ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА БАЗОВОГО УРОВНЯ

Том 1

(Комплект оценочной документации)

Код и наименование профессии (специальности) среднего профессионального образования	10.02.01 Организация и технология защиты информации
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 10.02.01 Организация и технология защиты информации, утвержденный приказом Министерства образования и науки Российской Федерации от 28.07.2014 № 805
Код комплекта оценочной документации	10.02.01-2023

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 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

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

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]	**4:00:00**

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	Применение программно-аппаратных и технических средств защиты информации	Использовать информационно-коммуникационные технологии в профессиональной деятельности Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных	иметь практический опыт участия в эксплуатации систем и средств защиты информации защищаемых объектов иметь практический опыт выявления возможных угроз информационной

[2] В академических часах
[3] В соответствии с ФГОС СПО.
[4] Наименование модуля задания совпадает с видом профессиональной деятельности (ФГОС СПО).

		задач, профессионального и личностного развития Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах Выявлять и анализировать возможные угрозы информационной безопасности объектов Ориентироваться в условиях частой смены технологий в профессиональной деятельности Проводить регламентные работы и фиксировать отказы средств защиты	безопасности объектов защиты работать с защищенными автоматизированными системами передавать информацию по защищенным каналам связи фиксировать отказы в работе средств вычислительной техники

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	Применение программно-аппаратных и технических средств защиты информации	Использование информационно-коммуникационные технологий в профессиональной деятельности	100,00

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

		Осуществление поиска и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развитии	
		Применение программно-аппаратных и технических средств защиты информации на защищаемых объекта	
		Выявление и анализ возможных угроз информационной безопасности объектов	
		Ориентация в условиях частой смены технологий в профессиональной деятельности	
		Проведение регламентных работ и фиксирование отказов средств защиты	
Итого			**100,00**

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	Компьютер или ноутбук	4-ядерный процессор, не менее 16ГБ ОЗУ, SSD, ПО для виртуализации с поддержкой драйверов для операционных систем семейства UNIX, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh-клиент, sftp/scp-клиент, ftp-клиент, архиватор, программа просмотра pdf, ПО для генерации сертификатов, возможность записи и трансляции экрана на все время проведения экзамена
2	Виртуальная машина (контроллер домена)	Предустановленная виртуальная машина совместимая с серверными ОС с преднастроенным доменом с внесенными пользователями домена, предустановленым и настроенным DNS сервером, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh-клиент, sftp/scp-клиент, ftp-клиент, архиватор, программа просмотра pdf, ПО для генерации сертификатов
3	Виртуальная машина (сервер DLP)	Предустановленная виртуальная машина совместимая с DLP версии не ниже 6 или аналог с компонентами DLP системы и запущенной работоспособной серверной частью DLP системы

4	Виртуальная машина	Предустановленная виртуальная машина с возможностью подключения к домену или функциональный аналог с возможностью установки MSI пакетов или виртуальная машина с возможностью установки deb-пакетов, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh-клиент, sftp/scp-клиент, ftp-клиент, архиватор, программа просмотра pdf
5	Виртуальная машина (клиент)	Предустановленная виртуальная машина с возможностью подключения к домену или функциональный аналог с возможностью установки MSI пакетов или виртуальная машина с возможностью установки deb-пакетов, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh-клиент, sftp/scp-клиент, ftp-клиент, архиватор, программа просмотра pdf
6	Монитор на каждого выпускника	не менее 20" и разрешением не менее 1920×1080 пкс, можно устанавливать 2 шт (для удобства)
7	Клавиатура на каждого выпускника	универсальная
8	Мышь компьютерная на каждого выпускника	универсальная
9	Носитель информации на каждого выпускника	USB-флешка не менее 4 ГБ
10	Программное DLP для борьбы с внутренними утечками информации и обеспечения корпоративной безопасности	Программное обеспечение для борьбы с внутренними утечками информации минимальной версии Standard или функциональный аналог (Состав: DLP сервер уровня сети, DLP сервер уровня хоста, компонент сканирования общих сетевых каталогов, соответствующие лицензии на весь период проведения , БД, совместимая с продуктом в соответствии с заданием
11	Программное обеспечение для генерации сертификатов (PKI)	любое

