СОГЛАСОВАНО
Начальник отдела защиты информации
Департамента цифрового развития
Смоленской области
А.Н. Калугин
«31» 08 2021 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СМОЛЕНСК
Сертификат: 009533997B26BB162CCCB9A17C8FD30591
Владелец: Иванешко Ирина Васильевна
Действителен: с 22.05.2023 до 14.08.2024

Утверждаю
Зам. директора по учебной работе
И.В. Иванешко
«3» 08 2021 г.

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЭКЗАМЕНУ КВАЛИФИКАЦИОННОМУ)

по профессиональному модулю ПМ.03 Обеспечение информационной безопасности систем мобильной связи

Специальность 11.02.08 Средства связи с подвижными объектами

Экзамен квалификационный является итоговой формой контроля по профессиональному модулю и проверяет готовность студента к выполнению указанного вида профессиональной деятельности, сформированности у него компетенций, определенных в разделе «Требования к результатам освоения ППССЗ» ФГОС СПО.

При выполнении заданий студенты могут пользоваться различным оборудованием и наглядными пособиями, материалами справочного характера, нормативными документами и различными образцами, которые разрешены к использованию на экзамене квалификационном и указаны в билете в разделе инструкция.

Результаты экзамена квалификационного определяются на основании оценочной ведомости и/или результатов решения профессиональных задач оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», вносятся в итоговую ведомость экзамена квалификационного аттестационной комиссии и объявляются в тот же день.

Решение аттестационной комиссии об окончательной оценке студента по экзамену квалификационному принимается на закрытом заседании простым большинством голосов членов аттестационной комиссии, участвующих в заседании. При равном числе голосов голос председателя является решающим.

Критерии оценки экзамена квалификационного

Оценка	Критерии
«отлично»	Все задания выполнены в полном объеме.Ответы получены на все дополнительные вопросы членов аттестационной комиссии.
«хорошо»	Выполнены 2 задания в полном объеме.Ответы получены практически на все дополнительные вопросы членов аттестационной комиссии.
«удовлетворительно»	Выполнено 1 задание в полном объеме. Не получены ответы на дополнительные вопросы членов аттестационной комиссии.
«неудовлетворительно»	Не выполнено ни одно задание. Не получены ответы на дополнительные вопросы членов аттестационной комиссии.

Экзамен по профессиональному модулю проводится в устной форме по билетам. Билет содержит два практических задания для проверки освоенных профессиональных компетенций (ПК) и общих компетенций (ОК):

ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи

ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре выдавать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование систем и сетей.

ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Критерии оценивания экзаменационного задания.

Экзамен по профессиональному модулю проводится в устной форме по билетам. Билет содержит два практических задания для проверки освоенных профессиональных компетенций.

Задание 1.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК. fstec.ru.

Время выполнения: 15 минут.

Текст задания:

На предприятии связи обработка информации осуществляется группой сотрудников. В автоматизированной системы обработки данных работают пользователи с одинаковым уровнем доступа. Ресурсы, подлежащие защите, определены как ограниченные в доступе и имеющие статус конфиденциальной информации. Определите требуемый класс защищенности автоматизированной системы обработки данных (АСОД) на предприятии.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат	Правильность определения класса защищенности автоматизированной системы обработки данных, грамотное использование нормативных документов	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечениюбезопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой	1. Выполнение требований задания по определению минимального состава необходимых механизмов защиты и требований к содержанию защитных функций каждого из механизмов в каждом из классов систем. 2. Правильность определения класса защищенности автоматизированной системы обработки данных, грамотное использование нормативных документов 3. Грамотный выбор конкретного подхода к определению класса защищенности автоматизированной системы обработки данных.	2б 2б 1б

выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли		

Задание 2.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК.fstec.ru.

Время выполнения: 15 минут.

