ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА БАЗОВОГО УРОВНЯ

Том 1

(Комплект оценочной документации)

Код и наименование профессии (специальности) среднего профессионального образования	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Наименование квалификации	техник по защите информации

Федеральный государственный образовательный стандарт среднего профессионального образования по профессии (специальности) среднего профессионального образования (ФГОС СПО):	ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Минобрнауки РФ от 09.12.2016 №1553
Код комплекта оценочной документации	КОД 10.02.05-2023

СТРУКТУРА КОМПЛЕКТА ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ

1. Комплекс требований для проведения демонстрационного экзамена.
2. Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания.
3. План застройки площадки демонстрационного экзамена.
4. Требования к составу экспертных групп.
5. Инструкции по технике безопасности.
6. Образец задания.

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

Сокращение	Расшифровка
ОМ	Оценочный материал
КОД	Комплект оценочной документации
ЦПДЭ	Центр проведения демонстрационного экзамена
СПО	Среднее профессиональное образование
ФГОС СПО	Федеральный государственный образовательный стандарт среднего профессионального образования
ОК	Общая компетенция
ПК	Профессиональная компетенция
ГИА	Государственная итоговая аттестация

1. КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ

Настоящий КОД предназначен для организации и проведения аттестации обучающихся по программам среднего профессионального образования в форме демонстрационного экзамена базового уровня.

1.1. Комплекс требований для проведения демонстрационного экзамена

Организационные требования[1]:

1. Демонстрационный экзамен проводится с использованием КОД, включенных образовательными организациями в программу ГИА.
2. Задания демонстрационного экзамена доводятся до главного эксперта в день, предшествующий дню начала демонстрационного экзамена.
3. Образовательная организация обеспечивает необходимые технические условия для обеспечения заданиями во время демонстрационного экзамена выпускников, членов ГЭК, членов экспертной группы.
4. Демонстрационный экзамен проводится в ЦПДЭ, представляющем собой площадку, оборудованную и оснащенную в соответствии с КОД.
5. ЦПДЭ может располагаться на территории образовательной организации, а при сетевой форме реализации образовательных программ — также на территории иной организации, обладающей необходимыми ресурсами для организации ЦПДЭ.
6. Выпускники проходят демонстрационный экзамен в ЦПДЭ в составе экзаменационных групп.
7. Образовательная организация знакомит с планом проведения демонстрационного экзамена выпускников, сдающих демонстрационный экзамен, и лиц, обеспечивающих проведение демонстрационного экзамена, в срок не позднее чем за 5 рабочих дней до даты проведения экзамена.
8. Количество, общая площадь и состояние помещений, предоставляемых для проведения демонстрационного экзамена, должны обеспечивать проведение демонстрационного экзамена в соответствии с КОД.
9. Не позднее чем за один рабочий день до даты проведения демонстрационного экзамена главным экспертом проводится проверка готовности ЦПДЭ в присутствии членов экспертной группы, выпускников, а также технического эксперта, назначаемого организацией, на территории

[1] Отдельные положения Порядка проведения государственной итоговой аттестации по программам СПО, утвержденного приказом Министерства просвещения Российской Федерации от 08.11.2021 № 800.

которой расположен ЦПДЭ, ответственного за соблюдение установленных норм и правил охраны труда и техники безопасности.

10. Главным экспертом осуществляется осмотр ЦПДЭ, распределение обязанностей между членами экспертной группы по оценке выполнения заданий демонстрационного экзамена, а также распределение рабочих мест между выпускниками с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между выпускниками фиксируются главным экспертом в соответствующих протоколах.

11. Выпускники знакомятся со своими рабочими местами, под руководством главного эксперта также повторно знакомятся с планом проведения демонстрационного экзамена, условиями оказания первичной медицинской помощи в ЦПДЭ. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

12. Допуск выпускников в ЦПДЭ осуществляется главным экспертом на основании документов, удостоверяющих личность.

13. Образовательная организация обязана не позднее чем за один рабочий день до дня проведения демонстрационного экзамена уведомить главного эксперта об участии в проведении демонстрационного экзамена тьютора (ассистента).

