

Рисунок 45 – «Пользователи консоли, как должно быть»

Перед тем, как создавать новые политики в консоли IWDm, необходимо создать задачи распространения агента Device Monitor на компьютеры сети. Для этого, перейдите во вкладку «Задачи» в левой нижней части интерфейса программы. Для создания задачи нажмите кнопку «Создать задачу...» (зеленый плюс). Произвольно назовите задачу и задайте ей тип «Задача первичного распространения» (рис. 46).

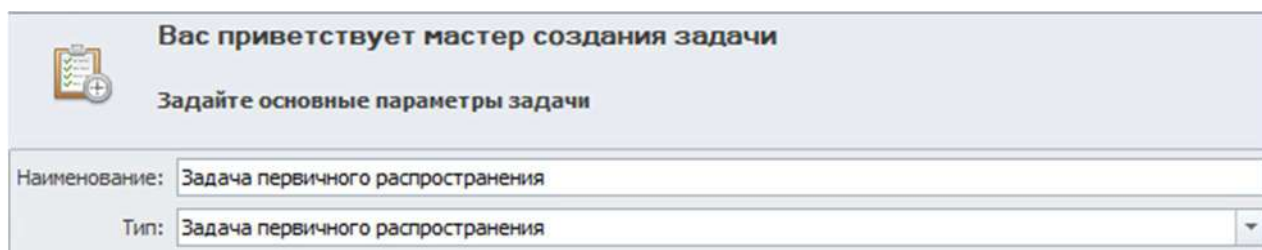


Рисунок 46 – «Шаг 1»

Теперь, на Шаге 2, задайте компьютеры, на которые будет распространяться задача. Нажмите кнопку «Добавить...» и добавьте компьютеры из Active Directory. Папка с устройствами AD называется «Директория:demo.lab». (рис. 47), после чего выберите компьютеры пользователей (w10-cli1, w10-cli2) и перейдите к след шагу.

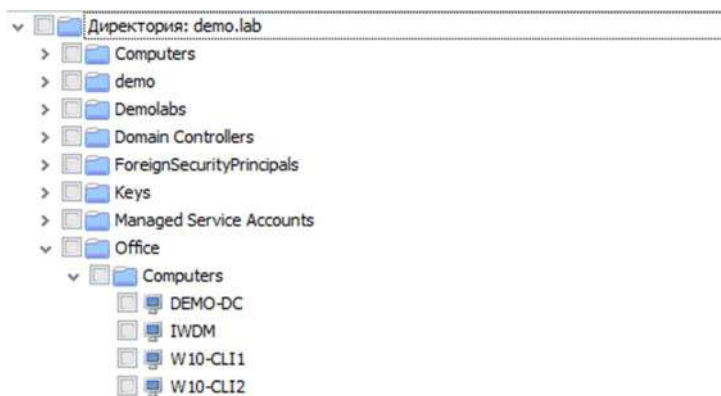


Рисунок 47 – «Добавление компьютеров»

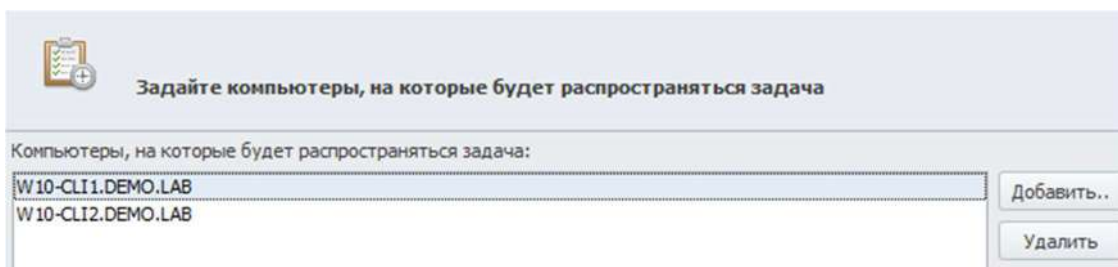
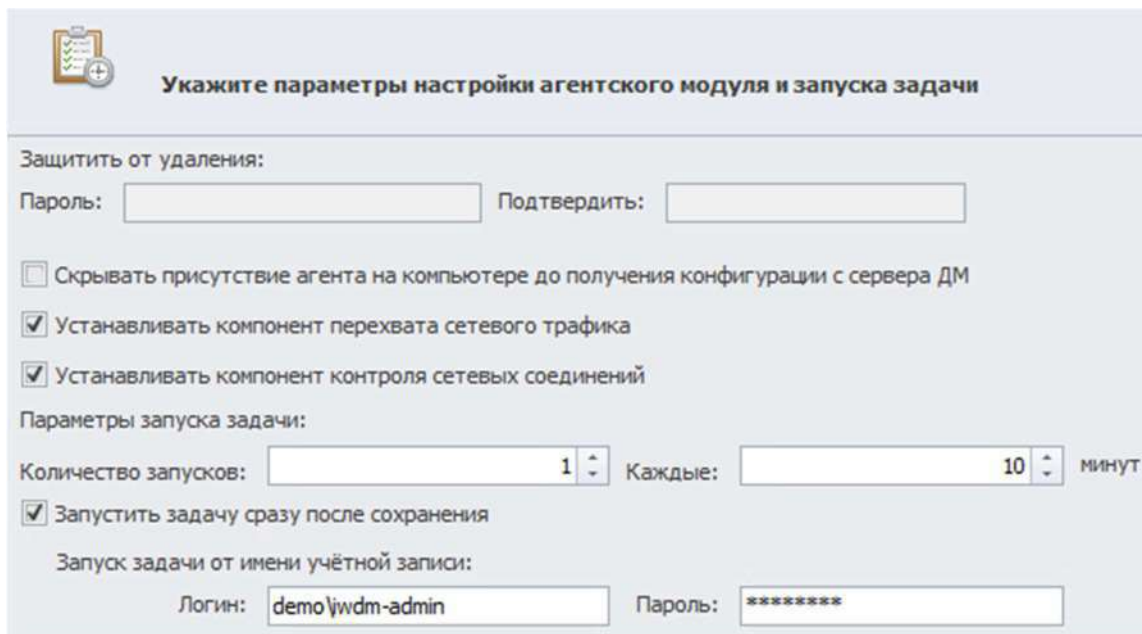


Рисунок 48 – «Шаг 2»

На третьем шаге необходимо выбрать серверы Device Monitor – он у вас один, его и выбирайте. На шаге 4 нужно указать проху-сервера Device Monitor оно указано изначально - менять его не нужно. Следующее, что необходимо сделать – указать параметры настройки агентского модуля и запуска задачи. В этом пункте не нужно ничего менять, единственная необходимость – задать логин и пароль в пункте «задачи от имени учётной записи» (рис. 49). Логин – iwdm-admin, пароль – ххХХ1234. На шаге 6 – указание параметров перезагрузки установите следующие параметры: ожидать перезагрузки без уведомления сотрудника – не ожидать; уведомлять сотрудника о необходимости перезагрузки и ожидать

перезагрузки – не уведомлять (рис. 50). На шаге 7 перепроверьте информацию и закончите создание задачи, после чего она автоматически запустится.



Укажите параметры настройки агентского модуля и запуска задачи

Защитить от удаления:

Пароль: Подтвердить:

☐ Скрывать присутствие агента на компьютере до получения конфигурации с сервера ДМ

☒ Устанавливать компонент перехвата сетевого трафика

☒ Устанавливать компонент контроля сетевых соединений

Параметры запуска задачи:

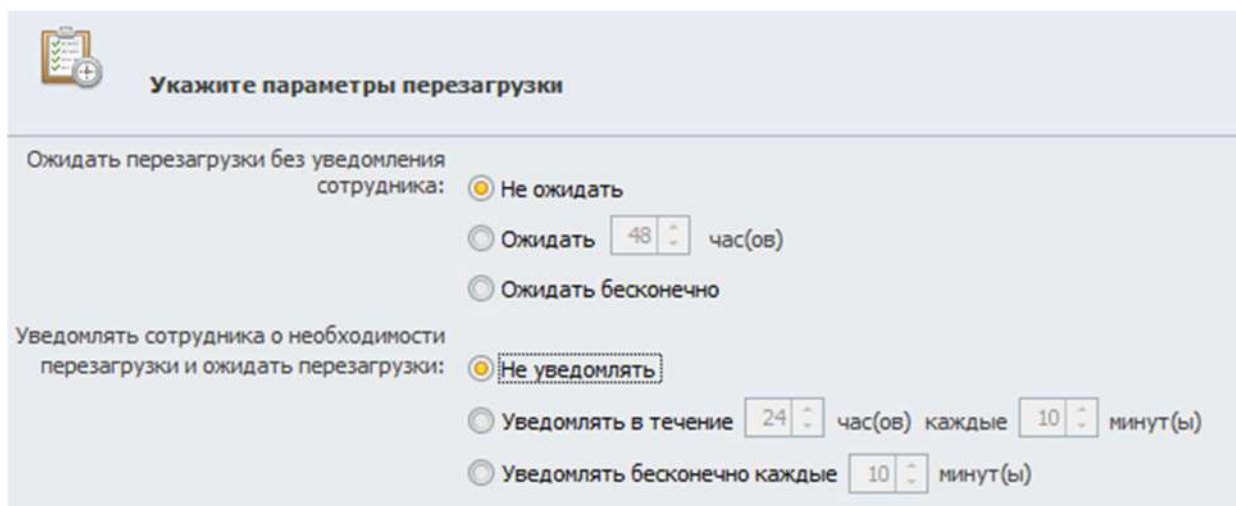
Количество запусков: Каждые: минут

☒ Запустить задачу сразу после сохранения

Запуск задачи от имени учётной записи:

Логин: Пароль:

Рисунок 49 – «Шаг 5»



Укажите параметры перезагрузки

Ожидать перезагрузки без уведомления сотрудника:

☒ Не ожидать

☐ Ожидать час(ов)

☐ Ожидать бесконечно

Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки:

☒ Не уведомлять

☐ Уведомлять в течение час(ов) каждые минут(ы)

☐ Уведомлять бесконечно каждые минут(ы)

Рисунок 50 – «Шаг 6»

В первый раз задача не запустится из-за того, что необходимые порты на конечных устройствах не открыты. Открывать их – бессмысленное занятие, поэтому легче полностью отключить фаервол (на 02.2022 за это не снимают баллы). Откройте на обеих виртуальных машинах (w10-cli1, w10-cli2) командную

строку с правами администратора и введите команду **netsh advfirewall set allprofiles state off**. Ожидаемый вывод – «ОК.». Plusом ко всему, необходимо изменить параметры общего доступа. Откройте «Панель управления» (рис. 51), перейдите ко вкладке «Сеть и Интернет» (рис. 52), а затем в «Центр управления сетями и общим доступом» (рис. 53).

