ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ
для специальности
11.02.15 Инфокоммуникационные сети и системы связи

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ
МДК.03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ
(6 семестр)

Перечень вопросов и заданий для проведения дифференцированного зачета

Теоретические вопросы:
1. Актуальность проблемы обеспечения безопасности информационных технологий.
2. Место и роль информационных систем в управлении бизнес-процессами.
3. Основные причины обострения проблемы обеспечения безопасности информационных технологий.
4. Основные понятия в области безопасности информационных технологий.
5. Информация и информационные отношения.
6. Субъекты информационных отношений, их безопасность.
7. Угрозы безопасности информационных технологий.
8. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.
9. Классификация угроз безопасности.
10. Принципы обеспечения безопасности информационных технологий.
11. Виды мер противодействия угрозам безопасности.
12. Достоинства и недостатки различных видов мер защиты.
13. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
14. Правовые основы обеспечения безопасности информационных технологий.
15. Защищаемая информация.
16. Персональные данные.
17. Коммерческая тайна.
18. Информация в ключевых системах информационной инфраструктуры.
19. Государственная система защита информации.
20. Организация защиты информации в системах и средствах информатизации и связи.
21. Контроль состояния защиты информации.
22. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.
23. Идентификация и аутентификация пользователей.
24. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
25. Регистрация и оперативное оповещение о событиях безопасности.
26. Понятие технологии обеспечения безопасности информации.
27. Влияние на безопасность со стороны руководства организаций.
28. Институт ответственных за обеспечение безопасности ИТ.
29. Обязанности пользователей и ответственных за обеспечение безопасности ИТ.
30. Общие правила обеспечения безопасности ИТ при работе сотрудников.
31. Ответственность за нарушения безопасности ИТ.

32. Порядок работы с носителями ключевой информации.
33. Документы, регламентирующие правила парольной и антивирусной защиты.
34. Инструкция по организации парольной защиты.
35. Инструкция по организации антивирусной защиты.
36. Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей.
37. Регламентация допуска сотрудников к работе.
38. Правила именования пользователей.
39. Процедура авторизации сотрудников.
40. Порядок изменения конфигурации программно-аппаратных средств.
41. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы.
42. Экстренная модификация.
43. Регламентация процессов разработки, внедрения и сопровождения задач.
44. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.
45. Определение требований к защите и категорирование ресурсов.
46. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.
47. Категорирование защищаемых ресурсов.
48. Проведение информационных обследований и документирование защищаемых ресурсов.
49. Планы защиты и планы обеспечения непрерывной работы и восстановления.
50. Составные части планов защиты и обеспечения непрерывной работы.
51. Средства обеспечения непрерывной работы.
52. Обязанности и действия персонала по обеспечению непрерывной работы.
53. Основные задачи подразделений обеспечения безопасности ИТ.
54. Организационная структура подразделения безопасности.
55. Организационно-правовой статус службы обеспечения безопасности информации.
56. Концепция безопасности информационных технологий предприятия.
57. Вопросы, которые должны быть отражены в Концепции.

Практические задания (типовые):
1. Выполните сканирование логических дисков с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
2. Получите список пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
3. Создайте отчет на базе СПО ЗИ (например, РЕВИЗОР-1XP).
4. Установите права доступа с помощью СПО ЗИ.
5. Выполните считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
6. Выполните сканирование дерева ресурсов с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
7. Выполните регистрацию пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP).
8. Выполните установку и снятие СЗИ с помощью программы СЗИ НСД (например, Страж NT).
9. Выполните исследование программной среды с помощью СЗИ НСД (например, Страж NT).
10. Сравните возможности управления пользователями с помощью СЗИ НСД (например, Страж NT).
11. Выполните учет пользователей и контроль устройств с помощью СЗИ НСД (например, Страж NT).
12. Проанализируйте избирательное управление с помощью СЗИ НСД (например, Страж NT).
13. Выполните сортировку и поиск с помощью СЗИ НСД.
14. Выполните редактирование пользователей с помощью СЗИ НСД (например, Страж NT).
15. Проанализируйте изменения настроек СЗИ с помощью СЗИ НСД (например, Страж NT).
16. Выполните защиту съемных носителей с помощью СЗИ НСД (например, Страж NT).
17. Выполните настройку маркировки документов с помощью СЗИ НСД (например, Страж NT).