12	Коммутатор	Не менее 12 портов Gigabit или аналог, управляемый, L2, преднастроены виртуальные сети до мест выпускников, серверной части, комнаты экспертов.
13	Маршрутизатор или виртуальный аналог	Не менее 4 портов Gigabit или аналог, преднастроены виртуальные сети (по 1 на выпускника, 1 на экспертов, 1 на серверную инфраструктуру). Доступ между сетями выпускников запрещен, доступ с мест участников к интернет/серверам и наоборот разрешен, доступ из сети экспертов к сетям выпускников разрешен
14	Устройство для вывода таймера	ТВ-панель/проектор не менее 24", HDMI/VGA/Прочее, должен быть виден всем участникам
15	Удлинитель (сетевой фильтр) 220В или необходимое количество розеток для каждого выпускника	Кол-во розеток не менее 5, не менее 1,5 м

Перечень инструментов

№ п/п	Наименование инструментов	Минимальные характеристики
1	2	3
1	Стул со спинкой	На колесиках
2	Стол	Не менее 1300х700, можно использовать 2 стола

Перечень расходных материалов

№ п/п	Наименование расходных материалов	Минимальные характеристики
1	2	3
1	Картридж для МФУ	Картридж или дозаправка картриджа для МФУ из основного ИЛ, на усмотрение организатора
2	Ручка на каждого выпускника	Синяя, Шариковая или гелевая
3	Карандаш на каждого выпускника	Простой, средней жесткости
4	Файлы прозрачные А4	Пачка 100 шт
5	Степлер для бумаг	Не менее 30 листов

6	Набор скоб к степлеру	Не менее 200 шт, совместимость со степлером из п.6
7	Бумага	А4, 500 листов, плотность не менее 80г/м2
8	Скотч прозрачный широкий	от 48 до 50 мм
9	Ножницы канцелярские	длина 150-210 мм
10	Папка-сшиватель	формат А4 из цветного пластика толщиной не менее 0,18 мм (180 мкм), с прозрачным титульным листом толщиной не менее 0,12 мм (120 мкм) и усиленный корешок с прозрачным карманом для маркировки

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	воздухообмен из расчета на 1 человека в час: 20 $м^3$/ч
2.	Полы	ровный без выбоин, обладающий антистатическими свойствами
3.	Освещение	в пределах 300-500 лк над поверхностью рабочего стола
4.	Электричество	Необходимо подключение не менее 3 розеток 220В к каждому месту, не менее 0,5КВт/место
5.	Водоснабжение	отсутствует
6.	Отходы	Мусорная корзина
7.	Температура	В пределах 19 -22 градуса Цельсия

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:

Участник экзамена должен знать месторасположение первичных средств пожаротушения.

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

При неисправности инструмента и оборудования – прекратить выполнение задания и сообщить об этом Эксперту, а в его отсутствие заместителю главного Эксперта.

При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т. д.), участнику следует немедленно сообщить о случившемся Экспертам. Выполнение задания продолжить только после устранения возникшей неисправности.

В случае возникновения у участника плохого самочувствия или получения травмы сообщить об этом эксперту.

При возникновении пожара необходимо немедленно оповестить Главного эксперта и экспертов. При последующем развитии событий следует руководствоваться указаниями Главного эксперта или эксперта, заменяющего его.

При обнаружении взрывоопасного или подозрительного предмета не подходите близко к нему, предупредите о возможной опасности находящихся поблизости экспертов или обслуживающий персонал.

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.

По окончании работы участник экзамена при необходимости должен сообщить эксперту о выявленных во время выполнения заданий неполадках и неисправностях оборудования, и других факторах, влияющих на безопасность выполнения задания.

1.6. Образец задания демонстрационного экзамена

Модуль: Применение программно-аппаратных и технических средств защиты информации
Задание модуля: **Задание 1** Настройка контроллера домена Внутри созданного подразделения “Filial” необходимо создать и настроить следующих доменных пользователей с соответствующими правами: Логин: iwtm-adm, пароль: xxXX6677, права пользователя домена Логин: ldap-user, пароль: xxXX6677, права пользователя домена Логин: iwdm-root, пароль: xxXX6677, права администратора домена и локального администратора Логин: user-client, пароль xxXX6677, права пользователя домена Логин: user-gp, пароль xxXX6677, права пользователя домена 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. Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам. Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-user.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-adm с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

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.

Установка и настройка сервера агентского мониторинга

Сервер агентского мониторинга предустановлен, есть необходимость в его настройке.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя iwdm-root, установить полный доступ к системе, установить все области видимости.

Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

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.

Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-client.

После входа в систему необходимо переместить веденный в домен компьютер в ранее созданное подразделение “Filial” на домене.

Установить агент мониторинга:

На машину 1 (user-client) с помощью задачи первичного распространения с сервера агентского 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.

Задание 2

Следующие 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 (это всегда указывается отдельно). 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.

Формат названия скриншотов политик:
Пример 1 для сохранения скриншота созданной политики: CP-1.jpg
где CP – сокращение от англ. creating a policy, 1 – номер задания
Пример 2 для сохранения скриншота работающей политики: PW-1.jpg
где PW – сокращение от англ. policy work, 1 – номер задания.
Пример 3 для сохранения нескольких скриншотов одной работающей политики: PW-1-2.jpg
где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер скриншота для задания 1.

Необходимо создать новую группу компьютеров: «Подразделение», а также создать новую политику: «Подразделение».

Зафиксировать выполнение скриншотом.

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно). Пароль: xxXX6677

Проверить работоспособность и зафиксировать выполнение скриншотами.

Следующие правила создаются в политике «Подразделение».

Задание 3

Запретить печать документов на сетевых принтерах. Также необходимо отдельным правилом разрешить печать на локальных принтерах.

Зафиксировать факт настройки правил (политик) скриншотами.

Задание 4

Необходимо полностью запретить использование облачного сервиса YandexDisk, разрешить полное использование сервиса EverNote, остальные сервисы настроить только в режиме чтения (разрешить скачивание).

Зафиксировать факт настройки правил (политик) скриншотами.

Задание 5

Запретить запуск приложения charmap и control.exe.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Задание 6

Необходимо запретить создание снимков экрана в wordpad для предотвращения утечки секретных документов.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Задание 7

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.

Задание 8

С учетом ранее созданной блокировки необходимо разрешить копирование только на один доверенный USB-накопитель с помощью белого списка. В случае отсутствия USB-накопителей создать исключение для любого другого конкретного устройства (кроме CD/DVD).

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Задание 9

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.

Задание 10

Осуществить выдачу временного доступа (240 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).

Задание 11

Необходимо запретить доступ к буферу обмена в приложениях notepad и putty.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами.

Задание 12

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик IWTM.

Проверить работоспособность, зафиксировать факт настройки правил (политик) и их работоспособность скриншотами (обязательно с рабочим событием печати в веб-консоли).

Групповые политики домена

Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Использование компонентов DLP будет считаться некорректным выполнением задания.

Задание 13

Настроить политику паролей и блокировки:

- Максимальный срок действия пароля: 30 дней
- Минимальная длина пароля: 6 символов
- Блокировка пользователя при неправильном вводе пароля: 5
- Блокировка учетной записи при вводе пароля: 20 минут

Зафиксировать настройки политики скриншотами.

Запретить запуск приложений ipconfig.exe, dialer.exe.

Зафиксировать настройки политики и выполнение скриншотами.

Запретить использование командной строки и редактора реестра пользователем стандартной политикой запрета (не с помощью списка).

Зафиксировать настройки политики и выполнение скриншотами.

Запретить пользователю самостоятельно выключать компьютер.

Зафиксировать настройки политики и выполнение скриншотами.

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задача 1–1 и т. д.)

Необходимо называть политики / объекты / категории / теги и прочее ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик:

Политика 1, Политика 2, Политика 3, Политика 4, Политика 5, Политика 6, Политика 7, Политика 8, Политика 9, Политика 10, Политика 11, Политика 12

Задание 14

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты. Стоит учесть, что стандартные политики и объекты можно модифицировать под свои нужды.

Создайте локальную группу пользователей «На перевод в отдел» в Traffic Monitor. Добавьте в нее трех любых пользователей.

Создать список веб-ресурсов «Партнерские домены». Добавить в список следующие сайты: mydemo.org, demolab.ru, demosys.lab.

Для работы системы необходимо настроить периметр компании:

- Почтовый домен: demo.lab.
- Список веб ресурсов «Партнерские домены» (созданный ранее).
- Группа персон: пользователи домена (все).
- Исключить из перехвата почту генерального директора.

Задание 15

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела кадров (HR) отправлять документы, содержащие информацию о СНИЛС и паспортных данных (в текстовом и графическом виде) за пределы компании. Отдел кадров может отправлять файлы без ограничений. Можно использовать стандартные технологии и объекты.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 1

Задание 16

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании (документ «Анкета.docx»), контролируя любую внешнюю передачу документов, содержащих заполненные бланки, при этом пустые бланки контролировать не нужно.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Задание 17

В связи с введением оплаты с помощью кредитных карт, необходимо запрещать передачу как текстовых, так и графических данных о кредитных картах за пределы компании для всех сотрудников, кроме отдела договоров (accounting). Политика может быть настроена с использованием стандартных технологий и объектов.

Вердикт: заблокировать

Уровень нарушения: средний

Тег: Политика 3

Задание 18

Необходимо отслеживать любые документы, передающиеся за пределы компании и содержащие печать компании всем сотрудникам, кроме отдела продаж (Sales) и директора компании. Они могут обмениваться документами внутри и за пределами компании без контроля.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Задание 19

Отдел продаж занимается продажей продуктов для офиса, таких как «молоко», «печеньки», «кофе», «чай», «конфеты» (учитывая морфологию). В последнее время было замечено продажа «налево», сотрудники были заподозрены в хищении средств. Таким образом, вам нужно установить слежку за сотрудниками отдела продаж (sales), и детектировать случаи передачи информации о товарах.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 5

Задание 20

Необходимо настроить виджеты и отчеты в системе предотвращения утечек.

Необходимо создать пользователя DLP системы с правами просмотра и выполнения сводок, отчетов и событий. Прав на редактирование (изменение) быть не должно.

Пользователь: eventview, пароль: xxXX6677

Создайте новые вкладки сводки в разделе «Сводка» под названием «ДЭ» и «Отчетность»

При создании выборок для сводок необходимо помещать их в каталог выборок «ДЭ»

Создайте в сводке «ДЭ» 4 виджета:

1. Выборка по событиям копирования за последний месяц
2. Выборка по политикам с технологиями: графические объекты, печати, эталонные документы за последнюю неделю
3. Статистика по политикам за последний день
4. Топ нарушителей за последние 3 дня

