление безопасной сетью Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости.	4	
68.	Cisco ASA	4	
69.	Социальная инженерия	2	
70.	Исследование сетевых атак и инструментов проверки защиты сети	2	
71.	Настройка безопасного доступа к маршрутизатору	2	
72.	Обеспечение административного доступа AAA и сервера Radius	2	
73.	Настройка политики безопасности брандмауэров	2	
74.	Настройка системы предотвращения вторжений (IPS)	2	
75.	Настройка безопасности на втором уровне на коммутаторах	2	
76.	Настройка Site-to-SiteVPN используя интерфейс командной строки	2	
77.	Исследование методов шифрования	2	
78.	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	2	

79.	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	2	
80.	Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и	2	
81.	Настройка Clientless Remote Access SSL VPNs используя ASDM	2	
82.	Настройка AnyConnect Remote Access SSL VPN используя ASDM	2	
			«5» (отлично), «4» (хорошо), «3» (удовл.), «2» (неудовл.)

Руководитель производственной
практики (по профилю специальности) _____
(подпись)

_____ (Ф.И.О.)

«___» _____ 201__ г.

Областное государственное автономное профессиональное
образовательное учреждение
«Белгородский индустриальный колледж»

ДНЕВНИК

ПП. 03 ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

ПМ .03 «Эксплуатация объектов сетевой инфраструктуры»
для специальности
09.02.06 Сетевое и системное администрирование

Ф.И.О (практиканта)

студента группы _____

семестр _____ с _____ 201 года по _____ 201 года
(время прохождения практики)

Место проведения практики _____

Программа производственной практики (по профилю специальности) по ПМ.03
выполнена _____
(указать полностью или не полностью)

За время прохождения практики пропустил _____ дней

Практика была _____
(указать оплачиваемая или не оплачиваемая, при возможности указывается
примерная сумма заработка)

_____/_____/

МП

подпись руководителя практики от предприятия

_____/_____/

МП

подпись руководителя практики ООП

**Содержание и виды ежедневных работ
по учебной практике**

Дата	Наименование работ	Оценка работы

Наставник _____ / _____ /

(подпись)

Куратор _____ / _____ /

(подпись)

ПРОИЗВОДСТВЕННАЯ ХАРАКТЕРИСТИКА

на практиканта _____

_____ фамилия, имя, отчество

проходившего производственную практику по профессиональному модулю

ПМ03. Эксплуатация объектов сетевой инфраструктуры

(на) _____

в период с _____ г. по _____ г.

трудовая дисциплина, отношение к порученной работе, взаимоотношения в коллективе, участие в рационализаторской работе, полученный профессиональный опыт, качество выполнения работ).

Обучающийся _____ освоил

ПК:

ОК:

Руководитель производственной практики
от предприятия

_____ / _____ /
должность, подпись, Ф.И.О.

Начальник ОК

« _____ » _____ 201 г.

(М.П.)

Руководитель производственной
практики от колледжа _____ / _____