СОГЛАСОВАНО
Начальник отдела защиты информации
Министерства цифрового развития
Смоленской области
_____ Калугин А.Н.
«31» 08 2023 г.

Утверждаю
Зам. директора по учебной работе
_____ И.В. Иванешко
«31» 08 2023г.

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЭКЗАМЕНУ КВАЛИФИКАЦИОННОМУ)

по профессиональному модулю ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

Специальность 11.02.15 Инфокоммуникационные сети и системы связи

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
5 «отлично»	Общее количество набранных баллов (по весу критерия) по всем двум заданиям билета 9-10.
4 «хорошо»	Общее количество набранных баллов (по весу критерия) по всем двум заданиям билета 7-8.
3 «удовлетворительно»	Общее количество набранных баллов (по весу критерия) по всем двум заданиям билета 5-6.
2 «неудовлетворительно»	Общее количество набранных баллов (по весу критерия) по всем двум заданиям билета менее 5.

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):

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской

	Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

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; Oracle VM VirtualBox; VM ИКС.
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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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. Правильность настройки модуля Fail2ban. 3. Правильность решения задания: при авторизации после 3 неудачных попыток учетная запись блокируется.	2б 2б 1б

Задание 2.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 3.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 4.
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.
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) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований	1б 2б

информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа к Web серверу.	2б

Задание 5.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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	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 FTP серверу.	1б 2б 2б

контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		способов решения профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 6.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 почтовому DNS серверу.	1б 2б 2б

Задание 7.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 серверу IP-телефонии.	1б 2б 2б

Задание 8.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 веб-авторизации	1б 2б 2б

Задание 9.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять,	1. Выполнение требований задания по реализации политики МЭ.	1б

методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения доступа для программы авторизации	2б 2б

Задание 10.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи;	1. Выполнение требований задания по реализации политики МЭ. 2. Выполнение требований задания по настройке адресов и подсетей. 3. Правильность создания необходимых правил для разрешения	1б 2б 2б

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	доступа к локальному DNS серверу.	

Задание 11.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией	Реализация политики МЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач	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

на государственном и иностранном языках.		по обеспечению безопасности сетей 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 12.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; Oracle VM VirtualBox; VM ИКС.

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;

Базы правил: «Emerging Threats», «Positive Technologies Open Ruleset», «Списки НКЦКИ».

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики IDS/IPS.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 13.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; VM Kali Linux, VM Server.

Время выполнения задания – 15 минут.

Текст задания:

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

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

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Средства мониторинга и анализа локальных сетей; правильность использования правил утилиты настраиваемого сканирования Nmap.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 обследованию подсистемы защиты сетевых взаимодействий и анализу данных сервера. 2. Правильность сканирования server с помощью утилиты nmap с использованием NSE скриптов. 3. Правильность поиска возможных учётных записей на конечном хосте.	2 б 2б 1б

Задание 14.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Правильность определения класса защищенности автоматизированной системы обработки данных, грамотное использование нормативных документов	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения информационной безопасности (программных и программно-аппаратных); 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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

Задание 15.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях	Правильность определения класса защищенности средств вычислительной техники, грамотное использование	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их	1. Выполнение требований задания по определению программных и технических частей систем обработки данных. 2. Правильность определения класса	2б

и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	нормативных документов	проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.	защищенности средств вычислительной техники, грамотное использование нормативных документов 3. Грамотный выбор конкретного подхода к определению класса защищенности средств вычислительной техники.	2б 1б

Задание 16.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК; www.Ideco.ru (вход через личный кабинет).

Время выполнения: 15 минут.

Текст задания:

Проверить защиту корпоративной сети, используя тестирование Ideco UTM: 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 почте в известных базах данных хакеров.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы	Грамотно проведенное тестирование корпоративной сети	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи;	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

решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. 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.

Время выполнения: 15 минут.

Текст задания:

Злоумышленники зашифровали файлы корпоративного компьютера трояном семейства Yanluowang. Зашифрованные критически важные данные необходимо восстановить. Предложите алгоритм действий в условиях произошедшего вирусозависимого инцидента.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные	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 проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск	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

технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		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 18.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Dr.Web vxCube.

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) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Выбор механизмов тестирования антивирусной защиты информационной системы	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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 19.