Текст задания:

На предприятии связи обработка информации осуществляется группой сотрудников. В автоматизированной системы обработки данных работают пользователи с одинаковым уровнем доступа. Ресурсы, подлежащие защите, определены как ограниченные в доступе и имеющие статус конфиденциальной информации. Класс защищенности АС предприятия определен как 2А.Определите требуемый класс защищенности средств вычислительной техники (СВТ) АСОД предприятия.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Правильность определения класса защищенности средств вычислительной техники, грамотное использование нормативных документов	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного	1. Выполнение требований задания по определению программных и технических частей систем обработки данных. 2. Правильность определения класса защищенности средств вычислительной техники, грамотное использование нормативных документов 3. Грамотный выбор конкретного подхода к определению класса защищенности средств вычислительной техники.	2б 2б 1б

		обеспечения, развития отрасли		

Задание 3.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; www.Ideco.ru.

Время выполнения: 15 минут.

Текст задания:

Проверить защиту корпоративной сети, используя он-лайн тестирование IdecoUTM: открытые порты и ответы сервисов на внешнем интерфейсе интернет-шлюза; есть ли IP-адрес в чёрных списках заражённых хостов; возможность проникновения тестовых образцов вирусов и эксплойтов; торренты, скачанные из сети за последний месяц; наличие пароля к почтев известных базах данных хакеров.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Грамотно проведенное тестирование корпоративной сети	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	1. Выполнение требований задания по анализу защищенности всех устройств, на которых работают сотрудники компании. 2. Грамотное владение сервисами, обеспечивающими проведение анализа защищенности сети 3. Грамотный выбор механизмов и средств для проведения анализа защищенности сети	2б 2б 1б

Задание 4.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:
Оборудование, ПО: ПК.
Время выполнения: 15 минут.
Текст задания:
Злоумышленники зашифровали файлы корпоративного компьютера трояном семейства Yanluowang. Зашифрованные критически важные данные необходимо попытаться восстановить. Предложите алгоритм действий в условиях произошедшего вирусозависимого инцидента.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Выбор механизмов и средств обеспечения информационной безопасности (программных и программно-аппаратных); построение системы антивирусной защиты в телекоммуникационных системах и сетях связи.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	1. Выполнение требований задания по обеспечению защищенности всех устройств, на которых работают сотрудники компании. 2. Грамотное владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи. 3. Грамотный выбор механизмов и средств для построения системы антивирусной защиты в телекоммуникационных системах и сетях связи	2б 2б 1б

Задание 5.
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, Dr.WebvxCube.
Время выполнения: 15 минут.
Текст задания:
В сети компании есть важные документы и конфиденциальные сведения, а Вы выявили подозрительное неизвестное приложение, но не уверены в его вредоносности, а антивирус считает файл «чистым», но у вас есть сомнения. Предложите алгоритм действий в данной ситуации.

Предмет(ы) оценивания	Объект(ы) оценивани	Показатели оценки	Критерии оценки	Вес критер

	я			ия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Выбор механизмов тестирования антивирусной защиты информационной системы	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	1. Выполнение требований задания по обеспечению защищенности всех устройств, на которых работают сотрудники компании. 2. Грамотное владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи. 3. Грамотный выбор механизмов и средств для тестирования системы антивирусной защиты в телекоммуникационных системах и сетях связи	2б 2б 1б

Задание 6.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК.fstec.ru.

Время выполнения: 15 минут.

Текст задания:

Для защиты физической границы (периметра) информационной системы предприятия, содержащей сведения, отнесенные к государственной тайне, приобрели межсетевой экран4-го класса защиты, профиль Б.Необходимо проверить выбор МЭ, сформулировать требования к сертифицированным межсетевым экранам и дать рекомендации по защите информации.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес крит ерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре,	Грамотный выбор МЭ, сформулированные требования к сертифицированным межсетевым	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной	1. Выполнение требований задания по обоснованию выбора МЭ. 2. Выполнение требований задания к средствам обеспечения	2 2

выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	экранам	безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	безопасности информационной системы предприятия, содержащей сведения, отнесенные к государственной тайне. 3. Рациональность распределения времени на описание выбранного решения.	1

Задание 7.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК.fstec.ru.