Критерии оценки

Оценка «5» «отлично» - обучающийся дает полный, развернутый ответ на поставленные вопросы; изложение материала структурированное, системное в соответствии с требованиями учебной программы; знание об объекте демонстрируется на фоне понимания его в системе данного курса и междисциплинарных связей; ответ изложен литературным языком с использованием научной терминологии.

Оценка «4» «хорошо» - обучающийся дает полный, развернутый ответ на поставленный вопрос, показывает умение выделять существенные и несущественные признаки; имеющиеся у обучающегося знания соответствуют минимальному объему содержания предметной подготовки; изложение знаний системное в соответствии с требованиями учебной программы; возможны несущественные ошибки в формулировках; ответ логичен, изложен литературным языком с использованием научной терминологии.

Оценка «3» «удовлетворительно» - обучающийся дает недостаточно полный и недостаточно развернутый ответ; допущены ошибки в раскрытии понятий, употреблении терминов; изложение материала требует поправок, коррекции.

Оценка «2» «неудовлетворительно» - обучающийся дает неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях; изложение неграмотно, допущены существенные ошибки; отсутствует интерес, стремление к добросовестному и качественному выполнению учебных заданий.

ЭКЗАМЕН

(7 семестр)

Перечень вопросов и заданий для проведения экзамена

Теоретические вопросы:

1. Назначение и возможности средств защиты информации от НСД.
2. Защита от вмешательства в процесс функционирования АС посторонних лиц.
3. Регистрация действий пользователей.
4. Обеспечение аутентификации абонентов.
5. Рекомендации по выбору средств защиты информации от НСД.
6. Распределение показателей защищенности по классам для автоматизированных систем.
7. Требования руководящих документов ФСТЭК к средствам защиты информации.
8. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK).
9. Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть»).
10. Назначение и особенности применения СЗИ НСД (например, «Страж NT»).
11. Назначение и специфика применения комплекса ЗИ (например, «Соболь»).
12. Устройства аутентификации на базе смарт-карт и USB-токенов.
13. Реализация схем аутентификации.
14. Программные средства, реализующие инфраструктуру открытых ключей.
15. Назначение и функциональные возможности eToken и Рутокен.
16. Алгоритм генерации одноразовых паролей.
17. Формирование электронной цифровой подписи.
18. Вычисление ключа согласования Диффи- Хеллмана.
19. Особенности разграничения доступа к ресурсам системы.
20. Избирательное разграничение доступа.
21. Проблемы обеспечения безопасности в компьютерных системах и сетях.
22. Типовая корпоративная сеть.
23. Уязвимости и их классификация.
24. Назначение, возможности и защитные механизмы межсетевых экранов.
25. Угрозы, связанные с периметром сети.

26. Типы межсетевых экранов.
27. Сертификация межсетевых экранов.
28. Анализ содержимого почтового и WEB-трафика.
29. HTTP-трафик.
30. Виртуальные частные сети.
31. Решение на базе ОС Windows 2003.
32. VPN на основе криптошлюза (например, «Континент-К»).
33. Обнаружение и устранение уязвимостей.
34. Архитектура систем управления уязвимостями.
35. Особенности сетевых агентов сканирования.
36. Специализированный анализ защищенности.
37. Обзор средств анализа защищенности.
38. Мониторинг событий безопасности.
39. Инфраструктура управления журналами событий.
40. Категории журналов событий.
41. Введение в технологию обнаружения атак.
42. Классификация систем обнаружения атак.