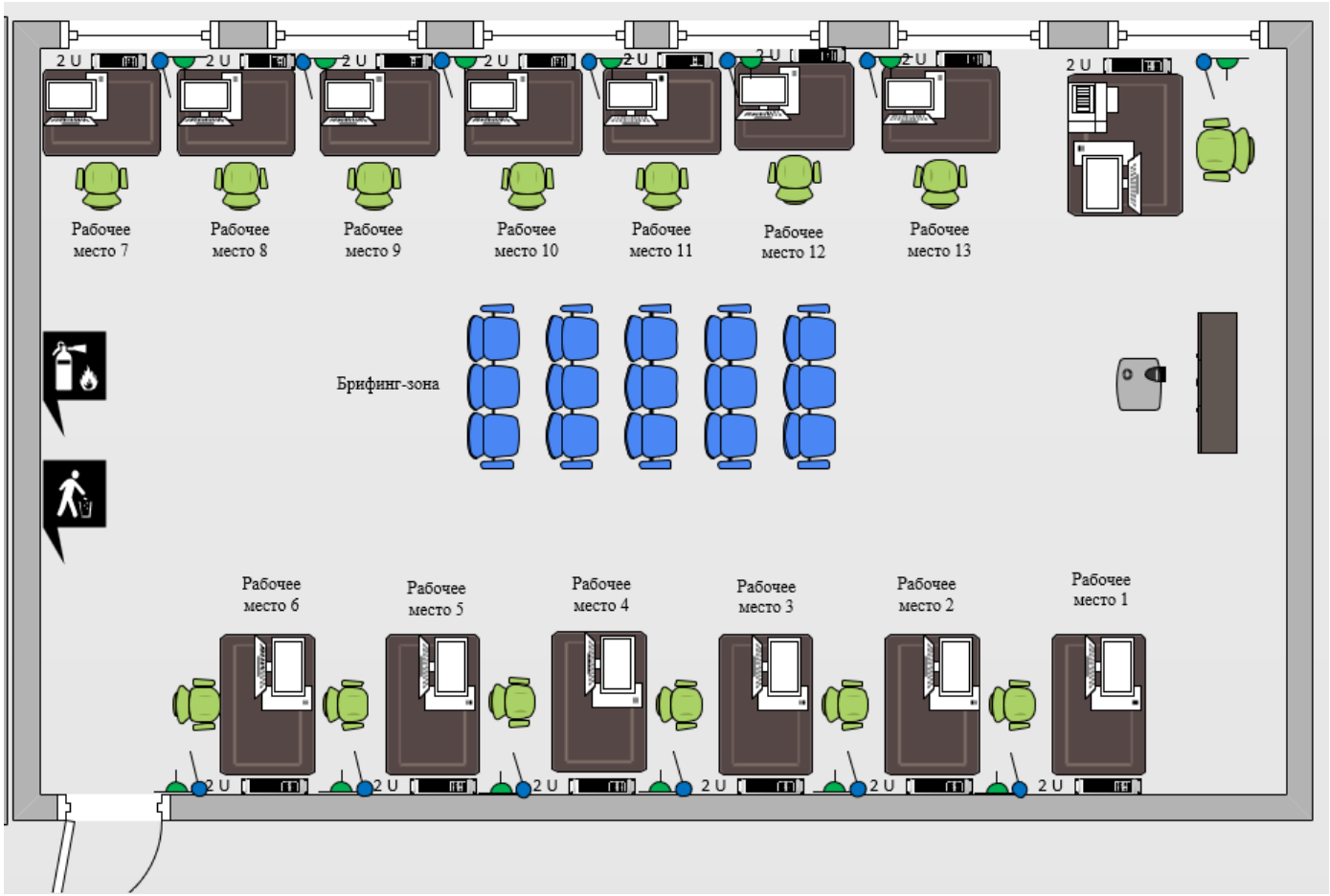
Необходимо создать виджет в разделе «Сводка», вкладка «Отчетность», отображающий события с уровнем угрозы от низкого до высокого на правила передачи и работы в приложениях (буфера) за последние 7 дней.

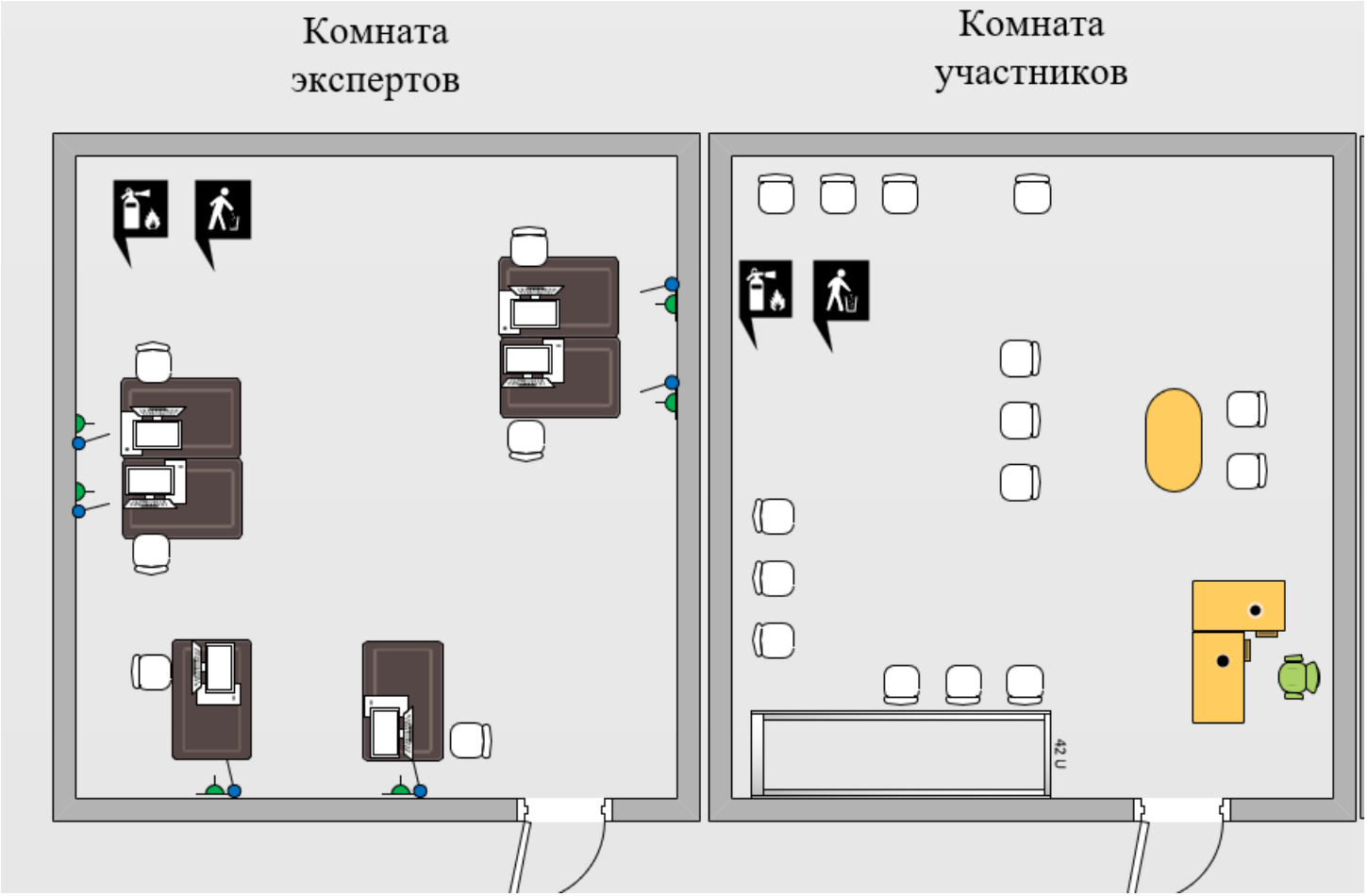
Зафиксировать скриншотом конструктора выборки.

Необходимо создать виджет в разделе «Сводка», вкладка «Отчетность» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) с низким и высоким уровнем угрозы за последние 30 дней.

Приложение к оценочным материалам (Том 1)

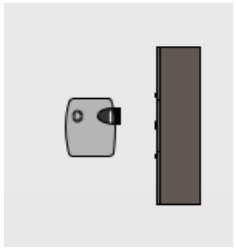
План застройки площадки



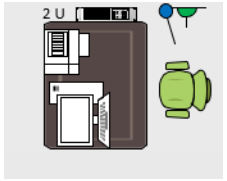

Комната
экспертов
Комната
участников
42 U

Условные обозначения:

Рабочее место участника, состоящее из системного блока, монитора, клавиатуры, компьютерной мыши, размещенных на рабочем столе; стола; компьютерного стула; пилота с розетками 220 В



Для брифингов и презентаций: короткофокусный проектор с экраном ИЛИ плазменная панель, подключенные к компьютеру



Рабочее место Главного эксперта (1 место): компьютер с монитором, подключенный к интернету (ноутбук, моноблок), на который установлены операционная система, браузер, клавиатура, компьютерная мышь, размещенная на рабочем столе; стол; компьютерный стул; пилот с розетками 220 В

Место участника в брифинг-зоне, состоящее из стула и 1 общего стола для подписания протоколов. По усмотрению организаторов можно установить стол для каждого участника