Время выполнения: 15 минут.

Текст задания:

Для антивирусной защиты серверов в государственной информационной системе, при отсутствии сведений, составляющих государственную тайну, приобрели средство антивирусной защиты 6 класса защиты, тип В. Необходимо проверить выбор средств антивирусной защиты, сформулировать требования к антивирусным средствам и дать рекомендации по защите информации.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач,	Грамотный выбор средств антивирусной защиты, сформулированные требования к сертифицированным средствам антивирусной защиты, понимание классификации средств антивирусной защиты.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций,	1. Выполнение требований задания по обоснованию выбора средств антивирусной защиты. 2. Выполнение требований задания к средствам обеспечения безопасности информационных технологий по применению средств антивирусной	2 2

оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	защиты. 3. Рациональность распределения времени на описание выбранного решения.	1

Задание 8.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, fstec.ru

Время выполнения: 15 минут.

Текст задания:

Для защиты корпоративной сети и обнаружения попыток злоумышленников проникнуть в сеть, выявления их присутствия в инфраструктуре предприятия (на предприятии отсутствуют сведения, составляющие государственную тайну), планируется приобрести систему обнаружения вторжений1 класса защиты. Необходимо проверить выбор СЗИ и сформулировать требования к системам обнаружения вторжений (использовать спецификацию профилей защиты ФСТЭК России).

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и	Грамотный выбор СОВ, сформулированные требования к сертифицированным СОВ, понимание спецификации профилей защиты	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение	1. Выполнение требований задания по обоснованию выбора СОВ. 2. Выполнение требований задания к средствам обеспечения безопасности информационных технологий по уровню доверия, требования к СОВ выбранного класса защиты 3. Рациональность распределения времени на описание выбранного решения.	2 2 1

использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли		

Задание 9.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, https://bdu.fstec.ru/calc.

Время выполнения: 15 минут.

Текст задания:

Провести оценку уязвимости в веб-приложении (уязвимость, позволяет атаку типа «подделка межсайтовых запросов» *[cross-site request forgery]* в панели администратора, позволяет добавить нового пользователя, удалить имеющегося пользователя или вообще всех пользователей).

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	Грамотное использование средств оценки уязвимостей	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и	1. Выполнение требований задания по реализации оценки уязвимостей с помощью CVSS 2.0 2. Грамотное использование базовых метрик. 3. Правильность использования калькулятора оценки уязвимостей.	2б 2б 1б

ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли		

Задание 10.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения: 15 минут.

Текст задания:

Настроить работу Модуля «Fail2ban» для анализа логов авторизации в веб-почте; почтовом сервере, SSH, FTP. Количество неудачных попыток авторизаций – 3. Интервал неудачных попыток авторизаций – 10 мин. Блокировать на 15 минут. Заблокируйте IP адрес: 192.168.1.101.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	1. Выполнение требований задания по реализации политики МЭ. 2. Правильность настройки модуля Fail2ban. 3. Правильность решения задания: при авторизации после 3 неудачных попыток учетная запись блокируется.	2б 2б 1б

Задание 11.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 10000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к почтовому серверу: разрешить TCP трафик, входящий на ИКС на порт SMTP(25), порт IMAP(143), порт POP3(110) через внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к почтовому серверу.	1б 2б 2б

Задание 12.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 8000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к VPN-серверу: разрешить TCP трафик, входящий на ИКС на порт pptp(1723) через внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к VPN серверу.	1б 2б 2б

Задание 13.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 7000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к WEB-серверу: разрешить TCP трафик, входящий на ИКС на порт веб-сервера (80) через внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы)	Показатели оценки	Критерии	Вес

	оценивания		оценки	критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к Webсерверу.	1б 2б 2б

Задание 14.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 5000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к FTP-серверу: разрешить TCP трафик, входящий на ИКС на порт FTP (21) через внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для	Реализация политики МЭ; основные требования к средствам и	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение	1б 2б

обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	видам МЭ	информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к FTPсерверу.	2б

Задание 15.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 6000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к DNS-серверу: разрешить UDP трафик, входящий на ИКС на порт dns (53) через внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых	1б 2б 2б

методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	правил для разрешения доступа к почтовому DNSсерверу.	