Практические задания (типовые):
1. Выполните ввод информации в САПР СЗИ.
2. Выполните расчет радиуса контролируемой зоны с помощью САПР СЗИ (например, «Гроза-К»).
3. Выполните исследование защищенности с помощью САПР СЗИ.
4. Сформируйте и выполните вывод проекта протокола в САПР СЗИ (например, «Гроза-К»).
5. Составьте план тестирования при помощи СПО ЗИ.
6. Выполните тестирование при помощи СПО ЗИ (например, «Ревизор-2XP»).
7. Выполните исследование содержимого текущего диска с помощью СПО ЗИ (например, «Terrier»).
8. Выполните доступ в систему с использованием СПО ЗИ и УП (например, «SecretNet»).
9. Выполните разграничение доступа с использованием СПО ЗИ и УП (например, «SecretNet»).
10. Выполните контроль и регистрацию с использованием СПО ЗИ и УП (например, «SecretNet»).
11. Отследите события НСД с использованием СПО ЗИ и УП (например, «SecretNet»).
12. Выполните обновление клиента с использованием СПО ЗИ и УП.
13. Выполните удаление клиента с использованием СПО ЗИ и УП (например, «SecretNet»).
14. Изучите возникшую проблемную ситуацию с использованием СПО ЗИ и УП (например, «SecretNet»), сделайте вывод.

Критерии оценки
Оценка «5» «отлично» - при ответе на теоретический вопрос обучающийся показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний; обучающийся самостоятельно и правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия, ссылаясь на нормативно-правовую базу.
Оценка «4» «хорошо» - при ответе на теоретический вопрос обучающийся показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы; в тоже время при ответе допускает несущественные погрешности; обучающийся самостоятельно и в основном правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия.
Оценка «3» «удовлетворительно» - при ответе на теоретический вопрос обучающийся показывает достаточные, но не глубокие знания программного материала; при ответе не

допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами; для получения правильного ответа требуется уточняющие вопросы; обучающийся в основном решает учебно-профессиональные задачи (задания), допускает несущественные ошибки, слабо аргументирует свое решение, используя в основном понятия.

Оценка «2» «неудовлетворительно» - при ответе на теоретический вопрос дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками; обучающийся не решил учебно-профессиональные задачи (задания).

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ
МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи

ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ
(7 семестр)

Перечень вопросов и заданий для проведения дифференцированного зачета

Теоретические вопросы:
1. Основные понятия информационной безопасности.
2. Сущность и понятия защиты информации.
3. Значение информационной безопасности и ее место в системе национальной безопасности.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.
6. Виды и источники угроз информационной безопасности Российской Федерации.
7. Доктрина информационной безопасности Российской Федерации.
8. Состояние информационной безопасности РФ и основные задачи по ее обеспечению.
9. Государственная система обеспечения информационной безопасности Российской Федерации.
10. Регуляторы в области информационной безопасности.
11. Структура правовой защиты информации.
12. Система документов в области защиты информации.
13. Организационные основы защиты информации.
14. Принципы организационной защиты информации.
15. Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции.
16. Обзор стандартов и методических документов в области защиты информации.
17. Регулирующие организации в области защиты информации.
18. Классификация информации по категориям доступа.
19. Критерии оценки информации.
20. Категории нарушений по степени важности.
21. Ответственность за правонарушения в информационной сфере.
22. Руководящие документы, регламентирующие ответственность.
23. Виды ответственности за правонарушения в информационной сфере.
24. Общая характеристика комплексной защиты информации.
25. Основы обеспечения комплексной защиты информации.
26. Сущность и задачи комплексной защиты информации.
27. Стратегии комплексной защиты информации.
28. Структура и основные характеристики комплексной защиты информации.
29. Конфиденциальные сведения. Виды конфиденциальной информации.
30. Персональные данные.
31. Коммерческая тайна.
32. Банковская тайна.
33. Система физической защиты.
34. Обобщенная структурная схема охраны объекта. Посты охраны.
35. Подсистема инженерной защиты.
36. Периметровая сигнализация и ограждение. Периметровое освещение.
37. Способы и средства обнаружения угроз.
38. Комплексное обследования защищенности информационной системы.