Требование к продолжительности демонстрационного экзамена

Продолжительность демонстрационного экзамена (не более)[2]	**3:00:00**

Требования к содержанию[3]

№ п/п	**Модуль задания[4]** (вид деятельности, вид профессиональной деятельности)	**Перечень оцениваемых ПК (ОК)**	**Перечень оцениваемых умений и навыков / практического опыта**
1	2	3	4
1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК. Производить установку и настройку компонентов, автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование,

[2] В академических часах

[3] В соответствии с ФГОС СПО.

[4] Наименование модуля задания совпадает с видом профессиональной деятельности (ФГОС СПО).

		ПК. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам. иметь практический опыт в: эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности; администрировании автоматизированных систем в защищенном исполнении;

			установке компонентов систем защиты информации автоматизированных информационных систем.
2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	уметь: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. иметь практический опыт в: установке и настройке программных средств защиты информации; тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

Требования к оцениванию

Максимально возможное количество баллов	**100**

№ п/п	**Модуль задания** (вид деятельности, вид профессиональной деятельности)	**Критерий оценивания**[5]	**Баллы**
1	2	3	4
1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Установка и настройка компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации. Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	50
2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Установка и настройка отдельных программных, программно-аппаратных средств защиты информации Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	50
Итого			**100**

[5] Формулировка критерия оценивания совпадает с наименованием профессиональной (общей) компетенции и начинается с отглагольного существительного.

Рекомендуемая схема перевода результатов демонстрационного экзамена из стобалльной шкалы в пятибалльную:

Оценка (пятибалльная шкала)	**«2»**	**«3»**	**«4»**	**«5»**
1	2	3	4	5
Оценка в баллах (стобалльная шкала)	0,00 – 19,99	20,00 – 39,99	40,00 – 69,99	70,00 - 100,00

1.2. Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания

Перечень оборудования

№ п/п	Наименование оборудования	Минимальные характеристики
1	2	3
1	ПК или ноутбук	Процессор не менее 3,2 ГГц с поддержкой виртуализации или аналог, не менее 6 физических ядер не менее 12 потоков, не менее 24 ГБ ОЗУ, не менее 480 ГБ SSD со свободным местом не менее 200 ГБ, не менее 100 ГБ свободного места на этом же или дополнительных носителях (HDD/SSD) для хранения резервных образов, в случае ноутбука необходим дополнительный монитор, ОС с графическим интерфейсом, ПО для виртуализации, офисный пакет, тестовый редактор, браузер, ssh-клиент, sftp/scp-клиент, ftp-клиент, архиватор, программа просмотра pdf, ПО для генерации сертификатов
2	Монитор	не менее 20" и разрешением не менее 1920×1080 пкс
3	Клавиатура	На усмотрение организатора
4	Мышь компьютерная	На усмотрение организатора
5	Носитель информации	Не менее 1ГБ
6	Виртуальная машина (сервер DLP)	Предустановленная виртуальная машина совместимая с компонентами DLP системы и запущенной работоспособной серверной частью DLP системы
7	Виртуальная машина (контроллер домена)	Предустановленная виртуальная машина с преднастроенным доменом, с внесенными пользователями домена, предустановленым и настроенным DNS сервером
8	Виртуальная машина (сервер)	Предустановленная виртуальная машина с возможностью установки MSI пакетов, офисный пакет, текстовый редактор, браузер,

		ssh-клиент, scp-клиент, ftp-клиент, архиватор, программа просмотра pdf
9	Виртуальная машина (клиент)	Предустановленная виртуальная машина с возможностью установки MSI пакетов, офисный пакет, текстовый редактор, браузер, ssh-клиент, scp-клиент, ftp-клиент, архиватор, программа просмотра pdf
10	Стол	Не менее 1000х700
11	Стул со спинкой	На колесиках, на усмотрение организатора
12	Огнетушитель (1шт)	Огнетушитель порошковый
13	Аптечка (1шт)	Аптечка первой медицинской помощи, СанПин 2.1.3684-21
14	Урна	Пластик, вместимость не менее 5 литров.

Перечень инструментов

№ п/п	Наименование инструментов	Минимальные характеристики
1	2	3
-	-	-
-	-	-

Перечень расходных материалов

№ п/п	Наименование расходных материалов	Минимальные характеристики
1	2	3
1	Ручка	Синяя, Шариковая или гелевая
2	Файлы прозрачные А4	Пачка 100 шт
3	Бумага	А4, 500 листов, плотность не менее 80г/м2
4	Скотч прозрачный широкий	На усмотрение организатора, не менее 10 м
5	Папка-сшиватель	До 30 файлов, на усмотрение организатора

1.3. План застройки площадки демонстрационного экзамена

План застройки площадки представлен в приложении к настоящему тому № 1 оценочных материалов демонстрационного экзамена базового уровня.

Требования к застройке площадки

№ п/п	Наименование	Технические характеристики
1	2	3
1.	Вентиляция	Норма воздухообмена из расчета на 1 человека в час: 20 м3/ч для аудиторий и учебных классов

2.	Полы	Выполнены из материалов допускающих влажную уборку и дезинфекцию. Не допускается скольжение
3.	Освещение	Уровни искусственной освещенности кабинетах информатики не менее - 300 лк.
4.	Электричество	Необходимо подключение не менее 3 розеток 220В к каждому месту, не менее 0,5КВт/место Необходимо подключение не менее 1 точки локальной сети в случае с 1 компьютером или коммутатором на каждом рабочем месте, либо не менее 2 точек в случае с 1 компьютером и 1 ноутбуком; все кабели сведены в серверную или коммутатор на площадке, рекомендуется единая локальная сеть с доступом к ней экспертов
5.	Температура	Min. и max. t воздуха – 16°С и 22°С.

1.4. Требования к составу экспертных групп

Количественный состав экспертной группы определяется образовательной организацией, исходя из числа сдающих одновременно демонстрационный экзамен выпускников. Один эксперт должен иметь возможность оценить результаты выполнения задания выпускников в полной мере согласно критериям оценивания.

Количество главных экспертов на демонстрационном экзамене	1
Минимальное (рекомендованное) количество экспертов на 1 выпускника	1
Минимальное (рекомендованное) количество экспертов на 5 выпускников	3

1.5. Инструкция по технике безопасности

1. Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, выпускников с требованиями охраны труда и безопасности производства.

2. Все участники демонстрационного экзамена должны соблюдать установленные требования по охране труда и производственной безопасности, выполнять указания технического эксперта по соблюдению указанных требований.

Инструкция:

Запрещается находиться возле ПК в верхней одежде, принимать пищу и курить, употреблять во время выполнения задания алкогольные напитки, а также приходить на площадку в состоянии алкогольного, наркотического или другого опьянения.

В течение всего времени выполнения задания со средствами компьютерной и оргтехники участник экзамена обязан:

- содержать в порядке и чистоте рабочее место;
- следить за тем, чтобы вентиляционные отверстия устройств ничем не были закрыты;
- выполнять требования инструкции по эксплуатации оборудования;
- соблюдать, установленные расписанием, перерывы в выполнении задания, выполнять рекомендованные физические упражнения.

Участнику запрещается во время выполнения задания:

- отключать и подключать интерфейсные кабели периферийных устройств если это не указано в задании;
- класть на устройства средств компьютерной и оргтехники бумаги, папки и прочие посторонние предметы;
- прикасаться к задней панели системного блока (процессора) при включенном питании;
- отключать электропитание во время выполнения программы, процесса;
- допускать попадание влаги, грязи, сыпучих веществ на устройства средств компьютерной и оргтехники;
- производить самостоятельно вскрытие и ремонт оборудования;
- работать со снятыми кожухами устройств компьютерной и оргтехники;
- располагаться при работе на расстоянии менее 50 см от экрана монитора.

Продолжительность работы на ПК без регламентированных перерывов не должна превышать 1-го часа. Во время регламентированного перерыва с целью снижения нервно-эмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений. При неисправности инструмента и оборудования – прекратить выполнение задания и сообщить об этом Эксперту, а в его отсутствие заместителю главного Эксперта.

1.6. Образец задания

Описание общих требований
В компании «SoC» возникла необходимость внедрения DLP системы для лучшей защиты корпоративной информации и предотвращения утечек данных. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием. Серверные компоненты установлены, сетевые интерфейсы настроены. Подготовлены следующие виртуальные машины для дальнейшей работы: • Контроллер домена; • DLP сервер установлен, активирована лицензия, есть LDAP синхронизация; • Виртуальная машина с установленным сервером агентского мониторинга; • Виртуальная машина «нарушителя» в домене (1 шт).