Задание 16.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 9500;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ для звонков через сервер IP-телефонии: разрешить трафик, входящий на ИКС на порт IP-телефонии (5060), 5061, порты для VoIP-соединений (10000-20000), порт IAX (4569) через внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к серверуIP-телефонии.	1б 2б 2б

ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.		

Задание 17.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 8000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к веб-авторизации: разрешить TCP трафик, входящий на ИКС от Локальные сети, DMZ сети на ИКС на порт 82 через внутренние интерфейсы, VPN-интерфейсы, DMZ.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами.	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к веб-авторизации	1б 2б 2б

профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.		

Задание 18.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 10000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ для программы авторизации: разрешить TCP трафик, входящий на ИКС от Локальные сети, DMZ сети на ИКС на порт Xauth (4888) через внутренние интерфейсы, VPN-интерфейсы, DMZ.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа для программы авторизации	1б 2б 2б

Задание 19.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:

- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 9000;
- режим работы межсетевого экрана - ipfw ->pf.

Создать разрешающие правила: доступ к локальному DNS-серверу: разрешить UDP трафик, входящий на ИКС от Локальные сети, DMZ сети на ИКС на порт dns (53) через внутренние интерфейсы, VPN-интерфейсы, DMZ.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к локальному DNS серверу.	1б 2б 2б

Задание 20.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/

Время выполнения задания – 15 минут.

Текст задания:

Настроить работу межсетевого экрана:
- адреса и подсети, с которых разрешен доступ к управлению ИКС через веб-интерфейс и к серверу ИКС по SSH - 192.168.17.206/24;
- максимальное количество активных соединений - 5500;
- режим работы межсетевого экрана - ipfw ->pf.
Создать разрешающие правила: доступ по протоколу ICMP: разрешить ICMP трафик, входящий на ИКС на внешние интерфейсы.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа по протоколу ICMP.	1б 2б 2б

Задание 21.
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК; ИКС https://demo-server.a-real.ru/
Время выполнения задания – 15 минут.
Текст задания:
Настроить работу детектора атак Suricata. Для корректного применения базы сигнатур модуля укажите расположение объектов (сетей, серверов и портов), подверженных проверке:
Интерфейсы: внешние интерфейсы;
Внутренние сети: локальные сети;
Внешние сети: внешние диапазоны адресов;
HTTP-порты: порты служб ИКС;
SHELLCODE-порты: !80
Режим работы детектора атак: IDS/IPS;
Базыправил: «Emerging Threats», «Positive Technologies Open Ruleset», «СпискиНКЦКИ».

Предмет(ы) оценивания	Объект(ы)	Показатели оценки	Критерии	Вес

	оценивания		оценки	критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики МЭ; основные требования к средствам и видам МЭ	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке детектора атак. 3. Правильность корректного применения базы сигнатур модуля.	1б 2б 2б

Задание 22.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox;VMKaliLinux, VMWindowsServer.

Время выполнения задания – 15 минут.

Текст задания:

Провести обследование подсистемы защиты сетевых взаимодействий (Penetrationtest) и анализ данных сервера:

- сканировать serverc целью определения сервисов;
- сканировать serverc целью поиска возможных учётных записей на конечном хосте.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	Средства мониторинга и анализа локальных сетей; правильность определения признаков атаки;	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления;	1. Выполнение требований задания по обследованию подсистемы защиты сетевых взаимодействий и анализу данных сервера.	2 б

ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	правильность использования правил утилиты настраиваемого сканирования Nmap	ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развитияотрасли.	2. Правильность сканирования server с помощью утилиты nmap с использованием NSE скриптов. 3. Правильность поиска возможных учётных записей на конечном хосте.	2б 1б

Задание 23.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; VMKaliLinux, VMWindowsServer.