39. Средства нейтрализации угроз.
40. Основы инженерно-технической защиты информации.
41. Подразделения технической защиты информации и их основные задачи.
42. Механические системы защиты.
43. Понятие несанкционированного доступа к защищаемой информации.
44. Понятие НСД к информации. Виды НСД к информации.
45. Технические каналы утечки информации.
46. Общая структура канала утечки информации.
47. Классификация каналов утечки информации.
48. Основные способы и средства НСД к защищаемой информации.
49. Активные способы НСД к информации.
50. Защита информации от утечки по техническим каналам передачи информации.
51. Пассивное противодействие НСД.
52. Обеспечение безопасности телефонных переговоров.
53. Противодействие незаконному подключению к линиям связи.
54. Противодействие контактному и бесконтактному подключению.
55. Защита от перехвата.
56. Противодействие несанкционированному доступу к источникам конфиденциальной информации.
57. Защита информации в каналах связи.
58. Акустический контроль.
59. Понятие разборчивости речи при перехвате информации.
60. Способы и средства информационного скрытия речевой информации от подслушивания.
61. Демаскирующие признаки закладных устройств.
62. Классификация средств обнаружения и локализации закладных устройств и их излучений.
63. Классификация средств обнаружения неизлучающих закладок.
64. Контроль линий связи, отходящих от технических средств.
65. Принципы контроля телефонных линий и цепей электропитания и заземления.
66. Принципы контроля цепей электропитания.
67. Контроль слаботочных цепей.
68. Принципы контроля линий заземления
69. Средства нелинейной радиолокации.
70. Принципы работы устройств нелинейной радиолокации.
71. Нелинейные радиолокаторы.
72. Современные средства радиолокации
73. Методы поиска радиоизлучений закладных устройств.
74. Индикаторы поля.
75. Обнаружение радиоизлучений. Панорамные радиоприемники.
76. Сканирующие приемники.

Практические задания:

1. Продемонстрируйте порядок работы профессионального нелинейного радиолокатора (например, NR- 900EMS).
2. Продемонстрируйте порядок работы многофункционального поискового прибора (например, ST 033P Пиранья).
3. Продемонстрируйте порядок работы анализатора спектра (например, OSCORGreen-8).
4. Продемонстрируйте порядок работы имитатора источника радиосигналов с различными видами модуляции (например, АВРОРА-3).
5. Продемонстрируйте порядок работы комплекса обнаружения радиоизлучающих средств и радиомониторинга (например, КРОНА-ПРО).
6. Продемонстрируйте порядок работы скоростного приемника сигналов (например, СКОРПИОН-XL).
7. Дайте сравнительный анализ принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165).

8. Дайте сравнительный анализ возможностей работы фильтров сетевых помехоподавляющих (например, ЛФС-10-1Ф и ФСП-1Ф-10А).
9. Проанализируйте порядок работы генератора шума для защиты от ПЭМИН (например, ЛГШ-501).
10. Постройте модель угроз объекта защиты.
11. Разработайте комплексную систему инженерно-технической защиты информации на объекте.
12. Проанализируйте возможности устройства для защиты объектов информатизации (например, СОНАТА-Р2, САЛЮТ 2000Б).
13. Проанализируйте методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств (например, ПРОКРУСТ-2000).
14. Проанализируйте возможности автоматизированной системы изменений сверхмалых величин.
15. Проанализируйте технические средства и отходящие от них линий с помощью системы измерений сверхмалых величин (напри мер, ТАЛИС-НЧ-ЛАЙТ)
16. Продемонстрируйте на практике возможностей системы оценки защищенности оптических линий связи.
17. Измерьте параметры ВОСП с помощью системы оценки защищенности оптических линий связи.
18. Выполните оценку защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ).
19. Продемонстрируйте на практике возможности системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН.
20. Выполните оценку защищенности с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН.
21. Измерьте параметры ПЭМИН и рассчитайте показатели защищенности технического средства (например, СИГУРД-М19).
22. Продемонстрируйте на практике возможности системы оценки защищенности выделенных помещений.
23. Измерьте уровень звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений (например, ШЕПОТ).
24. Измерьте уровень виброускорения в ограждающих конструкциях.
25. Выполните расчет и оценку защищенности помещения по акустическому каналу.
26. Выполните расчет и оценку защищенности помещения по виброакустическому каналу (например, с помощью комплекса ШЕПОТ).

Критерии оценки

Оценка «5» «отлично» - при ответе на теоретический вопрос обучающийся показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний; обучающийся самостоятельно и правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия, ссылаясь на нормативно-правовую базу.