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.
При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и/или документацией на компьютерах и/или в общем сетевом каталоге. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания.

Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

При выполнении задания модуля необходимо достичь следующих целей:
1. Настроенный контроллер домена.
2. Работоспособный сервер мониторинга сетевого трафика.
3. Установленный и работоспособный сервер агентского мониторинга.
4. Установленные и работоспособные агент мониторинга на клиентском устройстве.

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например, «Задание_5_копирование.jpg». Все скриншоты и отчеты сохраняются на рабочий стол физического компьютера в один каталог или документ (важно соблюдать последовательность заданий). При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна. Не стоит вырезать только маленький кусочек (например, сообщение о событии), т. к. это не будет являться явным подтверждением работы.
Допускается последующее выделение рамкой, стрелкой или иным способом результата работы.

Задание модуля 1:

Задача 1: Настройка контроллера домена
Создать подразделение “DemoExam” в контроллере домена.
Внутри созданного подразделения “DemoExam” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:
- Логин: web-officer, пароль: xxXX3344, права пользователя домена;
- Логин: ldap-sync, пароль: xxXX3344, права пользователя домена;
- Логин: device-officer, пароль: xxXX3344, права администратора домена и локального администратора;
- Логин: violator, пароль xxXX3344, права пользователя домена.

Задача 2: Настройка DLP сервера
DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен:
- необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случае несовпадений настроить DNS правильно;
- синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-sync;
- для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена web-officer с полными правами системы.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

Задача 3: Установка и настройка сервера агентского мониторинга
Используя виртуальную машину агентского мониторинга:

- необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя device-officer (важно);
- после входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “DemoExam” на домене;
- установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя QWEasd123;
- установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД;
- при установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: web-officer с паролем QWEasd123;
- синхронизировать каталог пользователей и компьютеров с контроллером домена.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие данные, измененные вами, в текстовом файле «отчет.txt» с на рабочем столе компьютера.

Задача 4: Установка агента мониторинга на машине нарушителя

Используя виртуальную машину нарушителя:

- необходимо ввести клиентскую машину в домен, после перезагрузки войти в систему от ранее созданного пользователя violator;
- после входа в систему необходимо переместить введённый в домен компьютер в ранее созданное подразделение “DemoExam” на домене.

На машину нарушителя (violator) средствами групповых политик или сервера мониторинга установить агент мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального).

Ручная установка с помощью создания и переноса любым способом пакета установки является некорректным выполнением задания.

В случае проблем при установке компонентов стоит проверить настройки брандмауэра и DNS.

Задача 5: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности не более 1 года, длине ключа не менее 2048 бит и т. п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

корневой root-сертификат (ca);

серверный (server) сертификат;

по желанию допускается использование пользовательского и промежуточного сертификата.

Дополнительная информация сертификатов должна включать в себя:

Страна: RU.

Город: Moscow.

Компания (и иные дополнительные поля): DemoExam.

Отдел: SoC.

Пароли ключей (если применимо): QWEasd123.

Остальные поля заполняются самостоятельно.

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети.

В случае невозможности — это сделать, установить сертификат на машину домена и отобразить это в отчете.
Итоговый результат должен включать:

- Дерево из сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе в каталоге «Сертификаты».
- Содержимое команд по генерации ключей и сертификатов в текстовом файле «сертификаты.txt» на рабочем столе с комментариями.
- Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).
- Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации и т. п.

Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами

При выполнении задания модуля необходимо достичь следующих целей:
1.Настройка сервера агентского мониторинга для правильной работы системы.
2. Разработка политик и правил безопасности, предотвращающих утечки или попытку использования устройств и сервисов пользователями.
3. Разработка групповых политик домена для ограничения пользовательских действий.
4. Проверка работоспособности политик и правил безопасности

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании).
Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат. Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна.
Выполнение отдельных заданий необходимо подтвердить скриншотом. В этом случае необходимо протоколировать свои результаты с помощью двух и более скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания. Все скриншоты необходимо сохранить в папке «Модуль 2».
Формат названия скриншотов политик:
Пример 1 для сохранения скриншота созданной политики: CR-1.jpg где CR – сокращение от англ. creating a rule, 1 – номер задания
Пример 2 для сохранения скриншота работающей политики: RW-1.jpg где RW – сокращение от англ. rule work, 1 – номер задания.
Пример 3 для сохранения нескольких скриншотов одной работающей политики: RW-1-2.jpg где RW – сокращение от англ. rule1 work, 1 – номер задания; 2 – номер скриншота для задания 1.

Задание модуля 2:

Задача 1: Проверка работоспособности системы
Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих термин «Проверка системы» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «Проверка». Для отработки правил через сервер агентского мониторинга необходимо создавать правила в

отдельной политике «Модуль 2». После отработки политик необходимо оставить политику и открепить ее от групп компьютеров или выключить правила, но не удалять. Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя с установленным агентом. Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена), настроив конструктор выборки вручную.

Задача 2: подготовка сервера агентского мониторинга
Необходимо создать новую группу компьютеров: «DemoGroup», а также создать новую политику: «DemoPolicy». Политика должна применяться на ранее созданную группу компьютеров. Компьютер нарушителя необходимо переместить в группу «DemoGroup»
Зафиксировать выполнение скриншотом.

Задача 3: смена пароля удаления агента
Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно).
Пароль: QWEasd123
Зафиксировать выполнение скриншотом.

Следующие правила создаются в политике «DemoPolicy».
Правило 1
Запретить печать документов на сетевых принтерах. Также необходимо отдельным правилом разрешить печать на локальных принтерах.
Зафиксировать факт настройки правил (политик) скриншотами.

Правило 2
Необходимо полностью запретить использование облачного сервиса GoogleDrive, разрешить полное использование сервиса YandexDisk, остальные сервисы настроить только в режиме чтения (разрешить скачивание).
Зафиксировать факт настройки правил (политик) скриншотами.

Правило 3
Запретить запуск приложения wordpad или Libre/Open office Writer.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 4
Необходимо запретить создание снимков экрана в текстовых редакторах для предотвращения утечки.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 5
Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. В случае отсутствия USB-накопителей создать правило на сетевые расположения.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 6

С учетом ранее созданной блокировки необходимо разрешить копирование только на один доверенный USB-накопитель.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 7
Полностью заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине). В случае отсутствия CD/DVD привода его необходимо создать.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Правило 8
Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD/DVD привода.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Необходимо зафиксировать основные шаги выдачи доступа (например, ввод кода).

Правило 9
Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 30 секунд или при переходе в другое окно.
Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами. Также необходим скриншот сохраненных снимков экрана в системе.

Правило 10
Запретить передачу файлов документов типа PDF на съемные носители информации и в сетевые каталоги.
Проверить работоспособность любым из правил, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Групповые политики домена

Групповые применяются только на компьютер нарушителя (violator), должны быть созданы в домене, необходимо создать или 1 общий объект для всех политик и применить его к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю), или по 1 объекту на каждую политику и применить их к группе компьютеров/пользователей (или к конкретному компьютеру/пользователю).
Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например, запрет запуска).
Использование компонентов DLP будет считаться некорректным выполнением задания.

Групповая политика 1
Настроить политику паролей и блокировки:
- Максимальный срок действия пароля: 47 дней
- Минимальная длина пароля: 8 символов
- Блокировка пользователя при неправильном вводе пароля: 5
- Блокировка учетной записи при вводе пароля: 20 минут

Зафиксировать настройки политики скриншотами.

Групповая политика 2

Отключить анимацию первого входа в систему
Зафиксировать настройки политики скриншотами

Групповая политика 3
Запретить использование командной строки (терминала) пользователем стандартной политикой запрета (не с помощью списка, при наличии).
Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4
Запретить пользователю самостоятельный запуск панели управления.
Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5
Изменить изображение рабочего стола пользователя групповыми политиками.
Изображение необходимо создать самостоятельно, должно содержать в себе название компании («DemoExam») текстом в картинке.
Изменение изображения вручную не будет считаться корректным выполнением задания.

Приложение к оценочным материалам (Том 1)

План застройки площадки