control /name Microsoft.NetworkAndSharingCenter

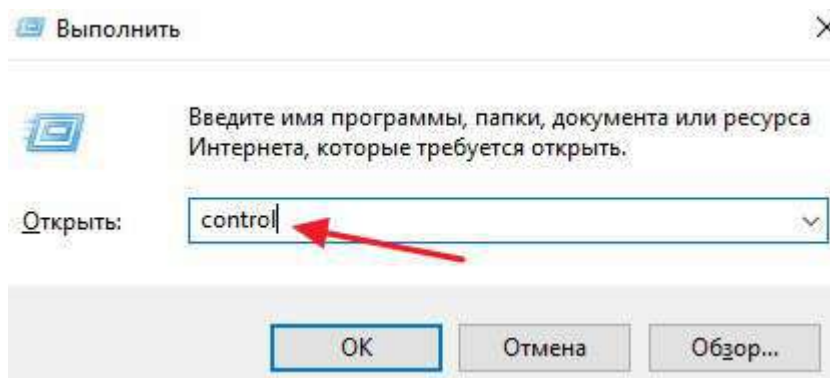


Рисунок 51 – «Запуск панели управления»

Настройка параметров компьютера

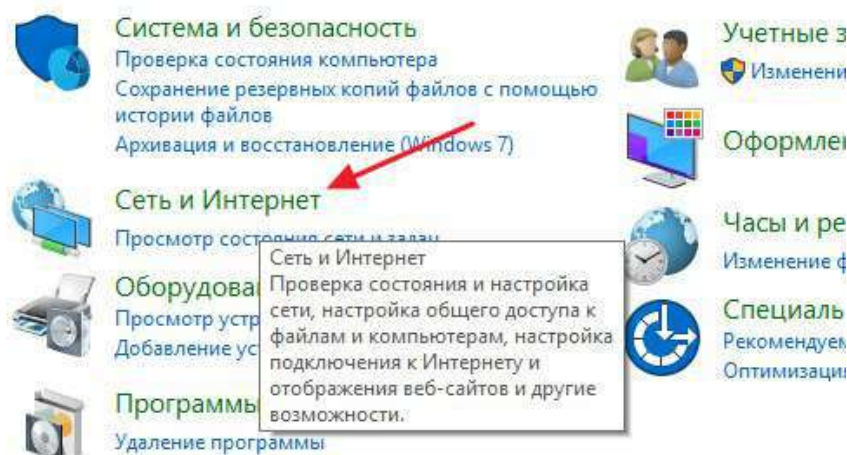


Рисунок 52 – «Сеть и Интернет»

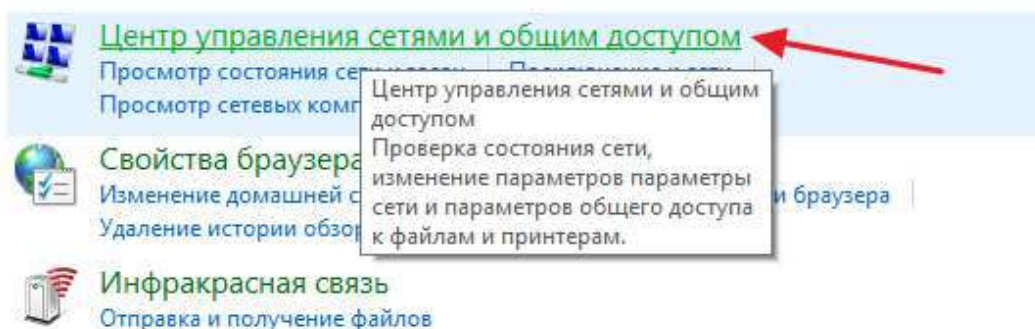


Рисунок 53 – «Центр управления сетями и общим доступом»

Затем, необходимо кликнуть по ссылке «Изменить дополнительные параметры общего доступа», которая находится в левом боковом меню (рис. 54).

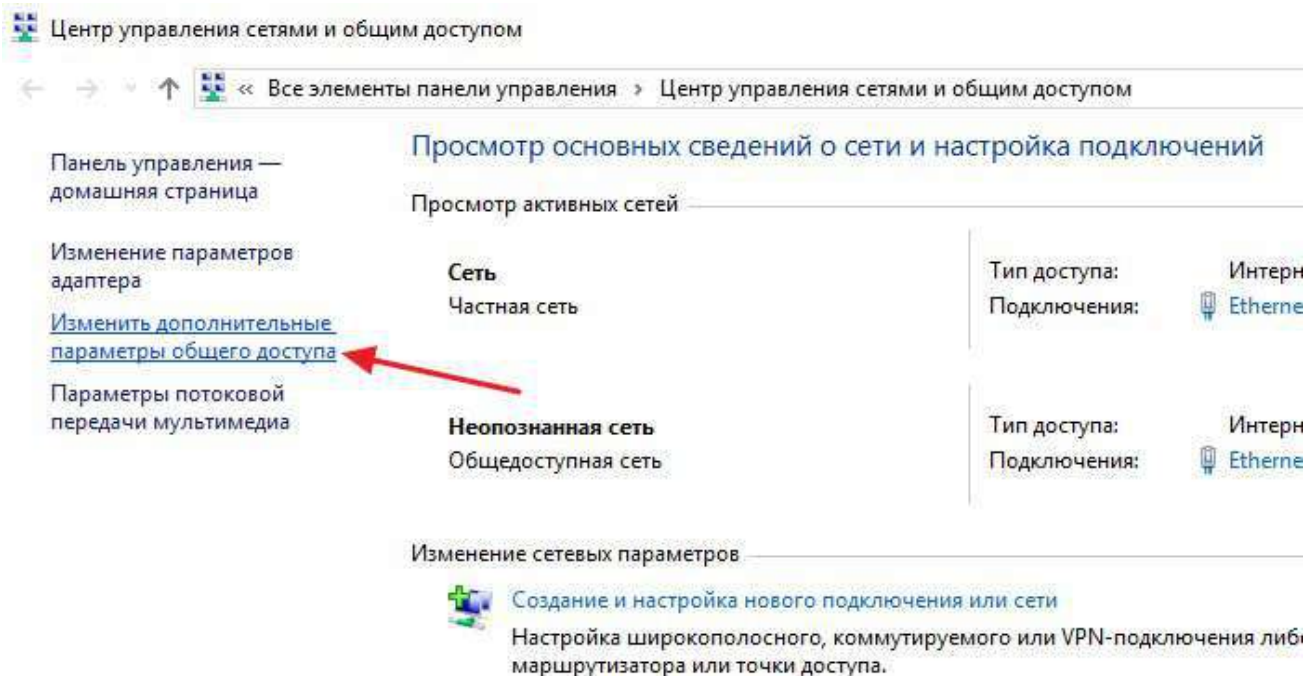


Рисунок 54 – «Изменить дополнительные параметры общего доступа»

В результате перед вами появится окно с большим списком настроек общего доступа. ВСЕ настройки во ВСЕХ вкладках, необходимо **ВКЛЮЧИТЬ**, активировать, запустить. Без этого, задача распространения Device Monitor работать не будет.

После включения общего доступа, запустите задачу распространения заново.

ВАЖНО: для проверки, заработали ли настройки общего доступа с виртуальной машины Device Monitor попробуйте зайти на сетевые ресурсы \\w10-cli1\admin\$ и \\w10-cli2\admin\$. Если вы не можете попасть на эти сетевые ресурсы – попробуйте снова **ОТКЛЮЧИТЬ** весь общий доступ, а затем снова **включить**.

Следующее, что необходимо сделать - создать 2 политики: «Политика 1», «Политика 2». Для этого, в левой части интерфейса консоли Device Monitor перейдите ко вкладке «Политики» и нажмите «Создать политику...» (рис. 55).

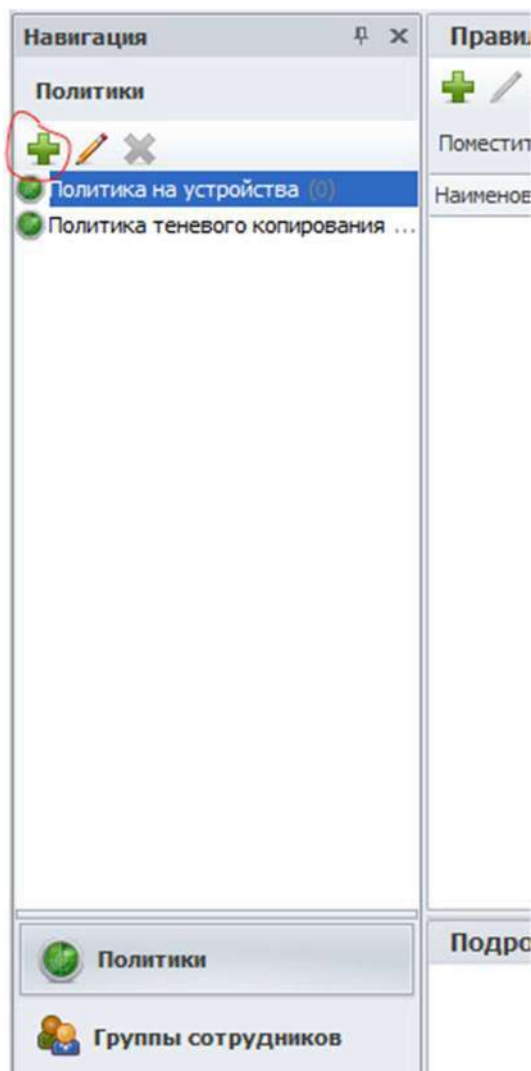


Рисунок 55 - «Создание политики»

Назовите создаваемую политику «Отдел 1» и не меняю никаких настроек сохраните. Повторите операцию для «Отдел 2». Затем перейдите ко вкладке «Группы компьютеров» в левой нижней части интерфейса программы Device Manager. Нажмите на кнопку «Создать группу устройств» и установите настройки в соответствии с рисунком 56. Создайте вторую группу устройств для «Политики 2» и w10-cli2.

Наименование:

Политика:

Компьютеры в группе:

Имя
W10-CLI1.DEMO.LAB

Скорость отправки данных с агента

☐ Переопределить настройки группы

Максимальная скорость отправки данных: «не определена»

Контроль дискового пространства на агенте

☐ Переопределить настройки группы

Минимальное свободное дисковое пространство на агенте: %

Поведение агента на компьютере

☐ Переопределить настройки группы

☒ Отображать уведомления сотруднику

☐ Скрывать присутствие агента на компьютере

Рисунок 56 - «Создание группы компьютеров»

Правила для Отдела 1:**Правило 1**

Необходимо запретить создание снимков экрана в табличных процессорах (Excel или LibreOffice Calc) и калькуляторе для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 2

Необходимо запретить печать на локальных принтерах, но при этом оставить возможность печати на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Правило 3

Создать политику по блокировке копирования исполняемых exe-файлов на USB-накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов).