Оценка «4» «хорошо» - при ответе на теоретический вопрос обучающийся показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы; в тоже время при ответе допускает несущественные погрешности; обучающийся самостоятельно и в основном правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия.

Оценка «3» «удовлетворительно» - при ответе на теоретический вопрос обучающийся показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами; для получения правильного

ответа требуется уточняющие вопросы; обучающийся в основном решает учебно-профессиональные задачи (задания), допускает несущественные ошибки, слабо аргументирует свое решение, используя в основном понятия.

Оценка «2» «неудовлетворительно» - при ответе на теоретический вопрос дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками; обучающийся не решил учебно-профессиональные задачи (задания).

ДИФФЕРЕНЦИРОВАННЫЙ ЗАЧЕТ

(8 семестр)

Перечень вопросов и заданий для проведения дифференцированного зачета

Теоретические вопросы:

1. Основы криптографии.
2. Структура криптосистемы.
3. Основные методы криптографического преобразования данных.
4. Требования, предъявляемые к криптографическим системам.
5. Симметричные и ассиметричные криптосистемы.
6. Шифрование методом замены.
7. Шифрование методом перестановки.
8. Шифрование методом гаммирования.
9. Криптосистемы с открытым ключом.
10. Основы шифрования с открытым ключом.
11. Алгоритм обмена ключами Диффи-Хеллмана.
12. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.
13. Системы электронной подписи.
14. Проблема аутентификации данных и электронная цифровая подпись.
15. Технология работы электронной подписи.
16. Безопасные хеш-функции, алгоритмы хеширования.
17. Контрольное значение циклического избыточного кода CRC.
18. Цифровые сертификаты.
19. Отечественный стандарт цифровой подписи.
20. Понятие криптоанализа.
21. Общие вопросы по аттестации ОИ по требованиям безопасности информации.
22. Основные стадии создания системы защиты информации на ОИ.
23. Порядок проведения аттестации объектов информатизации.
24. Организационная структура системы аттестации объектов информатизации.
25. Программа и методика проведения аттестационных испытаний.
26. Лицензирование деятельности в области защиты конфиденциальной информации.
27. Документы, разрабатываемые на объектах информатизации.
28. Документы, разрабатываемые на аттестуемое помещение.
29. Порядок действий при лицензировании.

Практические задания (типовые):

1. Выполните поиск и локализацию скрытых видеокамер (например, с помощью прибора ОПТИК-2).
2. Проанализируйте методы защиты сотовых телефонов от несанкционированного прослушивания (например, с помощью изделия Ладья-ИВТ).
3. Проанализируйте методы блокирования средств несанкционированного прослушивания и передачи данных различных стандартов (например, с помощью устройства КЕДР-1М).
4. Выполните поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора (например, с помощью NR-900EMS).

5. Выполните поиск устройств негласного съема информации с помощью многофункционального поискового прибора (например, с помощью ST 033P Пиранья).
6. Выполните оценку защищенности помещения с помощью многофункционального поискового прибора (напри мер, ST 033P Пиранья).
7. Выполните обнаружение цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165).
8. Выполните идентификацию цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165).
9. Выполните локализацию цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165).
10. Продемонстрируйте порядок работы генератора шума по сети электропитания и линиям заземления (например, ЛГШ-221)
11. Выполните поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО).

Критерии оценки

Оценка «5» «отлично» - обучающийся дает полный, развернутый ответ на поставленные вопросы; изложение материала структурированное, системное в соответствии с требованиями учебной программы; знание об объекте демонстрируется на фоне понимания его в системе данного курса и междисциплинарных связей; ответ изложен литературным языком с использованием научной терминологии.

Оценка «4» «хорошо» - обучающийся дает полный, развернутый ответ на поставленный вопрос, показывает умение выделять существенные и несущественные признаки; имеющиеся у обучающегося знания соответствуют минимальному объему содержания предметной подготовки; изложение знаний системное в соответствии с требованиями учебной программы; возможны несущественные ошибки в формулировках; ответ логичен, изложен литературным языком с использованием научной терминологии.

Оценка «3» «удовлетворительно» - обучающийся дает недостаточно полный и недостаточно развернутый ответ; допущены ошибки в раскрытии понятий, употреблении терминов; изложение материала требует поправок, коррекции.