Время выполнения задания – 15 минут.

Текст задания:

Провести обследование подсистемы защиты сетевых взаимодействий (Penetrationtest) и анализ данных сервера:

- подобрать пароль к административной учётной записи admin;
- подключиться к серверу.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Средства мониторинга и анализа локальных сетей; правильность определения признаков атаки; правильность использования правил утилиты настраиваемого сканирования Nmap	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов,	1. Выполнение требований задания по обследованию подсистемы защиты сетевых взаимодействий и анализу данных сервера. 2. Правильность сканирования server с помощью утилиты hydra/brutex. 3. Выполнение требований задания по подключению к серверу с помощью утилиты	2 б 2б 1б

ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	xfreerdp.	

Задание 24.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; VM Kali Linux, VM Windows Server, Process monitor, Microsoft Network Monitor, StealerForEducation.exe.

Время выполнения задания – 15 минут.

Текст задания:

Провести анализ вредоносного действия вируса типа Stealer.Проанализировать состояние Processmonitor. Основная задача: найти среди всех действий данного процесса информацию о файле, из которого происходит хищение информации любым из двух методов:

- метод последовательного перебора;
- разбор действий программы Processmonitor.

Файл содержит ПАРОЛИ в открытом виде. Найти сетевые адреса (IP и URL), с которыми взаимодействует исследуемый процесс.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них	Средства мониторинга и анализа локальных сетей; правильность определения признаков атаки; правильность использования действий Processmonitor, MicrosoftNetworkMonitor.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения	1. Выполнение требований задания по обследованию подсистемы защиты сетевых взаимодействий и анализу данных. 2. Правильность определения файла, из которого происходит хищение информации н сервере. 3. Выполнение требований задания по поиску сетевых адресов (IP и URL), с	2 б 2б 1б

ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	которыми взаимодействует исследуемый процесс (StealerForEducation.exe).	

Задание 25.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; VM Kali Linux, VM Windows Server, Process monitor, Microsoft Network Monitor, StealerForEducation.exe, Брандмауэр Windows.

Время выполнения задания – 15 минут.

Текст задания:

Заблокировать с помощью встроенного брандмауэра («Брандмауэр Windows в режиме повышенной безопасности» от имени Администратора) вредоносные действия вируса типа Stealer. Нужно сделать так, чтобы у процесса не было сетевой активности при повторном запуске.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	Средства мониторинга и анализа локальных сетей; правильность определения признаков атаки; правильность настроек брандмауэра Windows.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению	1. Выполнение требований задания по обследованию подсистемы защиты сетевых взаимодействий и анализу данных. 2. Выполнение требований задания по поиску сетевых адресов (IP и URL), с которыми взаимодействует исследуемый процесс (StealerForEducation.exe). 3. Правильность настроек брандмауэра Windows в режиме повышенной безопасности.	2 б 2б 1б

ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.		

Задание 26.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; BMAstra_Client_DAC_MAC.

Время выполнения: 15 минут.

Текст задания:

Авторизуйтесь в системе ВМ Astra_Client_DAC_MAC под учетной записью администратора astra-admin с высоким уровнем целостности и создайте в расположении "/home/public" папку "documents".

Для созданной папки установите следующие стандартные права доступа и дополнительные атрибуты Linux:

- Владелец – root, rwx;
- Группа владельца – root, rwx;
- Остальные – ---;
- sticky-бит.

Проверьте, что права доступа и атрибуты папки "documents" установлены верно.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	Реализация политики дискреционн ых прав доступа.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области	1. Выполнение требований задания по настройке дискреционных прав доступа. 2. Выполнение требований задания по установке стандартных прав доступа и дополнительны х атрибут Linux. 3. Правильность проведения проверки прав доступа и атрибут папки "documents".	2б 2б 1б

ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		программного обеспечения, развития отрасли.		

Задание 27.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; ВМ Astra_Client_DAC_MAC..

Время выполнения: 10 минут.

Текст задания:

Авторизуйтесь в системе ВМ Astra_Client_DAC_MAC под учетной записью администратора **astra-admin** с высоким уровнем целостности и создайте в расположении "/home/public" папку "documents".

Для папки "/home/public/documents/" установите следующие права доступа POSIX ACL и такие же права по умолчанию:

- для пользователя user1 – **rwx**;
- для пользователя user2 – **rwx**;
- для группы "office" – **r-x**.

Проверьте, что права доступа POSIX ACL и соответствующие права по умолчанию для папки "documents" установлены верно.

Завершите сеанс работы администратора, последовательно зарегистрируйтесь в системе с учетными записями **user1** / **user2** и убедитесь, что эти пользователи могут совершать разрешенные им файловые операции в папке "/home/public/documents/".

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной	Реализация политики дискреционных прав доступа.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по установке прав доступа POSIX ACL и соответствующих прав по умолчанию для папки "/home/public/documents/". 2. Правильность проведения проверки прав доступа POSIX ACL и соответствующих прав по умолчанию для папки "documents". 3. Правильность проведения проверки прав доступа для учетных записей user1,user2.	2б 2б 1б

деятельности.				

Задание 28.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_Client_SNLSP.

Время выполнения: 10 минут.

Текст задания:

Авторизуйтесь в системе ВМ Astra_Client_SNLSP под учетной записью администратора **astra-admin** с высоким уровнем целостности, запустите "Панель Безопасности SecretNetLSP".

Проверьте, что дискреционное управление доступом в SNLSP включено.

Средствами SNLSP создайте нового пользователя со следующими атрибутами:

– Имя пользователя – **user3**;
– Главная группа – **office**;
– Оболочка – **/bin/bash**;
– пароль / подтверждение – **P@ssw0rd**;
– число дней, после которых срок действия пароля истекает – **60**.

Убедитесь, что пользователь появился в системе.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация политики дискреционных прав доступа.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по установке прав доступа в SecretNetLSP. 2. Правильность использования средств SNLSP для установления прав доступа для папки "documents". 3. Правильность проведения проверки прав доступа для учетных записей user1, user3.	2б 2б 1б

Задание 29.

Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_Client_SNLSP.
Время выполнения: 10 минут.
Текст задания:
Авторизуйтесь в системе ВМ Astra_Client_SNLSP под учетной записью администратора **astra-admin** с высоким уровнем целостности, запустите "Панель Безопасности SecretNetLSP".
В расположении "/home/public" создайте папку "documents" и средствами SNLSP установите для нее следующие права доступа:
- Владелец – **root**, **rwx**;
- Группа владельца – **root**, **r-x**;
- Остальные – **r-x**;
- sticky-бит.
- для пользователя user2 – **rwx**;
- для пользователя user3 – **rwx**;
- для группы "office" – **r-x**.

Последовательно зарегистрируйтесь в системе с учетными записями **user1** / **user3** и убедитесь, что права доступа к папке "/home/public/documents/" у этих пользователей разные.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация дискреционных прав доступа в SecretNetLSP	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по установке прав доступа в SecretNetLSP. 2. Правильность использования средств SNLSP для установления прав доступа для папки "documents". 3. Правильность проведения проверки прав доступа для учетных записей user1, user3.	2б 2б 1б

Задание 30.
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_Client_SNLSP.

Время выполнения: 10 минут.

Текст задания:

Авторизуйтесь в системе ВМ Astra_Client_SNLSP под учетной записью администратора **astra-admin** с высоким уровнем целостности.

Настройте журнал событий SNLSP, связанных с изменениями доступа к объектам файловой структуры. Постройте отчет.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Настройка журнала событий SecretNetLSP	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по настройке журнала событий SecretNetLSP. 2. Правильность использования средств SNLSP для установления параметров: "Группа сообщений" – "Управление контролем доступа". 3. Выполнение требований задания по построению отчета.	2б 2б 1б

Задание 31.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_17, ВМ Astra_17_1.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd; реквизиты учетных записей пользователей samba: логины smb-user1, smb-user2 и smbadmin, пароль – P@ssw0rd.

Время выполнения: 10 минут.

Текст задания:

Сформируйте правила фильтрации так, чтобы были разрешены входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) с отслеживанием состояния соединения и блокирован весь остальной TCP/UDP-трафик с логированием событий.

Проверить действие правил.

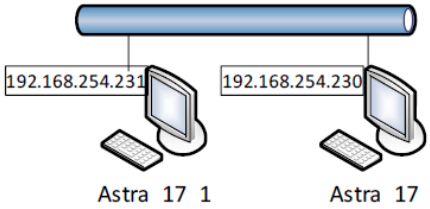

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Реализация правилафильтрации, разрешающее входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) с отслеживанием состояния соединения.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Правильность правилафильтрации, разрешающеевходящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) с отслеживанием состояния соединения 3. Правильность блокирования TCP/UDP-трафик с логированием событий.	1б 2б 2б

<u>Задание 32.</u>

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_17, ВМ Astra_17_1.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd; реквизиты учетных записей пользователей samba: логины smb-user1, smb-user2 и smbadmin, пароль – P@ssw0rd.

Время выполнения: 10 минут.

Текст задания:

- на ВМ Astra_17_1 проверить доступ к ВМ Astra_17 по SMB, по SSH, просмотреть сведения об установленных соединениях.
- на ВМ Astra_17 просмотреть записи системного журнала о заблокированных подключениях.

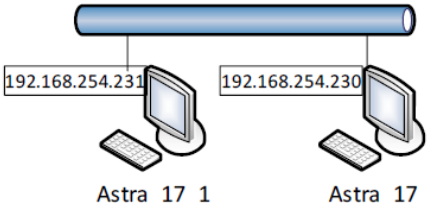

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Проверка действия настроенных правил МСЭ: на ВМ Astra_17_1 - доступ к ВМ Astra_17 по SMB, по SSH.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Правильность проверки действия настроенных правил МСЭ: на ВМ Astra_17_1 - доступ к ВМ Astra_17 по SMB, по SSH. 3. Правильность аудита записи системного журнала о заблокированны х подключениях	1б 2б 2б

Задание 33.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_17, ВМ Astra_17_1.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd; реквизиты учетных записей пользователей samba: логины smb-user1, smb-user2 и smbadmin, пароль – P@ssw0rd.

Время выполнения: 10 минут.

Текст задания:

Настроить автоматическую загрузку правил фильтрации при загрузке ОС на ВМ Astra_17:

- создать файл для сохранения правил;
- ограничить чтение файла для предотвращения атак с использованием открытых портов;
- выгрузить текущие правила iptables в файл;
- создать сценарий для выполнения в автоматическом режиме перед включением сетевого интерфейса и сделать файл сценария исполняемым.

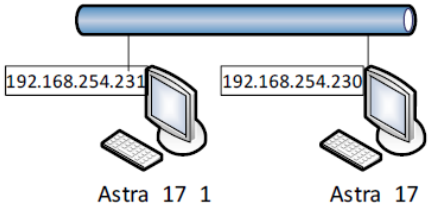

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Настройка автоматической загрузки правил фильтрации при загрузке ОС на ВМ Astra_17.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2.Реализация файла для сохранения правил фильтрации, ограничение чтения файла для предотвращения атак с использованием открытых портов. 3. Выгрузка правил iptables в файл, создание сценария для выполнения в автоматическом режиме перед включением сетевого интерфейса.	1б 2б 2б

Задание 34.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_17, ВМ Astra_17_1.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd; реквизиты учетных записей пользователей samba: логины smb-user1, smb-user2 и smbadmin, пароль – P@ssw0rd.

Время выполнения: 10 минут.

Текст задания:

На ВМ Astra_17 настроить правила МСЭ в SecretNetLSP: сформировать правила фильтрации так, чтобы были разрешены входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) и блокирован весь остальной TCP/UDP-трафик с логированием событий.

Проверить действие правил.

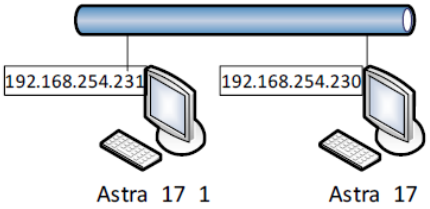

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Настройка разрешающих правил МСЭ в Secret-NetLSP. Проверка действия правил. МСЭ в SecretNetLSP.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2.Реализация правила фильтрации, разрешающих входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) и блокирование TCP/UDP-трафик с логированием событий. 3. Проверка действия правил. МСЭ в SecretNetLSP.	1б 2б 2б

Задание 35.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_17, ВМ Astra_17_1.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd; реквизиты учетных записей пользователей samba: логины smb-user1, smb-user2 и smbadmin, пароль – P@ssw0rd.

Время выполнения: 10 минут.

Текст задания:

На ВМ Astra_17 настроить правила МСЭ в SecretNetLSP: сформировать правила фильтрации так, чтобы были разрешены входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) и блокирован весь остальной TCP/UDP-трафик с логированием событий.

Проверить действие правил.

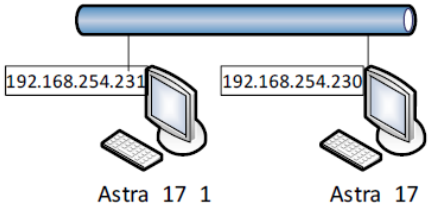

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Настройка запрещающих правил МСЭ в Secret-NetLSP. Проверка действия правил. МСЭ в SecretNetLSP.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2.Реализация правила фильтрации, запрещающих входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138). 3. Проверка действия правил. МСЭ в SecretNetLSP.	1б 2б 2б

Задание 36.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_17, ВМ Astra_17_1.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd; реквизиты учетных записей пользователей samba: логины smb-user1, smb-user2 и smbadmin, пароль – P@ssw0rd.

Время выполнения: 10 минут.

Текст задания:

В журнале SNLSP найдите события, связанные с работой ПМЭ SN LSP:

- события системного журнала об управлении ПМЭ;
- события журнала аудита о срабатывании правил ПМЭ.

Проведите запись в файл правил ПМЭ.

Убедитесь, что архивный файл резервной копии сохранен ("<имя_файла>.tar.gz").

Предмет(ы) оценивания	Объект(ы)	Показатели оценки	Критерии	Вес

	оценивания		оценки	критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей. ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Анализ событий системного журнала об управлении ПМЭ, анализ событий журнала аудита о срабатывании правил ПМЭ.	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	1. Выполнение требований задания по реализации политики МЭ. 2. Правильность проверки событий системного журнала об управлении ПМЭ и событий журнала аудита о срабатывании правил ПМЭ. 3. Создание резервной копии архивного файла.	1б 2б 2б

Задание 37.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, OracleVMVirtualBox; ВМ Astra_Client_SNLSP.

Время выполнения: 10 минут.

Текст задания:

Авторизуйтесь в системе ВМ Astra_Client_SNLSP под учетной записью администратора **astra-admin** с высоким уровнем целостности.

Настройте журнал событий SNLSP, связанных с изменениями доступа к объектам файловой структуры. Постройте отчет.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи. ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 3.3. Обеспечивать безопасное администрирование систем и сетей.	Настройка журнала событий SecretNetLSP	ОПОР 1 - Четкое понимание проблеминформационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средствобеспечения	1. Выполнение требований задания по настройке журнала событий SecretNetLSP. 2. Правильность использования средств SNLSP для установления параметров: "Группа	2б 2б

ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. ОК5. Использовать информационно-коммуникационные технологии в профессиональной деятельности. ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий. ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.		информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; ОПОР 13 - Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональныхзадач в области обеспечениябезопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасностисетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	сообщений" – "Управление контролем доступа". 3. Выполнение требований задания по построению отчета.	1б

Составила Грубник Е.М.