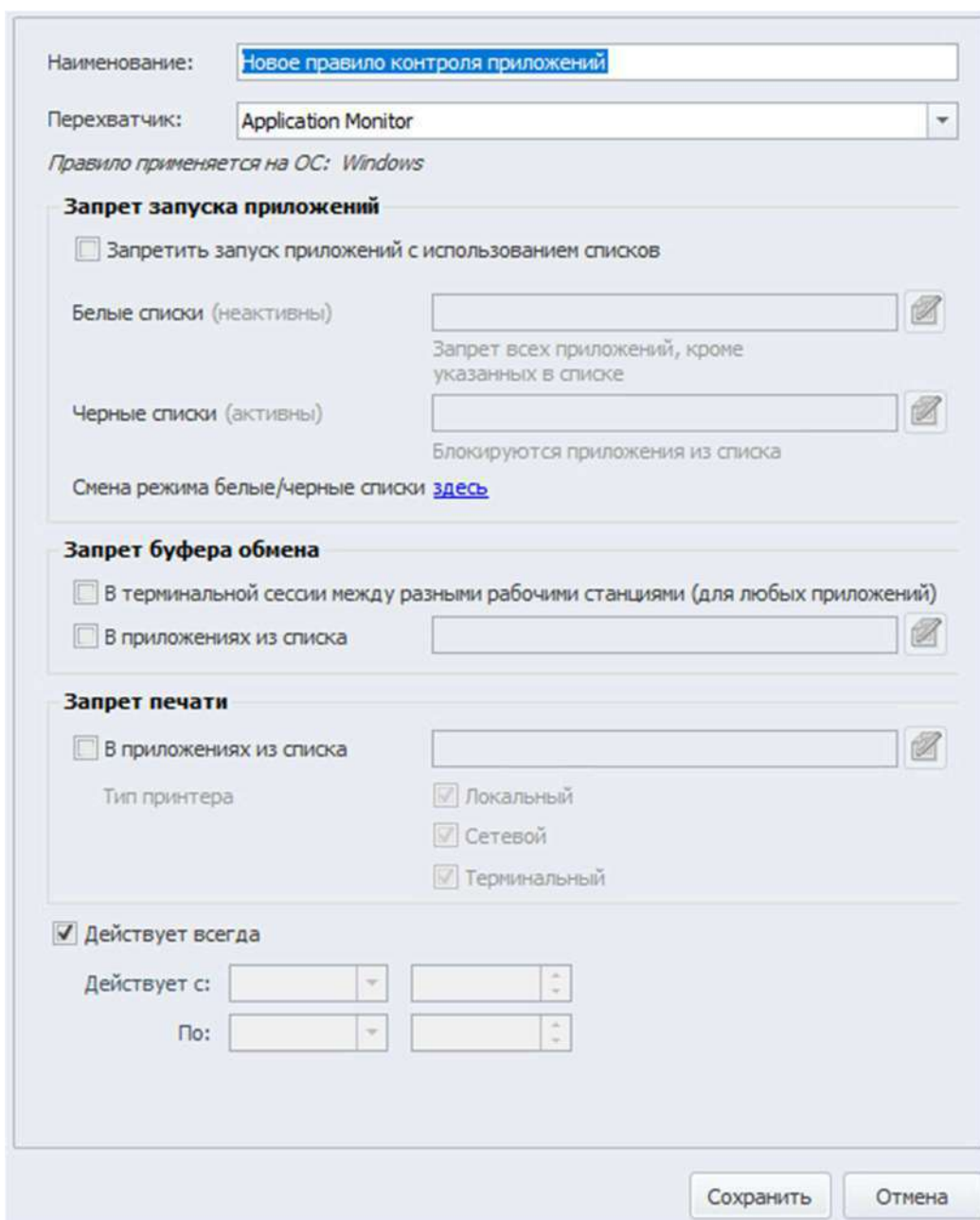
Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 4

В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить.

Проверить работоспособность на любом доступном файловом сервере и зафиксировать выполнение скриншотом.

Теперь вам нужно создать правила для Отдела 1. Первое правило, согласно заданию, должно запретить создание скриншотов в Excel или LibreOffice Calc. Для этого, прежде всего, необходимо узнать, как работают сами правила и как их создавать. Для того, чтобы создать и настроить правило, вам необходимо вернуться к разделу «Политики» в Device Monitor Console и перейти к политике «Отдел 1», после чего нажать кнопку «Создать правило...» (не путать с «создать политику...») обозначенную уже привычным зеленым плюсиком.




Наименование: Новое правило контроля приложений

Перехватчик: Application Monitor


Правило применяется на ОС: Windows

Запрет запуска приложений

☐ Запретить запуск приложений с использованием списков

Белые списки (неактивны) 

Запрет всех приложений, кроме указанных в списке


Черные списки (активны) 

Блокируются приложения из списка


Смена режима белые/черные списки [здесь](#)

Запрет буфера обмена

☐ В терминальной сессии между разными рабочими станциями (для любых приложений)

☐ В приложениях из списка 

Запрет печати

☐ В приложениях из списка 

Тип принтера

☒ Локальный

☒ Сетевой

☒ Терминальный

☒ Действует всегда

Действует с:

По:

Сохранить Отмена

Рисунок 57 – «Создание правила»

При создании правила, необходимо дать ему название и указать перехватчик. Перехватчик — это особый механизм захвата событий операционной системы. Всего перехватчиков 15, однако, в рамках задания, ВСЕ они не будут использованы. Каждый перехватчик индивидуален и отслеживает отдельные события в ОС. Например, перехватчик «Application Monitor» перехватывает информацию о приложениях и действиях в них. С помощью «Application Monitor» можно запретить запуск отдельных приложений, запретить использование буфера обмена внутри приложения или запретить печать из приложения.

Правило 1, требующее запретить создание снимков экрана в табличных процессорах (Excel, Calc) будет использовать Application Monitor. Для того, чтобы запретить запуск какого-либо приложения, его необходимо добавить в список. Для того, чтобы создать список перейдите ко вкладке «Приложения» в Device Monitor Console. Во вкладке «Приложения», вы увидите все приложения, которые запускали на клиентских компьютерах, и информацию о них.


















	Дата	Компьютер	Пользоват...	Имя прило...	Описание	Название п...	Издатель	Расположение
	17.02.2022 1...	W10-CLI1.DEMO.LAB	DEMO\USER...	taskhostw.exe	Host Proces...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
	17.02.2022 1...	W10-CLI1.DEMO.LAB	DEMO\USER...	background...	Background ...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
	17.02.2022 1...	W10-CLI1.DEMO.LAB	<система>	sppsvc.exe	Microsoft So...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
	17.02.2022 1...	W10-CLI1.DEMO.LAB	<система>	SppExtCom...	KMS Connec...	Microsoft® ...		c:\windows\system32\
	17.02.2022 1...	W10-CLI1.DEMO.LAB	<система>	RUXIMICS.exe	Reusable UX...	Microsoft® ...	O=Microsoft...	c:\program files\ruxim\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	taskhostw.exe	Host Proces...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	sppsvc.exe	Microsoft So...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	SppExtCom...	KMS Connec...	Microsoft® ...		c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	sc.exe	Service Con...	Microsoft® ...		c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	UpdateNotifi...	Update Noti...	Microsoft® ...	O=Microsoft...	c:\windows\system32\...
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	RUXIMICS.exe	Reusable UX...	Microsoft® ...	O=Microsoft...	c:\program files\ruxim\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	CONHOST.EXE	Console Win...	Microsoft® ...		c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	RUNDLL32.EXE	Windows ho...	Microsoft® ...		c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	GoogleUpda...	Google Inst...	Google Update	O=Google L...	c:\program files (x86)\...
	17.02.2022 1...	W10-CLI2.DEMO.LAB	DEMO\USER...	CTFMON.EXE	CTF Loader	Microsoft® ...		c:\windows\system32\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	DEMO\USER...	EXPLORER....	Windows Ex...	Microsoft® ...	O=Microsoft...	c:\windows\
	17.02.2022 1...	W10-CLI2.DEMO.LAB	DEMO\USER...	ShellExניה	Windows Sh...	Microsoft® ...	O=Microsoft...	c:\windows\exploraman

Рисунок 58 – «Протокол приложений»

Поскольку, согласно заданию, необходимо запретить создание скриншотов в Excel или Calc, нужно сначала этот табличный препроцессор открыть на клиентской машине – w10-cli1. Перейдите к соответствующей виртуальной машине и откройте LibreOffice (или Excel). Для того чтобы найти приложения воспользуйтесь поиском Windows: для Excel – введите запрос «Excel»; для Calc – введите запрос «LibreOffice Calc». Откройте табличный препроцессор и дождитесь полного запуска, после чего вернитесь к Device Monitor Console. Обновите вкладку «Приложения» (войдите в любую другую вкладку и вернитесь обратно) и найдите в колонке «Имя приложения» имя «scalc.exe», что соответствует LibreOffice Calc. Кликните по строке правой кнопкой мыши и, в контекстном меню, выберите «Добавить приложение в список вручную» и в открывшемся окне «Создать новый...», назовите новый список произвольным именем (рекомендую называть в соответствии с создаваемым правилом), а затем добавьте приложение в список.

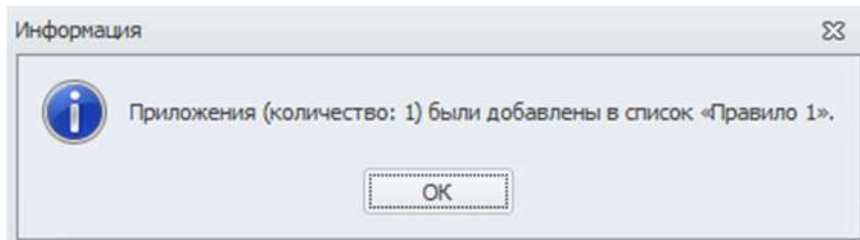
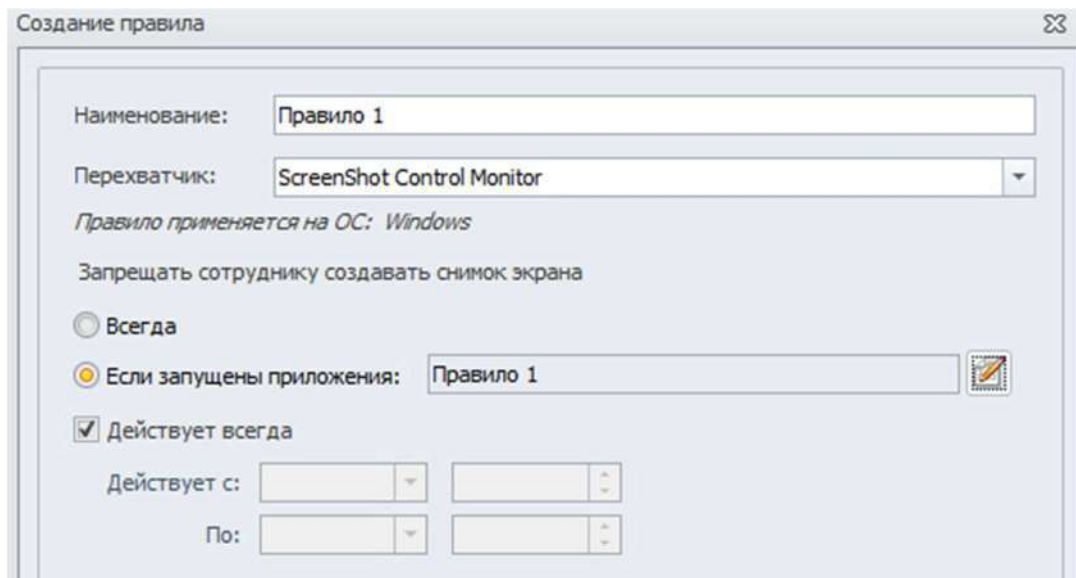


Рисунок 59 – «Успешное добавление приложения»

Вернитесь во вкладку «Политики», выберите политику «Отдел 1» и нажмите уже знакомую кнопку «Создать правило...» и назовите его «Правило 1». В качестве перехватчика установите ScreenShot Control Monitor. Отметьте радиобокс (кружочек для выбора) «Если запущены приложения:» в пункте «Запрещать сотруднику создавать снимок экрана». При отметке радиобокса, вас попросят выбрать список приложений – выберите ранее созданный список «Правило 1». Все должно выглядеть в соответствии с рисунком 60. Сохраните правило. На этом, создание правила 1 окончено, перейдем ко правилу 2.



Создание правила

Наименование:

Перехватчик:

Правило применяется на ОС: *Windows*

Запрещать сотруднику создавать снимок экрана

☐ Всегда

☒ Если запущены приложения:

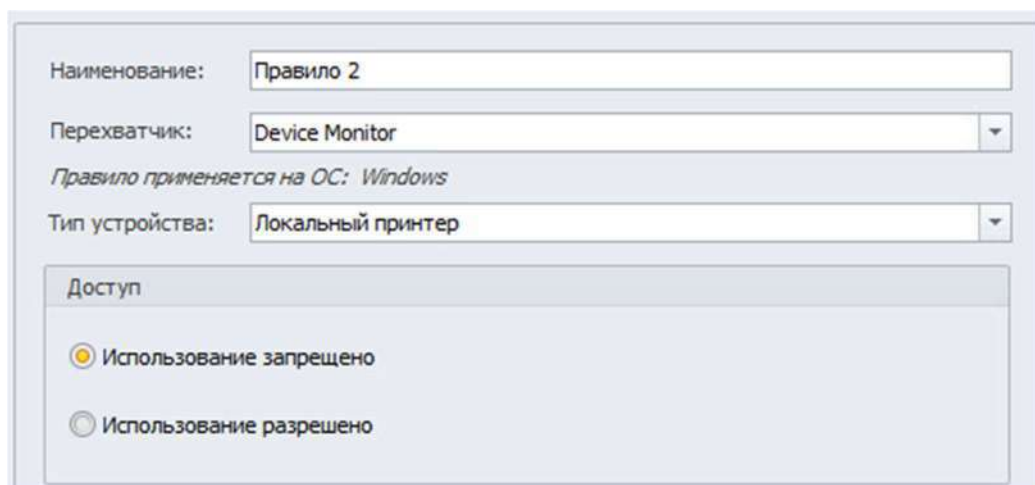
☒ Действует всегда

Действует с:

По:

Рисунок 60 – «Правило 1»

Согласно заданию, в правиле 2 необходимо запретить печать на локальных принтерах, но при этом оставить возможность печати на сетевых принтерах. Создайте новое правило, назовите его «Правило 2» и установите «Device Monitor» в качестве перехватчика. Тип устройства – Локальный принтер, доступ – использование запрещено. Все должно быть в соответствии с рисунком 61. Сохраните правило и выйдите.



Наименование:

Перехватчик:

Правило применяется на ОС: *Windows*

Тип устройства:

Доступ

☒ Использование запрещено

☐ Использование разрешено

Рисунок 61 – «Правило 2»

Правило 3 требует от вас заблокировать копирование исполняемых файлов .exe на USB-накопители. Однако, по какой-то неизвестной причине, это невозможно в актуальной версии IWDM. Поэтому, правило хоть и будет создано, однако не сможет функционировать правильно, поскольку радиобокс (кружочек для выбора) «Запретить копирование и создавать событие» попросту не активен. Создайте правило в соответствии с рисунком 62, сохраните и перейдите к следующему правилу.

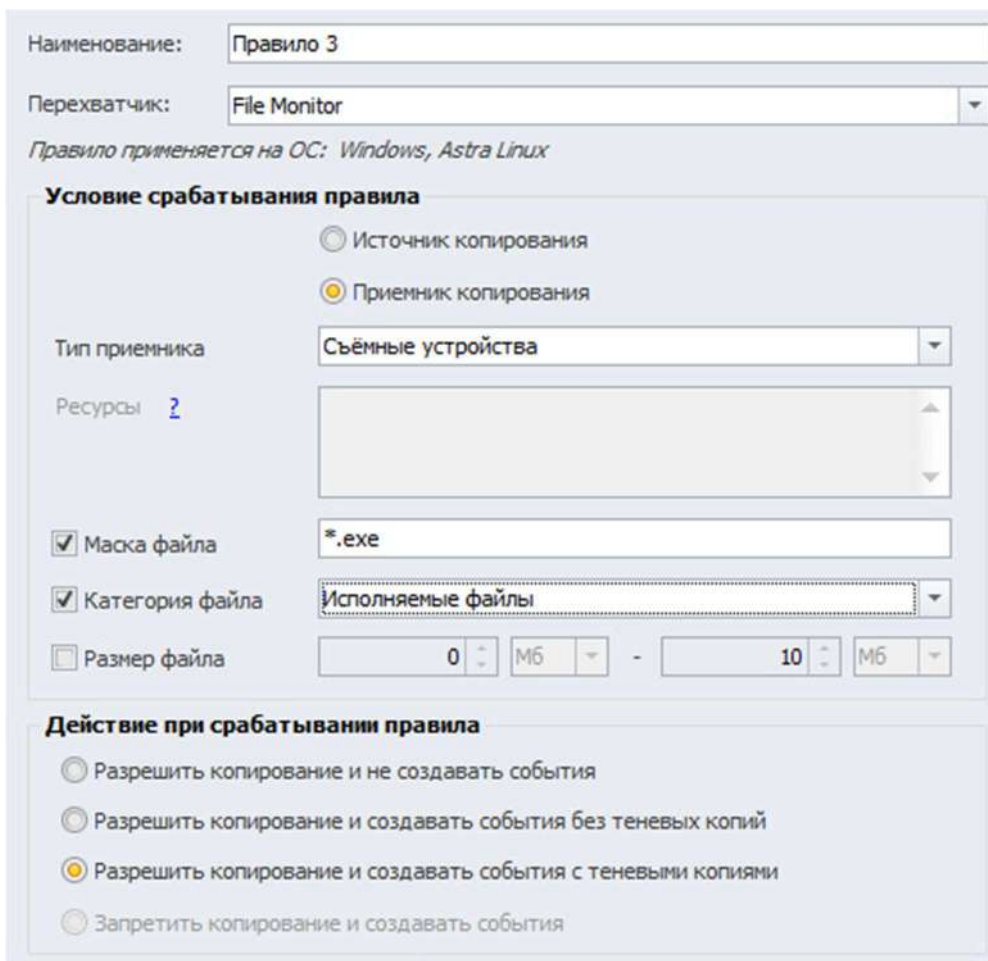


Рисунок 62 – «Правило 3»

Согласно правилу 4 нужно запретить загрузку файлов на FTP, но при этом разрешить скачивание. Тут все просто, создайте правило в соответствии с рисунком 63, сохраните правило и перейдите к созданию правил для политики «Отдел 2».

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Условия срабатывания правила

FTP адреса [?](#)

☐ Размер файла КБ - КБ

Действие при срабатывании правила

- ☐ Разрешить скачивать и записывать на FTP. Не создавать события
- ☐ Разрешить скачивать и записывать на FTP. Создавать события с теневыми копиями для случаев записи
- ☐ Разрешить скачивать и записывать на FTP. Создавать события без теневых копий для случаев записи
- ☒ Разрешить скачивать из FTP. Запретить записывать на FTP. Не создавать события.
- ☐ Запретить вход на FTP адреса

Рисунок 63 – «Правило 4»

Правила для Отдела 2:

Правило 5

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

Правило 6

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.

Правило 7

На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP, а в группе компьютеров по умолчанию необходимо контролировать буфер обмена при копировании из/в терминальных сессий.

*Проверить работоспособность попыткой копирования текста из сеанса RDP и зафиксировать выполнение скриншотом как блокировки, так и контроля.
Для работы RDP может потребоваться дополнительная настройка.*

Правило 8

Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad).

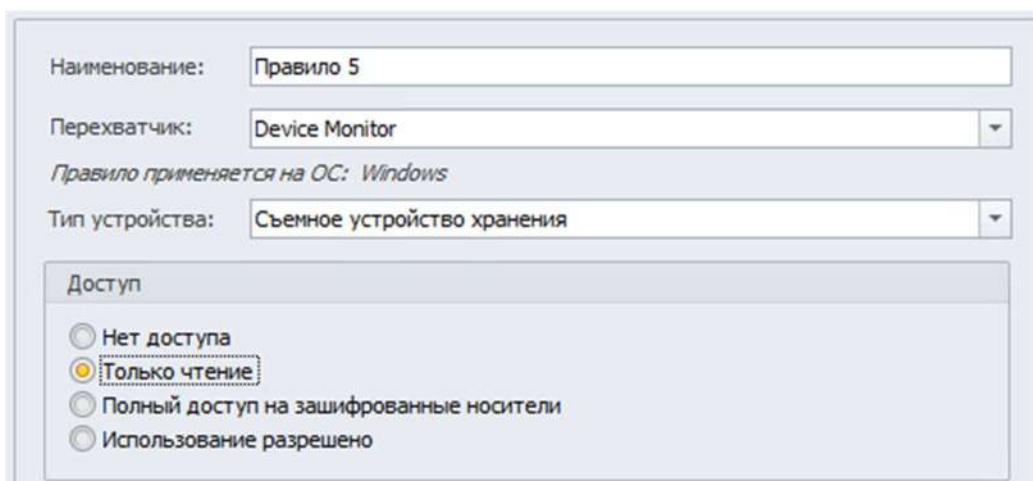
Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

Правило 9

Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mkv, *.mp4) в общих папках компании. Отдельно контролировать файлы больше 10 Мбайт и меньше 10 Мбайт. (1 Мбайт = 1000 Кбайт)

Проверить работоспособность и зафиксировать выполнение скриншотом

На вкладке «Политики» выберите политику «Отдел 2». Нажмите знакомую кнопку «Создать правило...» и начните создавать правило 5. Правило 5 требует от вас требуется запретить запись файлов на все съемные носители информации (флешки), оставив возможность возможности чтения и копирования с них. Создайте правило в соответствии с рисунком 64 и сохраните его.



Наименование:

Перехватчик:

Правило применяется на ОС: *Windows*

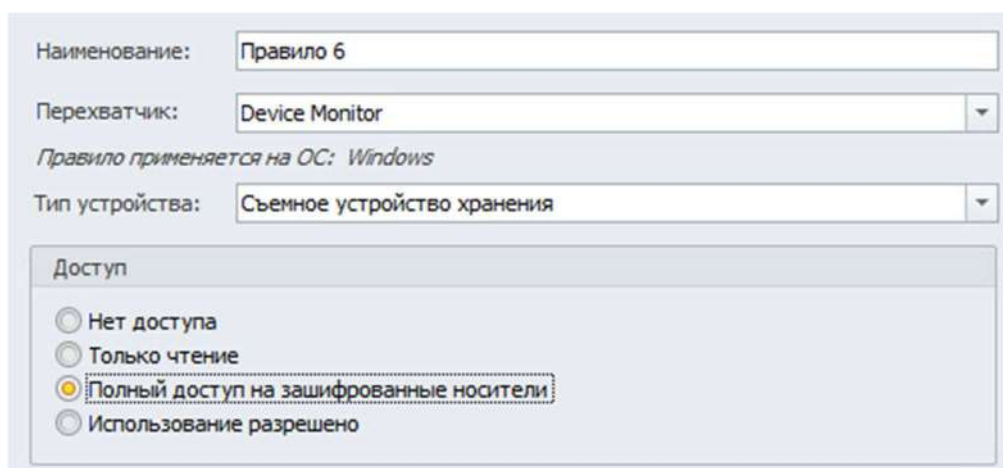
Тип устройства:

Доступ

- ☐ Нет доступа
- ☒ Только чтение
- ☐ Полный доступ на зашифрованные носители
- ☐ Использование разрешено

Рисунок 64 – «Правило 5»

Согласно правилу 6, вы должны разрешить запись файлов на доверенный носитель. Это правило частично противоречит правилу 5, однако так и должно быть. Создайте правило в соответствии с рисунком 65 и сохраните его.



Наименование:

Перехватчик:

Правило применяется на ОС: *Windows*

Тип устройства:

Доступ

- ☐ Нет доступа
- ☐ Только чтение
- ☒ Полный доступ на зашифрованные носители
- ☐ Использование разрешено

Рисунок 65 – «Правило 6»

Согласно правилу 7, вы должны запретить использование буфер обмена при подключении к удаленным машинам по RDP, а в группе компьютеров по умолчанию необходимо контролировать буфер обмена при копировании из или в терминальные сессии. В данном задании затрагивается не только политика «Отдел 2», но и «Политика на устройства» (создающаяся по умолчанию), к которой относится группа компьютеров по умолчанию. Для начала сделаем правило для политики «Отдел 2». Поскольку подключение по RDP подразумевает использование какого-либо приложения, перейдите к виртуальной машине w10-cl12 (ВМ отдела 2) и откройте приложение, чтобы в последующем создать список приложений для правила. Необходимое приложение – «Подключение к удаленному рабочему столу», чтобы открыть его, нажмите комбинацию клавиш Windows + R и в открывшемся окне введите «mstsc» (без кавычек).

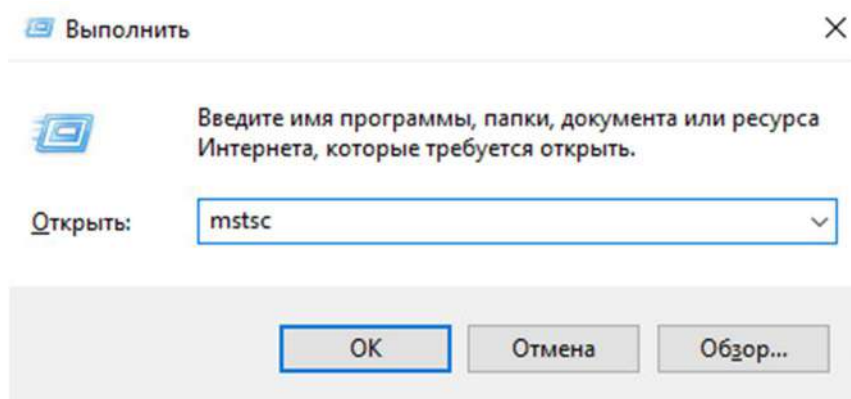


Рисунок 66 – «Открытие подключение к удаленному рабочему столу»

Теперь вернитесь к Device Monitor Console и создайте список приложений для правила, добавив в него «mstsc.exe». Вернитесь к политике «Отдел 2» и создайте правило в соответствии с рисунком 67. Затем, перейдите к политике «Политика на устройства» и создайте правило в соответствии с рисунком 68.

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Запрет запуска приложений

☐ Запретить запуск приложений с использованием списков

Белые списки (неактивны)

Запрет всех приложений, кроме указанных в списке

Черные списки (активны)

Блокируются приложения из списка

Смена режима белые/черные списки [здесь](#)

Запрет буфера обмена

☐ В терминальной сессии между разными рабочими станциями (для любых приложений)

☒ В приложениях из списка

Запрет печати

☐ В приложениях из списка

Тип принтера

☒ Локальный

☒ Сетевой

☒ Терминальный

Рисунок 67 – «Правило 7»

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Перехватывать вставку из буфера обмена

☒ В приложения терминальной сессии

☐ В приложения кроме терминальных сессий

☐ В пределах одного и того же приложения

☐ Создавать снимки экрана при копировании в буфер обмена и вставке из него

Рисунок 68 - «Правило 7, ч. 2»

Правило 8 требует от вас поставить на контроль буфер обмена в текстовых препроцессорах (Word, Writer или Wordpad). Как вы понимаете, нужно создать список приложений, а для этого перейти к виртуальной машине w10-cli2. В актуальном на февраль 2022 года образе, есть Writer и WordPad, открыть их нужно

оба. Что бы открыть их воспользуйтесь поиском Windows: для LibreOffice Writer – LibreOffice Writer, для WordPad – WordPad. Открыв оба приложения, вернитесь к Device Monitor Console. Во вкладке «Приложения» найдите «WORDPAR.exe» и «swriter.exe», после чего создайте список «Правило 8» и добавьте их к списку. Перейдите к политике «Отдел 2» и создайте правило в соответствии с рисунком 69.

Наименование:

Перехватчик:

Правило применяется на ОС: Windows

Перехватывать вставку из буфера обмена

☒ В приложения терминальной сессии

☒ В приложения кроме терминальных сессий

☐ В пределах одного и того же приложения

☐ Создавать снимки экрана при копировании в буфер обмена и вставке из него

Рисунок 69 - «Правило 8»

Правило 9 требует отслеживать движение видео контента (*.avi, *.mkv, *.mp4) в общих папках компании, при этом нужно отдельно контролировать файлы больше 10 Мбайт и меньше 10 Мбайт. На этом шаге понадобится создать два правила, так как Device Monitor не устанавливает два критерия размера файлов в одном правиле. Создайте правило 9 и правило 9.1 по аналогии с рисунками 70 и 71.

Наименование:

Перехватчик:

Правило применяется на ОС: *Windows, Astra Linux*

Условие срабатывания правила

☒ Источник копирования
☐ Приемник копирования

Тип источника:

Ресурсы:

☐ Маска файла:

☐ Категория файла:

☒ Размер файла: МБ - МБ

Действие при срабатывании правила

☐ Разрешить копирование и не создавать события
☐ Разрешить копирование и создавать события без теневых копий
☒ Разрешить копирование и создавать события с теневыми копиями
☐ Запретить копирование и создавать события

Рисунок 70 - «Правило 9»

UNC ПУТЬ НЕ ВПИСЫВАЕТСЯ???

По окончании работы с Device Monitor Console ОБЯЗАТЕЛЬНО нажмите кнопку «сохранить» на уведомлении о том, гласящем, что в схему безопасности были внесены изменения.

В схему безопасности были внесены изменения. Сохранить изменения?

Рисунок 71 - «Уведомление об изменении схемы безопасности»

Модуль 3: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Создайте в системе InfoWatch Traffic Monitor политики безопасности согласно нижеперечисленным заданиям.

- Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.
- Некоторые политики должны быть созданы с нуля, некоторые могут быть сделаны путём модификации существующих в системе.
- Для некоторых политик необходима работа с разными разделами консоли управления ТМ: 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, участник должен самостоятельно задать уровень угрозы при разработке политики).
- Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании
- После создания всех политик будет запущен автоматический «генератор трафика», который передаст на InfoWatch Traffic Monitor поток данных, содержащих как утечки, так и легальную информацию.
- При правильной настройке политики InfoWatch Traffic Monitor 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.
- В комплексных заданиях необходимо пользоваться объектами защиты.
- Задания можно выполнять в любом порядке.
- 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 «Additional files» в datastore1.

- 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 на рабочем столе 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

ВНИМАНИЕ! Необходимо называть политики/объекты/категории/тэги и т.п. ТОЛЬКО в соответствии с номером и названием задания:

Политики — Политика XX, например «**Политика 5**». Для комбинированных политик формат: **Политика 5.1, Политика 5.2** и т.д.

Объект защиты — Объект и XX, например «**Объект 11**».

Ошибки в названиях приводят к снижению баллов или даже к невозможности проверки. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.

ВНИМАНИЕ! ВСЕ политики «по-умолчанию», находящиеся в IWTM на момент старта соревнований, должны быть отключены или удалены

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

Задание 1

Создайте список веб-ресурсов и назовите его «Сайты партнеров». Туда необходимо включить следующие веб-ресурсы:

kb.infowatch.com, worldskills.moscow, worldskills.ru, infotecs.ru

Задание 2

Для правильной работы системы необходимо настроить периметр компании:

Домен: demo.lab.

Список веб ресурсов: Сайты партнеров

Группа персон: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Политика 1

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика (до ≈50%) как внутри компании, так и за ее пределы. Фотография котика есть в дополнительных данных.

Вердикт: Заблокировать ✗

Уровень нарушения: низкий ●

Тег: Политика 1

Политика 2

В последнее время бюджет компании стал резко падать. Подозрения пали на главного бухгалтера, директор подозревает его в проведении денежных средств «мимо кассы». В связи с этим необходимо отслеживать передачу всех номеров и сканов кредитных карт, отправляемых из отдела Бухгалтерии

Вердикт: Заблокировать ✗

Уровень нарушения: высокий ●

Тег: Политика 2

Политика 3

Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний. Критичными данными в выгрузке являются телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД и ОКОПФ и в 1 документе присутствует более 5 компаний. Для настройки используйте файл `stock_members_details_catch.csv`.

Вердикт: Разрешить Ö

Уровень нарушения: низкий ●

Тег: Политика 3

Политика 4

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 следующие номера: 777 и 315) - (дефис) от 1 до 3 букв (кириллица, верхний регистр) Например: jDT-123-Л , kSR-665-ЪГА Не должно быть срабатывания на следующие номера грузов (например: kdO-315-ю или jtfd-777-ШАП). Необходимо контролировать передачу, а также копирование на съемные носители и печать вышеуказанных данных. Проверить работоспособность. Учтите, что особо обобщенные регулярные выражения лучше разделить на несколько текстовых объектов для оптимизации поиска.

Вердикт: Разрешить Ö

Уровень нарушения: средний ●

Тег: Политика 4

Политика 5

Необходимо создать политики для отслеживания документов (передача и копирование), содержащих договор компании (договор компании.docx).

Политики должны работать следующим образом (за периметр компании):

1. Если передается только договор компании (шаблон и заполненный шаблон, до 25% изменений) – разрешать передачу, уровень угрозы низкий, тег «Политика 5.1».
2. Если передается договор компании, в котором присутствует фамилия

генерального директора, а также главного бухгалтера – разрешать передачу, уровень угрозы средний, дополнительный тег «Политика 5.2». Политика не должна срабатывать, если в документе только фамилия директора или только фамилия бухгалтера.

3. Если передается договор компании, в котором присутствует фамилия генерального директора, главного бухгалтера, а также стоит печать компании (ООО Повозка) – разрешить передачу, уровень угрозы высокий, тег «Политика 5.3».

Проверить работоспособность. Политики не должны срабатывать внутри компании, только при передаче за периметр.

Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 5.1, Политика 5.2, Технология 5.3 и т.д.)

Вердикт 1: Разрешить Ö

Уровень нарушения 1: низкий •

Тег 1: Политика 5.1

Вердикт 2: Разрешить Ö

Уровень нарушения 2: средний •

Тег 2: Политика 5.2

Вердикт 3: Заблокировать ✗

Уровень нарушения 3: высокий •

Тег 3: Политика 5.3

Политика 6

Стало известно, что сотрудники охраны (Security) ООО «Повозка» за определенную сумму пропускают автомобили из близлежащих домов на служебную парковку. В связи с ужесточением корпоративной политики в компании, правом въезда на территорию обладает только генеральный директор.

Сотрудники охраны ведут журнал учета автомобилей в электронном виде и обмениваются между собой данными о припаркованных автомобилях.

Необходимо детектировать номера всех автомобилей, которые незаконно парковались на частной территории компании ООО «Повозка», исключая номер автомобиля генерального директора K333OT777.

Буквы, используемые в автомобильных номерах:

А, В, Е, К, М, Н, О, Р, С, Т, У, Х (Верхний регистр)

Цифры, используемые в автомобильных номерах:

000 – 999

Регионы автомобильных номеров, подлежащие детектированию:

77, 97, 99, 177, 197, 199, 777, 799

Вердикт: заблокировать ✖

Уровень нарушения: Высокий ●

Тег: Политика 6

Политика 7

В честь юбилея компании была запущена акция с промокодами на скидку в 50% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов, в связи с этим необходимо контролировать защитить учечку текстового документа, содержащего промокоды («промокоды.docx»). Стоит учесть, что сотрудники могут воспользоваться жестким диском или флеш-накопителем, для того чтобы завладеть акционными купонами, а также слить не весь файл, а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах, а также отслеживать копирование этой информации на внешние носители, тег «Политика 7»

Проверить работоспособность на все купоны и на 1-2 купона.

Вердикт: заблокировать ✖

Уровень нарушения: средний ●

Тег: Политика 7

Политика 8

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела кадров отправлять сканы/скриншоты и документы, содержащие информацию о СНИЛС, ИНН, паспортных данных (в текстовом и графическом виде) за пределы компании.

Извлечение текстовых данных из сканированных документов, а также скриншотов подразумевает использование технологии OCR. Необходимо включить данную технологию (ABBYY), используя лицензию, которая

находится в папке дистрибутивов. (подробнее см. в доп. карточке задания)

Вердикт: заблокировать ✗

Уровень нарушения: средний ●

Тег: Политика 8

Политика 9

Два месяца назад в компании DemoLab заметили, что сотрудница отдела кадров расходует в три раза больше бумаги, чем прежде, хотя объем работ не был увеличен. Путем наблюдения за сотрудницей было установлено, что она, состоя в совете школьной родительской общности, регулярно собирает деньги с родителей за печать докладов и рефератов учеников класса, бесплатно распечатывая их в компании.

Необходимо создать политику безопасности, которая будет включать слова (с учетом морфологии): «реферат», «доклад», «ученик», «школа», «класс».

Проверку необходимо проверить путем отправки документа на печать и при помощи электронной почты.

Вердикт: Заблокировать ✗

Уровень нарушения: низкий ●

Тег: Политика 9

Политика 10

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 5%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 (пяти) популярных на данный момент сериалов при передаче через веб-сообщения и почту.

Список сериалов:

Ривердэйл, Сестра Рэтчед, Племена Европы, Сквозь снег, Варвары

Вердикт: разрешить ✓

Уровень нарушения: низкий ●

Тег: Политика 10

Политика 11

Оказалось, что сотрудники не только обсуждают сериалы, а еще и обмениваются ссылками и torrent-файлами для их скачивания, после чего скачивают их, используя интернет-канал компании или обмениваются скачанным материалом внутри компании, что также нагружает сеть и заполняет ненужными данными локальные диски пользователей.

В связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов формата .torrent и ссылок формата magnet: (и содержащей urn (хеш) файла). Ложных срабатываний просто на слово Magnet (в т.ч. с двоеточием) быть не должно.

Стоит учесть, что magnet-ссылки могут передаваться в том числе через буфер обмена в пределах браузера Google Chrome.

Вышеуказанными данными сотрудники могут обмениваться не только внутри компании.

Для торрент-файлов и ссылок:

Вердикт: запретить ✖

Уровень нарушения: средний ●

Тег: Политика 11

Политика 12

У директора компании скоро юбилей и сотрудники решили его поздравить, сделав коллаж из его фотографий. Для того чтобы данное поздравление не попало к директору раньше срока, необходимо контролировать передачу фотографий директора, как внутри компании, так и за его пределами. Критичным является минимум 20%-ное совпадение передаваемого фото.

Вердикт: разрешить ✔

Уровень нарушения: низкий ●

Тег: Политика 12

Политика 13

При переезде в новый просторный офис, компанией ООО Demo Lab был расширен штаб сотрудников — было решено взять несколько десятков выпускников технических вузов на стажировку. Для того, чтобы они работали более эффективно, директор компании предложил отслеживать доступ

сотрудникам, работающим в отделе ИТ, доступ к основным социальным сетям и анонимным имиджбордам – vk.com, ok.ru, t.me, 4chan.com, reddit.com

Контроль для тестовых целей установить за электронными письмами в эти доменные зоны.

Вердикт: разрешить ✓

Уровень нарушения: средний ●

Тег: Политика 13

Политика 14

Сотрудники и партнеры компании стали получать большое количество различных рекламных сообщений на мобильные номера, в связи с чем возникло подозрение о том, что кто-то производит «слив» номеров из баз данных компании путем передачи информации за пределы компании через браузер, почту или флешки.

Необходимо контролировать передачу как минимум 3 мобильных номеров в 1 сообщении, т.к. передача всего одного номера не является потенциальным сливом данных (может быть просто контактной информацией).

Мобильные номера могут быть только операторов РФ (код страны 7, код оператора начинается с 9), в различных форматах, например:

+7 (987) 123-45-67, +79871234567, +7 987 123 4567, 8-987 123-4567 и т.д.

Необходимо учесть все варианты, в т.ч. без кода страны, кода выхода на городскую телефонную сеть, комбинации пробелов, скобок, дефисов.

Вердикт: разрешить ✓

Уровень нарушения: Высокий ●

Отправить уведомление: офицеру безопасности

Тег: Политика 14

Политика 15

Необходимо поставить на мониторинг все зашифрованные и запароленные данные, так как попытки передачи таких данных несут потенциальную опасность утечки.

Проверить работоспособность.

Вердикт: разрешить ✓

Уровень нарушения: низкий ● **Тег:** Политика 15

Для создания политики, перейдите к веб-интерфейсу Traffic Monitor и в верхней части интерфейса перейдите ко вкладке «Политики». Перед созданием новых политик обязательно удалите все существующие.

Задание 1:

В веб-интерфейсе Traffic Monitor, в верхней части сайта перейдите ко вкладке «Списки» и из контекстного меню выберите «Веб-ресурсы». В левой части найдите кнопку «Создать список веб-ресурсов». Назовите его «Сайты партнеров».

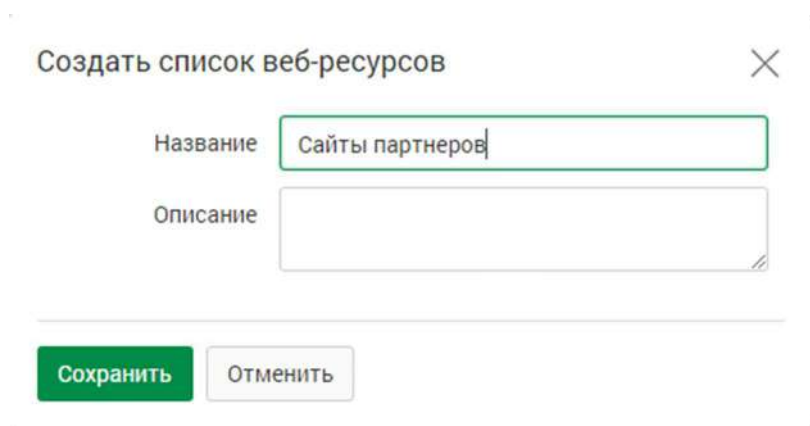


Рисунок 72 – «Создание список веб-ресурсов»

Перейдите к созданному списку и нажмите кнопку «Добавить веб-ресурс» и начните добавьте следующие ресурсы: kb.infowatch.com, worldskills.moscow, worldskills.ru, infotecs.ru.

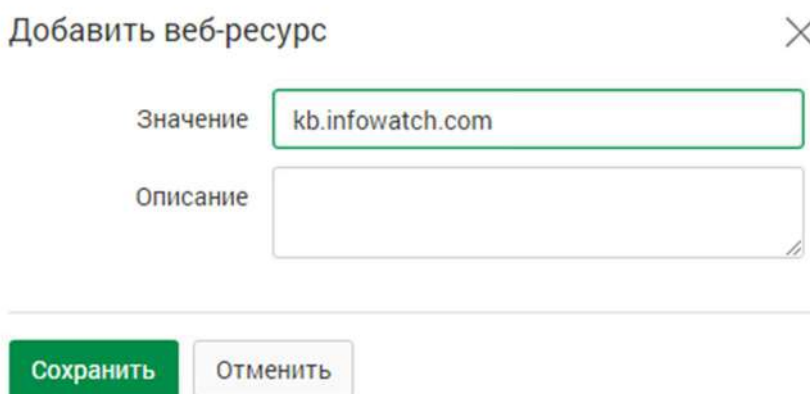


Рисунок 73 – «добавление веб-ресурсов»

Задание 2:

Для настройки периметра компании перейдите ко вкладке «Списки» и в выпадающем меню выберите «Периметры». Периметр «Компания» создается изначально, откройте его и приступите к редактированию. Необходимо указать домен (demo.lab), список веб ресурсов («Сайты партнеров») и группу персон («пользователи домена»).

Редактирование

Название: Компания

Список веб-ресурсов: Сайты партнеров ×

Почтовый домен: @ demo.lab ×

Группа персон: Domain Users ×

☐ Использовать только рабочие контакты

Добавить

Описание: Персоны и компьютеры компании. Используется для контроля информации, передаваемой за периметр компании.

Создан: 17.11.2021 05:29 Изменен: 17.11.2021 05:29

Сохранить Отменить

Рисунок 74 – «Изменение периметра компании»

Сохраните примененные изменения.

Вам также необходимо исключить из перехвата почту генерального директора. Для этого перейдите к периметру «Исключить из перехвата».

Редактирование

Название: Исключить из перехвата

Адрес электронной почты: kornilov@demo.lab ×

Добавить

Описание: Если включена политика 'Исключить из перехвата', то почтовые сообщения, отправленные входящими в данный периметр персонами,

Создан: 17.11.2021 05:29 Изменен: 17.11.2021 05:29

Сохранить Отменить

Рисунок 74 – «Изменение периметра компании»

Политика 1:

Необходимо создать политику, которая запретит обмен фотографией котике и ее немного измененной версией. Для того, чтобы добавить саму фотографию в Traffic Monitor и в последующем работать с ней, перейдите во вкладку технологии, и в выпадающем меню выберите «Эталонные документы».

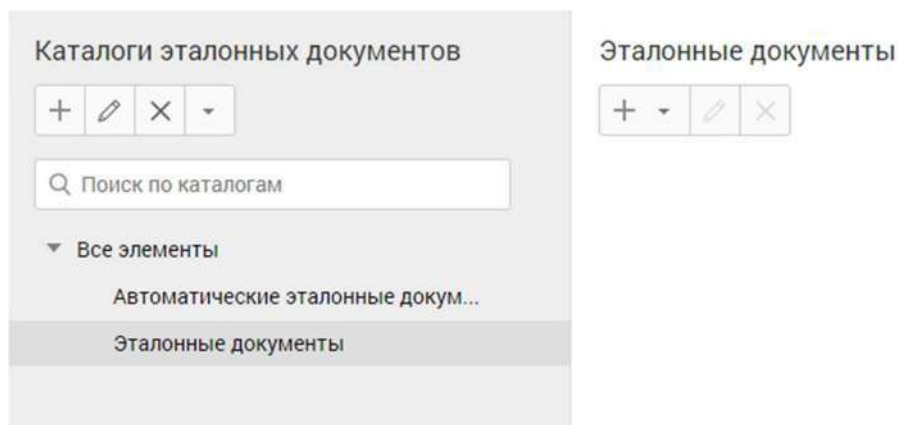


Рисунок 75 – «Эталонные документы»

Найдите кнопку «Создать», располагающуюся под текстом «Каталоги эталонных документов» и создайте новый каталог, назовите его «Политика 1». Установите порог цитируемости для бинарных данных на 50%.

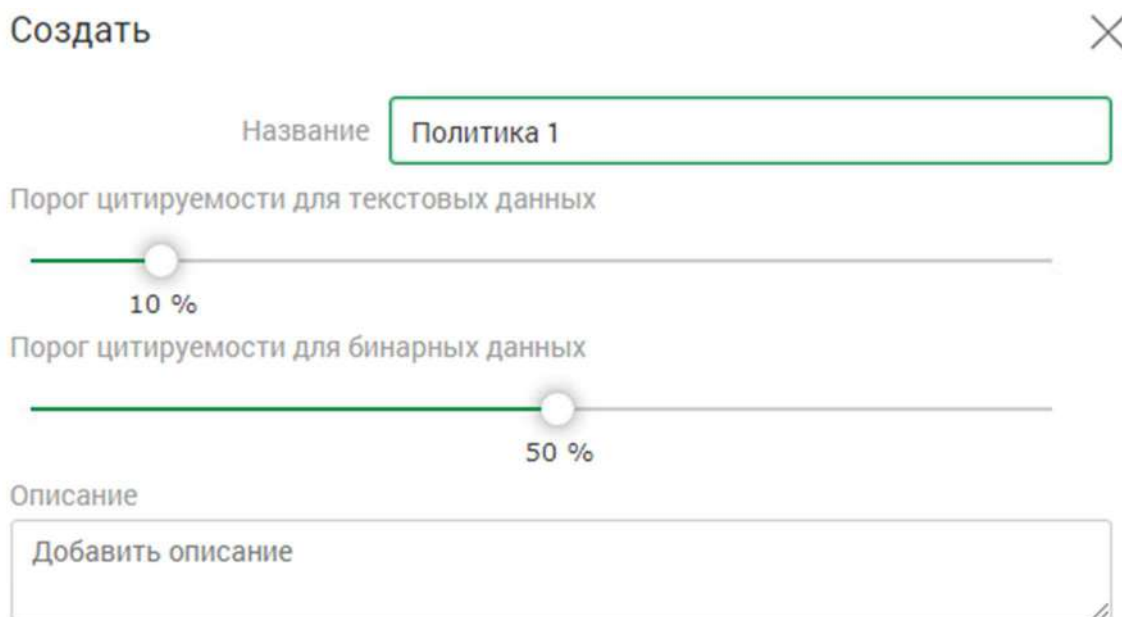


Рисунок 76 – «Создание каталога эталонных документов»

Перейдите к созданному каталогу и нажмите кнопку «+» для добавления

эталонного документа. В выпадающем меню выберите «На основе всех типов данных». Загрузите фотографию котика из открывшегося окна приложения Проводник. Настройки документа автоматически будут синхронизированы с настройками каталога. После добавления котика в эталонные документы, перейдите ко вкладке «Объекты защиты» и найдите кнопку «Создать», находящуюся под текстом «Каталоги объектов защиты» и создайте каталог «Политика 1» (политика защиты данных).

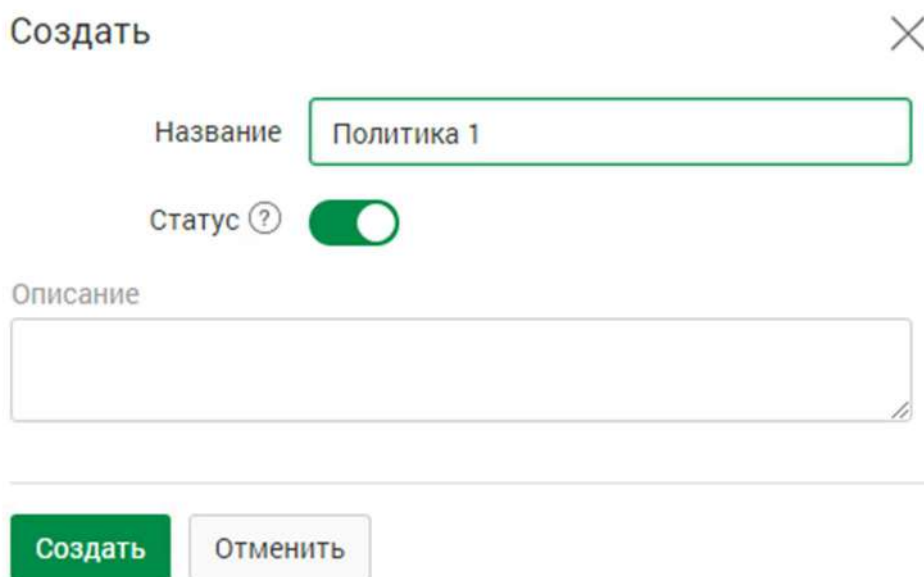


Рисунок 78 – «Создание каталога объектов защиты»

Перейдите к созданному каталогу и нажмите кнопку «Создать», в открывшемся окне создания объекта защиты перейдите ко вкладке «Эталонные документы», перейдите к созданному ранее каталогу и выберите фотографию котика. После чего будет предложено выбрать условие обнаружения – выберите котиков. Сделайте все в соответствии с рисунком 79.

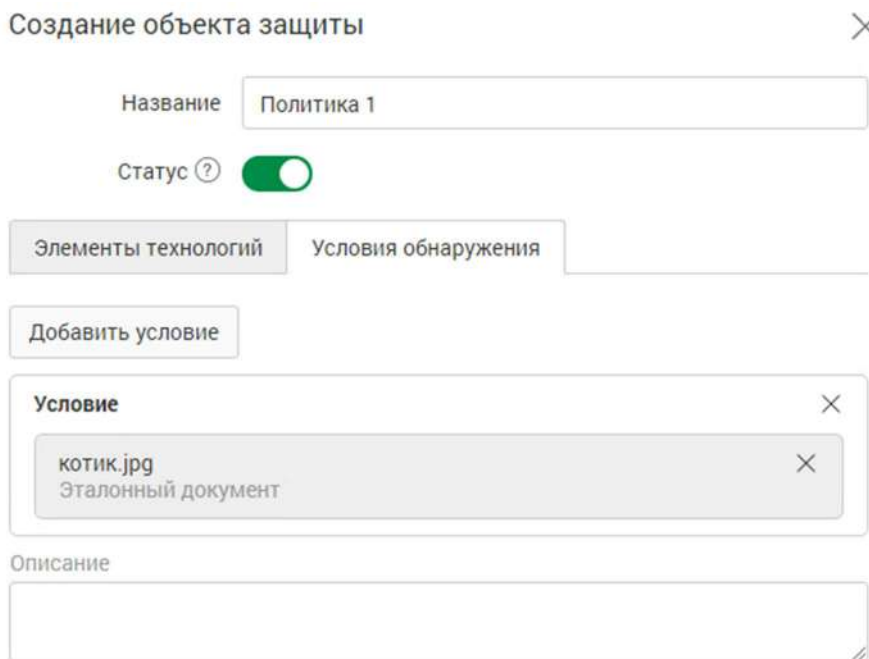


Рисунок 79 – «Создание объекта защиты»

После создания объекта защиты перейдите во вкладку «Списки» и в выпадающем меню выберите «Теги». Создайте новый тег «Политика 1»

Вернувшись ко вкладке «Политики» найдите созданную политику «Политика 1».

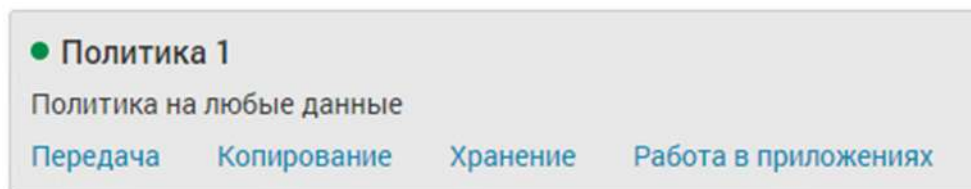


Рисунок 80 – «Политика 1»

Согласно заданию, политика должна ограничивать передачу картинки котика как в рамках компании, так и за ними. Нажмите на кнопку «Передача», а затем на кнопку «Создать правило», чтобы создать правило, которое ограничит движение картинки. Настройте правило в соответствии с рисунком 81. По окончании создания правила обязательно сохраните его.

Правило передачи

Направление маршрута	<input type="radio"/> В одну сторону <input checked="" type="radio"/> В оба направления	
Тип события	<div>Тип ▾</div>	
Компьютеры	<div> <div>DEMO-DC ×</div> <div>DEMOLAB ×</div> <div>IWDM ×</div> <div>W10-CLI1 ×</div> <div>W10-CLI2 ×</div> </div> <div>+</div>	
Отправители ?	<div>= ▾</div>	<div>Начните вводить текст</div> <div>+</div>
Получатели ?	<div>= ▾</div>	<div>Начните вводить текст</div> <div>+</div>
Дни действия правила	<div>Любой день недели ▾</div>	
Часы действия правила	<div>0:00 ⌚ - 0:00 ⌚</div>	

Действия при срабатывании правила

Отправить почтовое уведомление ?	<div>Начните вводить текст</div> <div>+</div>
Назначить событию вердикт	<div>⛔ Заблокировать ▾</div>
Назначить событию уровень нарушения	<div>● Низкий ▾</div>
Назначить событию теги	<div> <div>Политика 1 ×</div> <div>+</div> </div>
Назначить отправителю статус	<div>Выберите статус ▾</div>
Удалить событие	<div><input type="checkbox"/></div>

Рисунок 81 – «Правило передачи политики 1»

Политика 2:

Согласно заданию, необходимо отслеживать передачу всех номеров и сканов кредитных карт, которые отправляются из отдела Бухгалтерии. В этот раз дополнительно ничего загружать не потребуется, так как в Traffic Monitor уже присутствуют такие технологии.

Перейдите ко вкладке «Объекты защиты» и создайте новый каталог объектов защиты – «Политика 2». В новый каталог добавьте три объекта защиты: Графический объект: Кредитная карта; Текстовый объект: номер кредитной карты; Текстовый объект: номер кредитной карты (16 цифр). Важным моментом при добавлении объектов защиты, является отметка чекбокса (квадратик для выбора) «Создать объект защиты на каждый выбранный элемент».

Создание объекта защиты

Категории Текстовые объекты 2 Эталонные документы Бланки Печати Выгрузки из БД Графические объекты

Поиск

<input type="checkbox"/>	Название	Дата создания	Описание
<input checked="" type="checkbox"/>	Кредитная карта	17.11.2021 05:29	Система срабатывает на изображение лицевой стороны б...
<input type="checkbox"/>	Паспорт гражданина РФ	17.11.2021 05:29	Система срабатывает на изображение главного разворота...

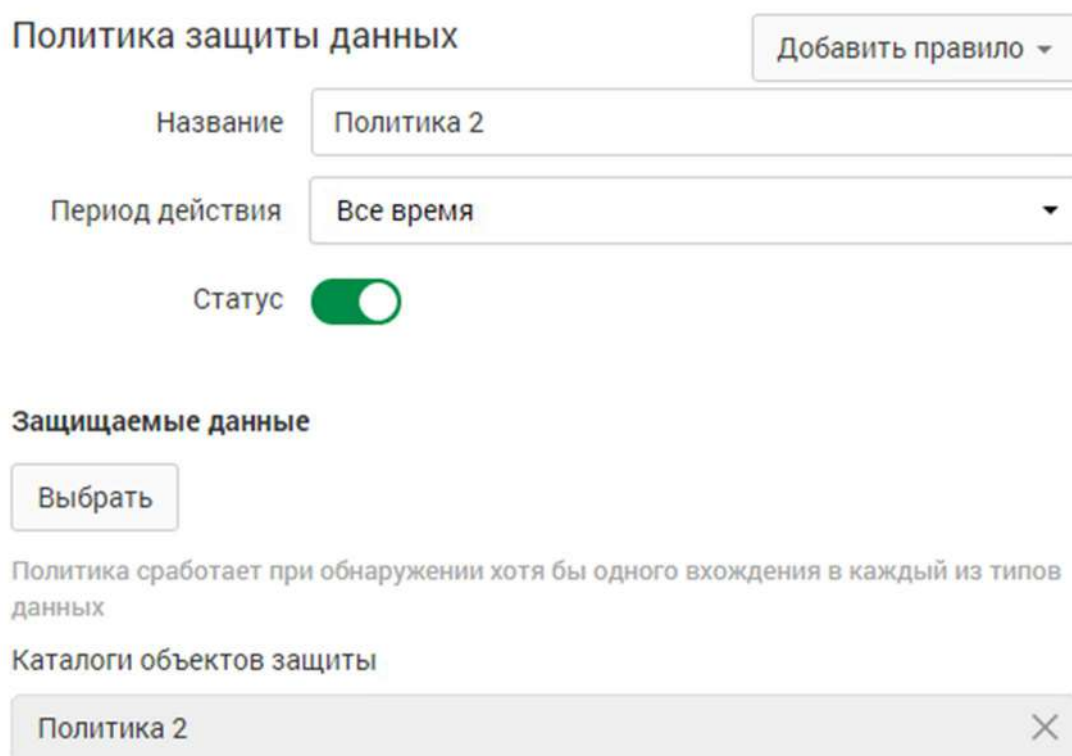
10

Создать Отменить ☒ Создать объект защиты на каждый выбранный элемент

Рисунок 82 – «Чекбокс “создать объект защиты на каждый выбранный элемент”»

После создания объекта защиты, перейдите ко вкладке «Списки» → «Теги». Создайте тег «Политика 2».

Перейдите на вкладку «Политики» и создайте новую политику - «Политика 2» (политика защиты данных). В качестве защищаемых данных выберите каталог объектов защиты «Политика 2».



Политика защиты данных Добавить правило ▾

Название

Период действия

Статус ☒

Защищаемые данные

Выбрать

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Каталоги объектов защиты

×

Рисунок 83 – «Политика 2»

Создайте новое правило передачи в соответствии с рисунком 84. Обязательно сохраните.

Правило передачи

Направление маршрута	→ В одну сторону ⇌ В оба направления	
Тип события	Тип ▾	
Компьютеры	<div> <div>🖥 W10-CLI1 ×</div> <div>🖥 W10-CLI2 ×</div> </div> <div></div> <div>+</div>	
Отправители ?	<div>= ▾</div> <div> <div>👤 Accounting ×</div> <div></div> </div> <div>+</div>	
Получатели ?	<div>= ▾</div> <div>Начните вводить текст</div> <div>+</div>	
Дни действия правила	Любой день недели ▾	
Часы действия правила	<div>0:00 ⌚</div> <div>-</div> <div>0:00 ⌚</div>	

Действия при срабатывании правила

Отправить почтовое уведомление ?	<div>Начните вводить текст</div> <div>+</div>	
Назначить событию вердикт	<div>🚫 Заблокировать ▾</div>	
Назначить событию уровень нарушения	<div>● Высокий ▾</div>	
Назначить событию теги	<div> <div>Политика 2 ×</div> <div>+</div> </div>	
Назначить отправителю статус	<div>Выберите статус ▾</div>	
Удалить событие	<div><input type="checkbox"/></div>	

Рисунок 84 – «Правило политики 2»

Политика 3:

Согласно заданию, необходимо настроить мониторинг выгрузок из БД, для контроля движения данных из базы данных страховых компаний. Критичными данными в выгрузке являются телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД и ОКОПФ если в 1 документе присутствует более 5 компаний. Поскольку готовой выгрузки из БД в Traffic Monitor не существует, ее нужно загрузить. Для загрузки выгрузки из БД перейдите в «Технологии» → «Выгрузки из БД». Создайте каталог выгрузок «Политика 3». Откройте созданный каталог и с помощью кнопки «+», загрузите в него выгрузку из БД. Затем, выберите загруженную выгрузку и нажмите кнопку «редактировать», изображенную в виде карандаша. Измените условие по умолчанию, чтобы оно совпало с условием, изображенным на рисунках 85 и 86.

Редактировать

Название

Выгрузка из БД.csv

Название файла

Выгрузка из БД.csv

Формат файла

text/csv

Режим обновления:

Ручной

Условие обнаружения

+

×

Название условия	Правило	Минимальное ко...
Условие по зада...	5 + 7 + 10 + 14 + 16 + 18	5

Описание

Введите описание

Создан: 22.02.2022 07:38

Изменен: 22.02.2022 07:38

Рисунок 85 – «Условие выгрузки из БД»

Редактировать

✕

Название условия

Условие по заданию

Минимальное количество строк

5

Условие обнаружения

5 + 7 + 10 + 14 + 16 + 18

Сохранить

Отменить

Рисунок 85 – «Условие выгрузки из БД»

Создайте тег «Политика 3». Перейдите к политикам и создайте «Политику 3» (политика защиты данных), в качестве защищаемых данных выберите каталог объектов защиты «Политика 3». Создайте новое правило передачи в соответствии с рисунком 86.

Правило передачи

Направление маршрута

→ В одну сторону ⇄ В оба направления

Тип события

Тип

Компьютеры

Начните вводить текст

+

Отправители ?

=

Начните вводить текст

+

Получатели ?

=

Начните вводить текст

+

Дни действия правила

Любой день недели

Часы действия правила

0:00

⌚

-

0:00

⌚

Действия при срабатывании правила

Отправить почтовое уведомление ?

Начните вводить текст

+

Назначить событию вердикт

✓ Разрешить

Назначить событию уровень нарушения

● Низкий

Назначить событию теги

Политика 3 ✕

+

Назначить отправителю статус

Выберите статус

Удалить событие

⏻

Рисунок 86 – «Правило передачи политики 3»