Оценка «2» «неудовлетворительно» - обучающийся дает неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях; изложение неграмотно, допущены существенные ошибки; отсутствует интерес, стремление к добросовестному и качественному выполнению учебных заданий.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

ЭКЗАМЕН
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
(8 семестр)

Типовое профессионально-ориентированное задание для проведения экзамена

На объекте имеется Wi-fi точка доступа, подключиться к которой можно используя следующие параметры:
Имя сети: DE-2024
Ключ: de24-key

Для организации подключения отдельной группы пользователей к беспроводной сети необходимо установить WDS соединение (мост), используя вторую точку доступа.

При организации соединения необходимо использовать следующие обозначения:
SSID – Student#
Ключ - #key
Тип защиты сети - WPA2-PSK.
Служба DHCP должна быть отключена.
IP-адрес: 172.16.0.10#
Маска подсети: 255.255.0.0

Убедитесь в наличии подключения к сети Интернет.

Помимо роутера на объекте должен быть установлен IP камера видеонаблюдения.

Для настройки IP камеры:
Имя IP-камеры DVR#
IP-адрес: 172.16.0.11#
Маска подсети: 255.255.0.0
Шлюз: 172.16.0.1
Параметры видеопотока: Разрешение: 1024x768

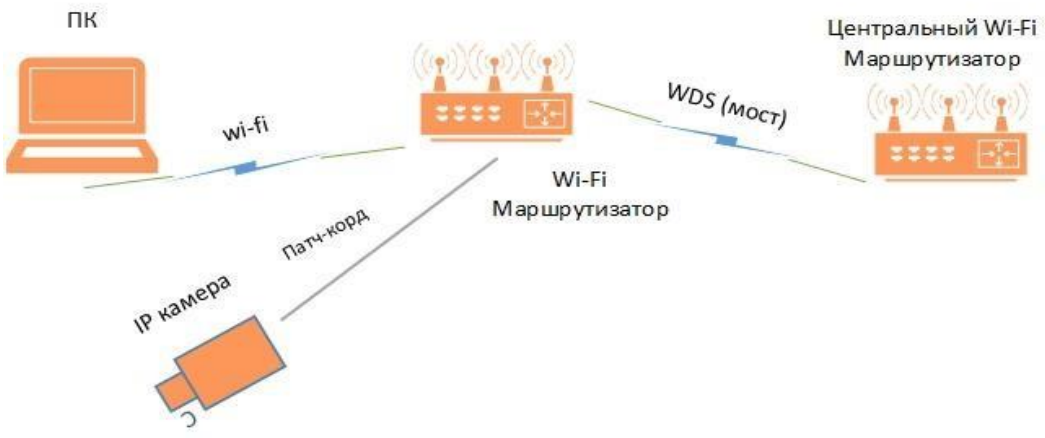
ПК должен быть подключен к созданной беспроводной сети.

Для подключения IP камеры необходимо изготовить патч-корд длиной 1 метр.

Трансляция видеопотока должна осуществляться на экране ПК, при помощи любого свободного программного обеспечения или WEB ресурса.

1. (# - номер рабочего места).

Схема организации подключения



Критерии оценки

Оценка «5» «отлично» - обучающийся самостоятельно и правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия, ссылаясь на нормативно-правовую базу; обучающийся демонстрирует полные и глубокие знания программного материала, показывает высокий уровень теоретических знаний и практических умений.

Оценка «4» «хорошо» - обучающийся самостоятельно и в основном правильно решает учебно-профессиональные задачи (задания), уверенно, логично, последовательно и аргументировано отвечает на вопросы, используя понятия; обучающийся показывает глубокие знания программного материала, грамотно его излагает, умело формулирует выводы; в тоже время при ответе допускает несущественные погрешности.

Оценка «3» «удовлетворительно» - обучающийся в основном решает учебно-профессиональные задачи (задания), допускает несущественные ошибки, слабо аргументирует свое решение, используя в основном понятия; обучающийся показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами; для получения правильного ответа требуется уточняющие вопросы.

Оценка «2» «неудовлетворительно» - обучающийся не решил учебно-профессиональную задачу (задание); дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками.