Задание для демонстрационного экзамена по комплекту оценочной документации № 1.1 по компетенции № F7 «Корпоративная защита от внутренних угроз информационной безопасности»

Вариант 1

Задание включает в себя следующие разделы:

1. Формат Демонстрационного экзамена
2. Формы участия
3. Вид аттестации
4. Модули задания, критерии оценки и необходимое время
5. Необходимые приложения

Продолжительность выполнения задания: 6,5 ч.

1. Формат Демонстрационного экзамена:

Очный

2. Форма участия:

Индивидуальная

3. Вид аттестации:

ГИА

4. Модули задания, критерии оценки и необходимое время

Модули и время сведены в Таблице 1.

Таблица 1.

№ п/п	Модуль, в котором используется критерий	Критерий	Время выполнения Модуля	Проверяемые разделы WSSS	Баллы		
					Судейские	Объективные	Общие
1.	1. Установка и конфигурирование компонентов DLP системы	A. Организация работы и управление B. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	2 часа	1, 2	0	18	18
2.	2. Технологии агентского мониторинга	C. Технологии агентского мониторинга	1,5 часа	6	0	13	13
3.	3. Разработка и применение политик, анализ выявленных инцидентов	D. Разработка политик безопасности, анализ выявленных инцидентов	3 часа	4, 7	0	23	23
				Итого		54	54

1. Модули с описанием работ

Модуль 1: Установка и конфигурирование компонентов DLP системы

Введение

В компания «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации.

Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием.

Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса нужно назначить согласно прилагаемой карточке. Подготовлены следующие виртуальные машины для дальнейшей работы:

AD Сервер с контроллером домена

DLP сервер установлен (но не настроен), активирована лицензия

Виртуальная машина для установки сервера агентского мониторинга

Виртуальные машины «нарушителей» для установки агентов

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

Для большей сетевой безопасности в компании все устройства должны иметь статический IP-адрес. Сетевые настройки указаны в дополнительных сведениях к заданию.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными в соответствии с номером рабочего места (например, server-16).

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в общем сетевом каталоге.

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания. Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания

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 или передаются экспертам иным способом по запросу.

Задание 1: Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: iwtm-officer, пароль: xxXX1234, запретить локальный вход в систему

Логин: ldap-user, пароль: xxXX1234, запретить локальный вход в систему

Логин: iwdm-admin, пароль: xxXX1234, права администратора домена и локального администратора

Логин: user-agent, пароль xxXX1234, права пользователя домена

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Настроить DNS на сервере для корректной работы.

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 использовать ранее созданного пользователя домена iwtm-officer с полными правами 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» с заголовком IWTM.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить базу данных с паролем суперпользователя xxXX1234.

Установить сервер агентского мониторинга с параметрами по умолчанию.

При установке необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, но можно сделать это и после установки сервера агентского мониторинга.

Настроить пользователя консоли управления: officer с паролем xxXX1234.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

Зафиксировать факт создания пользователя и настройку скриншотом.

Проверить работоспособность входа в консоль управления без ввода пароля. Стоит обратить внимание, что если сервер не введен в домен, данная опция работать не будет.

Зафиксировать факт подключения без пароля скриншотом.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину в домен от ранее созданного пользователя user-agent, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить агент мониторинга 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 пакета установки является неверным выполнением задания.

Зафиксировать успешное выполнение задачи скриншотом

В случае проблем стоит проверить настройки брандмауэра и DNS.

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга.

Необходимо создать общий каталог CrawlerShare в корне диска и установить права доступа на запись и чтение для всех пользователей.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Зафиксировать выполнение задания скриншотом настройки в web-консоли.

Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих термин «Проверка системы», установить низкий уровень угрозы для всех событий, добавить тег «Проверка».

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).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа 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 (user) сертификат

Итоговый результат должен включать:

Дерево из 2 (3)-х сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов.

Содержимое команд по генерации ключей и сертификатов в текстовом файле «отчет.txt»

Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертифкации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании Demo.lab и т.п.

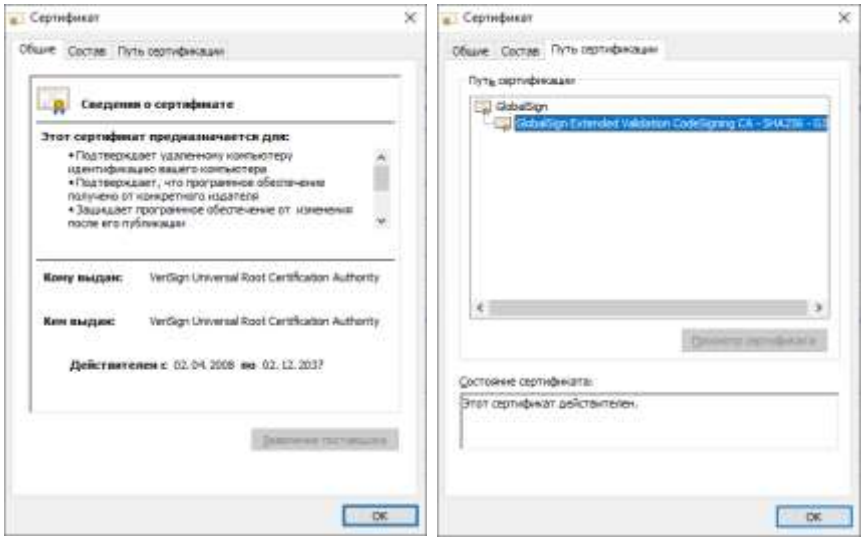

Рис1. Пример скриншотов задания 6

Генерацию сертификатов зафиксируйте скриншотами.

Модуль 2: Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т.д.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух 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: 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.

Задание 1

Необходимо создать новую политику под названием «Политика данных», применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину нарушителя для удаленного доступа к серверу агентского мониторинга.

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: iwdmassistant, пароль: xxXX1234

Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

Необходимо запретить создание снимков экрана в калькуляторе для предотвращения утечки секретных расчетов.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Задание 8

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.

Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

Задание 10

Создать политику по блокировке копирования файлов формата jpeg на USB-накопители.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 12

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования текстового процессора (word) путем создания снимков экрана каждые 30 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 13

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 14

Осуществить выдачу временного доступа (60 минут) клиенту до заблокированного CD привода.

Зафиксировать скриншотами факт выдачи доступа и необходимые действия для выдачи доступа.

Задание 15

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 16

Необходимо установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно).

Проверить работоспособность и зафиксировать выполнение скриншотом

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

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

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additions» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух 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 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg

где CP – сокращение от англ. creating a policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW-1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов

Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

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».

ВНИМАНИЕ!

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

ВНИМАНИЕ!

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

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.

Задание 1

Создайте локальную группу пользователей «*Сотрудники под наблюдением*» в Traffic Monitor. Добавьте в нее трех любых пользователей. *Подтвердите выполнение задания скриншотами.*

Задание 2

Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы IWTM с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Также добавить просмотр списка объектов защиты.

Области видимости: все.

Логин: auditor, пароль: xxXX1234

Подтвердите выполнение задания скриншотами.

Политика 4

В связи с секретностью при организации очередного мероприятия WorldSkills, совет директоров решил контролировать передачу информации о заданиях за пределы компании. В связи с этим необходимо создать политику

на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих фразу «Секретное задание» и «Secret task».

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы из, а также стоять/не стоять пробел между словами, например: «Секретноезадание», «секретное task». Ложных срабатываний быть не должно (например, просто на секретное, task).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мероприятие

Проверить работоспособность.

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа «Договор.docx» за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 40%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 6

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

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 7

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 8

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды.docx» (8 штук). Необходимо контролировать коды внутри компании, при этом запрещать передачу за пределы компании.

Передача кодов внутри компании:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: коды

Передача кодов за пределы компании:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 9

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «3 буквы (латиница, любой регистр) - (знак дефиса) номер груза (от 0 до 1000, исключая несчастливые номера: 666 и 13) . (точка) 1-2 буквы (кириллица, верхний регистр)

Например: jDt-123.УЛ , kdU-665.ЪЩ

Не должно быть срабатывания на несчастливые номера грузов (например: kdO-666.Д или jfd-13.ЮШ).

Необходимо отслеживать попытки передачи данных кодов только на все внешние адреса, но не блокировать.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: транспорт

Проверить работоспособность.

Политика 10

Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации.

Критичными данными в выгрузке являются телефоны, ИНН, ОКПО, ОКФС, ОКОГУ и ОКОПФ и в 1 документе присутствует 3 или более компаний. Для настройки используйте файл «Выгрузка из БД.csv».

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: база

Проверить работоспособность.

Политика 11

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить потенциальную утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты доменов компании: demo и demolab, демо, демолаб.

Важно, чтобы в одном сообщении содержалось минимум 4 адреса (т.к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, su, org, lab, рф.

Детектирование только частей адресов (например @demo.ru) недопустимо.

Пример формата адресов: e-mail@demolab.ru , mail+tag@demo.lab , мой.меил@демолаб.рф , элепочта@демо.рф и т. п.

Разрешенные спецсимволы в корпоративной почте: _ . - +

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: почты

Проверить работоспособность.

Политика 12

Для мониторинга движения анкет необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 13

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID (внутри любой фразы), SARS (внутри любой фразы, например SARS-CoV-2), Коронавирус.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 14

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме бухгалтерии передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: пдн

Проверить работоспособность.

Политика 15

Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также файлов XML. Стоит учесть, что файлы могут передаваться в том числе и на съемных носителях информации.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Задание 16: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю

Статистика по политикам за последние 3 дня

По типу событий: необработанные нарушения за месяц

По топ-нарушителям за сегодня

Задание 17: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:

Отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.

Отображающий события с любым одним тегом только с машины нарушителя.

5. Необходимые приложения

Приложение 1 Пояснения по подготовке площадки (документ docx)

Приложение 2 Карточка настроек сети и оборудования (документ docx)

Приложение 3 Эталонные файлы для выполнения заданий (архив zip)

Приложение 4 Пример пользователей и групп для домена (документ csv)