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 экран 4-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 критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Грамотный выбор МЭ, сформулированные требования к сертифицированным межсетевым экранам	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 обоснованию выбора МЭ. 2. Выполнение требований задания к средствам обеспечения безопасности информационной системы предприятия, содержащей сведения, отнесенные к государственной тайне. 3. Рациональность распределения времени на описание выбранного решения.	2 2 1

Задание 20.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Грамотный выбор средств антивирусной защиты, сформулированные требования к сертифицированным средствам антивирусной защиты, понимание классификации средств антивирусной защиты.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 обоснованию выбора средств антивирусной защиты. 2. Выполнение требований задания к средствам обеспечения безопасности информационных технологий по применению средств антивирусной защиты. 3. Рациональность распределения времени на описание выбранного решения.	2 2 1

Задание 21.

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 вторжений 1 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать	Грамотный выбор СОВ, сформулированные требования к сертифицированным СОВ, понимание	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать	1. Выполнение требований задания по обоснованию выбора СОВ. 2. Выполнение требований задания	2 2

комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	спецификации профилей защиты	угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	к средствам обеспечения безопасности информационных технологий по уровню доверия, требования к СОВ выбранного класса защиты 3. Рациональность распределения времени на описание выбранного решения.	1

Задание 22.

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 проводить 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач	Грамотное использование средств оценки уязвимостей	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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	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

профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		результате освоения тем, разделов, дисциплин, МДК, модулей. ОПОР 14 - Выбор и применение методов и способов решения профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 23.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; VM Kali Linux, VM Server.

Время выполнения задания – 15 минут.

Текст задания:

Провести обследование подсистемы защиты сетевых взаимодействий (Penetration test) 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на	Средства мониторинга и анализа локальных сетей.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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 xfreerdp.	2 б 2б 1б

государственном и иностранном языках.		программными средствами. ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.		

Задание 24.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

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

Время выполнения задания – 15 минут.

Текст задания:

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

- метод последовательного перебора;
- разбор действий программы Process monitor.

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Средства мониторинга и анализа локальных сетей.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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 которыми взаимодействует исследуемый процесс (StealerForEducation.exe).	2 б 2б 1б

Задание 25.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; VM Kali Linux, VM Windows Server, Process monitor, Network Monitor, StealerForEducation.exe.
Время выполнения задания – 15 минут.
Текст задания:
Заблокировать 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Средства мониторинга и анализа локальных сетей; правильность определения признаков атаки; правильность настроек брандмауэра.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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 в режиме повышенной безопасности.	2 б 2б 1б

Задание 26.
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, Oracle VM VirtualBox; ВМ Astra_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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация политики дискреционны х прав доступа.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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

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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты	Реализация политики дискреционн ых прав доступа.	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной	1. Выполнение требований задания по установке прав доступа POSIX ACL и	2б

информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	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 1б

Задание 28.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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 Secret Net LSP".

Проверьте, что дискреционное управление доступом в SN LSP включено.

Средствами SN LSP 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	Реализация политики дискреционных прав доступа.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в	1. Выполнение требований задания по установке прав доступа в Secret Net LSP. 2. Правильность использования средств SN LSP для установления прав доступа для папки "documents". 3. Правильность	2б 2б 1б

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	проведения проверки прав доступа для учетных записей user1, user3.	

Задание 29.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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 Secret Net LSP".

В расположении "/home/public" создайте папку "documents" и средствами SN LSP 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	Реализация дискреционных прав доступа в Secret Net LSP	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения информационной безопасности (программных и программно-аппаратных); ОПОР 7 - Владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи;	1. Выполнение требований задания по установке прав доступа в Secret Net LSP. 2. Правильность использования средств SN LSP для установления прав доступа для папки "documents". 3. Правильность проведения проверки прав	2б 2б 1б

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	доступа для учетных записей user1, user3.	

Задание 30.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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 SN LSP, 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной	Настройка журнала событий Secret Net LSP	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения	1. Выполнение требований задания по настройке журнала событий Secret Net LSP. 2. Правильность использования средств SN LSP для установления параметров: "Группа сообщений" – "Управление контролем доступа". 3. Выполнение требований задания по построению отчета.	2б 2б 1б

документацией на государственном и иностранном языках.		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 31.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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.

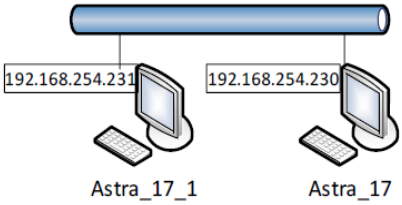

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Реализация правила фильтрации, разрешающее входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) с отслеживанием состояния соединения.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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. Правильность правила фильтрации, разрешающее входящие 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

		ОПОР 23 - Анализ инноваций в области программного обеспечения, развития отрасли.		

Задание 32.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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.

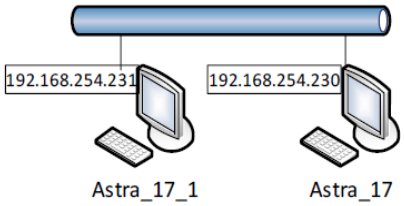

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Проверка действия настроенных правил МСЭ: на ВМ Astra_17_1 - доступ к ВМ Astra_17 по SMB, по SSH.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 заблокированных подключениях	1б 2б 2б

Задание 33.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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.

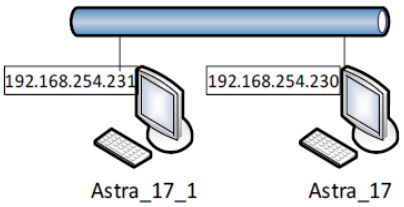

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Настройка автоматической загрузки правил фильтрации при загрузке ОС на ВМ Astra_17.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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, Oracle VM VirtualBox; 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 Secret Net LSP: 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.

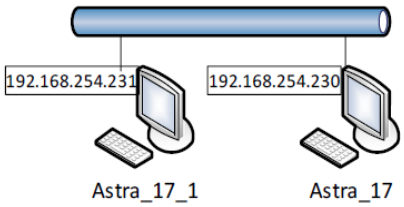

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Настройка разрешающих правил МСЭ в Secret Net LSP. Проверка действия правил. МСЭ в Secret Net LSP.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 Secret Net LSP.	1б 2б 2б

<u>Задание 35.</u>
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; 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 Secret Net LSP: 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.

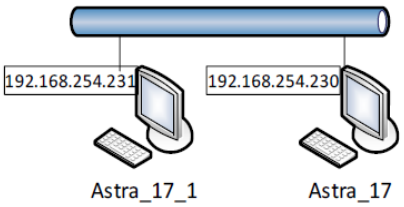

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Настройка запрещающих правил МСЭ в Secret Net LSP. Проверка действия правил. МСЭ в Secret Net LSP.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 Secret Net LSP.	1б 2б 2б

<u>Задание 36.</u>

Инструкция:

Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, Oracle VM VirtualBox; 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 SN LSP 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) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Анализ событий системного журнала об управлении ПМЭ, анализ событий журнала аудита о срабатывании правил ПМЭ.	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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, Oracle VM VirtualBox; 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 SN LSP, 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. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.	Настройка журнала событий Secret Net LSP	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и	1. Выполнение требований задания по настройке	2б

ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	журнала событий Secret Net LSP. 2. Правильность использования средств SN LSP для установления параметров: "Группа сообщений" – "Управление контролем доступа". 3. Выполнение требований задания по построению отчета.	2б 1б

Задание 38.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, VMware Workstation; стенд АПКШ "Континент".

Время выполнения: 15 минут.

Текст задания:

Настроить правило фильтрации, разрешающее прохождение трафика между компьютерами из внутренних сетей, защищаемых разными криптошлюзами.

Администратору необходимо обеспечить возможность подключаться пользователю из одной защищаемой сети к веб-серверу, который находится в защищаемой сети за другим КШ. На учебном стенде роль веб-сервера будет выполнять виртуальная машина ARM, а роль пользователя – ВМ WS1 (см. рис. 1).

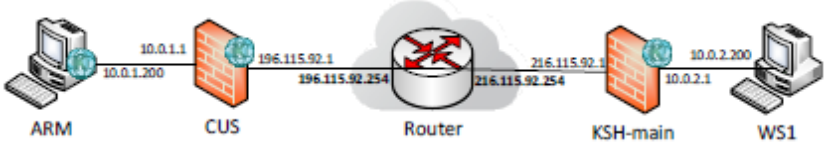

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с	Реализация правила фильтрации,	ОПОР 1 - Четкое понимание проблем информационной безопасности в	1. Выполнение требований задания по	1б

использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	разрешающее прохождение IP трафика между хостами, находящимися в сегментах сети, защищаемых разными криптошлюзами	телекоммуникационных системах и сетях связи; ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами.	реализации политики МЭ. 2. Правильность правила фильтрации, обеспечивающего прохождение IP трафика по протоколу http от WS1 к ARM. 3. Правильность проведения проверки подключения из одной защищаемой сети к веб серверу в другой защищаемой сети.	 2б 2б

Задание 39.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, VMware Workstation; стенд АПКШ "Континент".

Время выполнения: 15 минут.

Текст задания:

Администратору необходимо организовать VPN-соединение через сеть общего доступа между пользователями, находящимися в защищаемых сетях за разными криптошлюзами для обмена конфиденциальной информацией. На тестовом стенде роли пользователей за разными КШ выполняют виртуальные машины ARM и WS1, а роли криптошлюзов – виртуальные машины CUS и KSH_main (см. рис. 1).

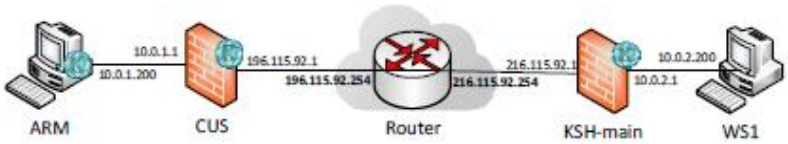

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и	Организация	ОПОР 1 - Четкое понимание проблем	1. Выполнение	1б

уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	L3VPN	информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами.	требований задания по организации L3VPN. 2. Правильность написания правила фильтрации, разрешающего прохождение трафика между виртуальными машинами ARM и WS1. 3. Правильность настройки связи между криптошлюзами CUS и KSH_main. 4. Правильность проведения проверки передачи трафика между КШ с ЦУС и KSH_main.	 1б 2б 1б

Задание 40.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, VMware Workstation; стенд АПКШ "Континент".

Время выполнения: 15 минут.

Текст задания:

Чтобы обеспечить обмен информацией между двумя удаленными сегментами одной сети администратору необходимо организовать защищенное соединение между ними. На учебном стенде роли криптокоммутаторов "Континент" выполняют виртуальные машины КК1 и КК2. Канал шифрования проверяется путем передачи трафика между виртуальными машинами АР и WS1. Рабочее место администратора – ВМ ARM (см. рис. 1).

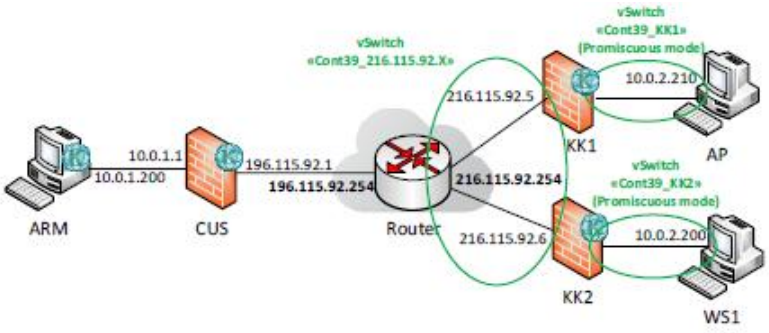

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы	Организация L2VPN	ОПОР 1 - Четкое понимание проблем информационной безопасности в телекоммуникационных системах и сетях связи;	1. Выполнение требований задания по	1б

анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		ОПОР 2 - Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; ОПОР 3 - Выбор механизмов и средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами.	организации L2VPN. 2. Правильность организации защищенного соединения между двумя сегментами сети и настройки канала шифрования между ними. 3. Правильность проведения проверки канала шифрования с помощью утилиты ping между виртуальными машинами AP и WS1.	2б 2б

Задание 41.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, VMware Workstation; стенд АПКШ "Континент".

Время выполнения: 15 минут.

Текст задания:

Администратору необходимо организовать VPN-канал для доступа удаленного пользователя к веб-серверу, который находится в защищаемой сети за КШ. На учебном стенде роль удаленного пользователя выполняет ВМ AP, а роль веб-сервера – ВМ ARM (см. рис. 1).

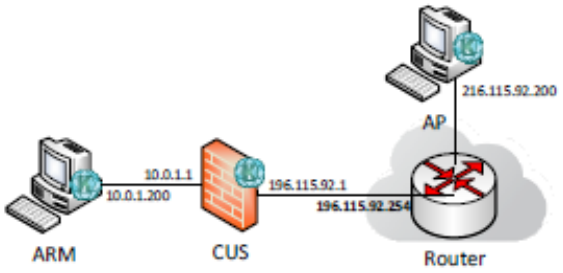

Рис. 1 Сетевая среда по условию задания

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять	Организация VPN-канала для доступа удаленного пользователя	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения информационной безопасности (программных и	1. Выполнение требований задания по организации VPN-канала для доступа удаленного пользователя. 2. Правильность настройки	1б 2б

текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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.	сервера доступа и VPN-канала для доступа удаленного пользователя к веб-серверу в защищаемой сети за КШ с ЦУСом. 3. Правильность подключения удаленного пользователя к защищаемой сети.	2б

Задание 42.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; VM Server, файл-дешифратора.

Время выполнения задания – 15 минут.

Текст задания:

Проанализировать структуру файла ***crypt.py*** (шифровальщик) и определить:

- файл (*.txt), зашифрованный этим алгоритмом.
- в каком месте файла расположен ключ для расшифровки;
- каким алгоритмом шифрования зашифрован файл.

Использовать скрипт (файл-дешифратор) для расшифровки файла, с целью получения *«пароля»*, находящегося в нём.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать	Организация поиска вредоносного ПО, поиск источника заражения в логах	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных	1. Грамотный анализ структуры файла crypt.py.. 2. Правильность определения пароля для расшифровки файла и расшифрованного пароля. 3. Правильность определения «секретного» сообщения, передаваемого malware.exe при установлении подключения к control.exe	1 б 2б 2б

современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.		задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей связи. ОПОР 16 - Эффективный поиск необходимой информации для решения задач в области сетевой безопасности. ОПОР 18 - Работа с различными программно-аппаратными и программными средствами.		

Задание 43.

Инструкция:

Внимательно прочитайте задание.

Вы можете пользоваться:

Оборудование, ПО: ПК, Oracle VM VirtualBox; ВМ Astra_17, Сканер-ВС 6, сервер tomcat.

реквизиты учетной записи администратора: логин – astra-admin, пароль – P@ssw0rd.

Время выполнения: 15 минут.

Текст задания:

Провести анализ уязвимостей сервера tomcat с помощью Сканер-ВС 6 по результатам сетевого сканирования и инвентаризации.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Грамотно проведенное тестирование сервера	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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 44.

Инструкция:

Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, Oracle VM VirtualBox; ВМ Astra_17, Сканер-ВС 6, 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.
Текст задания:
Провести контроль дискреционных и мандатных полномочий доступа локальных пользователей к объектам файловой системы ВМ Astra_17_1.

Предмет(ы) оценивания	Объект(ы) оценивания	Показатели оценки	Критерии оценки	Вес критерия
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Грамотно проведенное тестирование дискреционных и мандатных полномочий доступа локальных пользователей	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 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 45.
Инструкция:
Внимательно прочитайте задание.
Вы можете пользоваться:
Оборудование, ПО: ПК, Oracle VM VirtualBox; ВМ Astra_17, Сканер-ВС 6, 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.
Текст задания:
Провести проверку эффективности работы средств гарантированного уничтожения информации, осуществляющих оперативное удаление данных на ВМ Astra_17_1.

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

ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Грамотно проведенная проверка эффективности работы средств гарантированного уничтожения информации	ОПОР 1 - Четкое понимание проблем информационной 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 средств обеспечения 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 профессиональных задач в области обеспечения безопасности сетей связи. ОПОР 15 - Решение стандартных и нестандартных профессиональных задач по обеспечению безопасности сетей 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 проведению проверки эффективности работы средств гарантированного уничтожения информации. 2. Грамотное владение сервисами, обеспечивающими проведение проверки механизма очистки оперативной памяти. 3. Грамотный выбор механизмов и средств для проведения проверки механизма очистки оперативной памяти.	2б 2б 1б

Составила Грубник Е.М.