

# КОНКУРСНОЕ ЗАДАНИЕ

**Региональные чемпионаты 2021-22**

Сокращенное типовое задание – 85 баллов

Корпоративная защита от  
внутренних угроз  
информационной  
безопасности

**Модуль 1, 3, 5**

**День 1**

Менеджер компетенции: А.В. Сергеев



## Аннотация

Документ содержит типовое конкурсное задание 2021-22 региональных чемпионатов 2021-22 года по стандартам WorldSkills Russia по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности».

Конкурсное задание разработано на базе заданий Отборочных соревнований и IV Финала национального чемпионата Ворлдскиллс 2021 года. Практические задания собрали лучшие практические задачи в области обеспечения корпоративной безопасности в организациях реального сектора экономики и были апробированы на корпоративных чемпионатах ГК Росатом, ГК Роскосмос.

Использование документа печать (тиражом до 20 экз.) и распространение разрешено только в рамках организации и проведения региональных чемпионатов Ворлдскиллс. С вопросами и замечаниями можно обращаться по адресу: [avsergeev@hse.ru](mailto:avsergeev@hse.ru)

Состав рабочей группы по разработке типового КЗ:

- **А.В. Сергеев, менеджер компетенции,**  
НИУ ВШЭ, Москва;
- **А.П. Бозров, сертифицированный эксперт,**  
ГБПОУ «Колледж связи № 54», Москва;
- **А.А. Крылова, победитель МежВУЗ 2019,**  
ФГАОУ ВО «Санкт-Петербургский государственный университет  
аэрокосмического приборостроения», Санкт-Петербург;
- **А.В. Зябухина, эксперт-компатриот призёра ФНЧ 2021,**  
ГБПОУ КК "Краснодарский колледж электронного приборостроения",  
Краснодар;
- **Н.В. Матвеев, сертифицированный эксперт,**  
ФГАОУ ВО «Санкт-Петербургский государственный университет  
аэрокосмического приборостроения», Санкт-Петербург;
- **Е.В. Трапезников, сертифицированный эксперт,**  
ФГАОУ ВО «Омский государственный технический университет» , Омск.

## Дополнительные сведения (шаблон)

### Общие сетевые настройки

Шлюз по умолчанию: 172.16.x.1 (x - номер рабочего места)

DNS сервер провайдера

DNS сервер компании

### Компьютер с виртуальными машинами:

Логин: root, пароль: xxXX1234

Документация находится в папке Temp на ПК участника

Дистрибутивы находятся в datastore1

Образы систем находятся в datastore1

### Контроллер домена (DEMO.LAB):

IP адрес: 172.16.x.2 Маска: 255.255.255.248

Домен: demo.lab

логин: administrator пароль: xxXX1234

### DLP-система (IWTM)

Локальный вход: логин: root пароль: xxXX1234

IP адрес: 172.16.x.3 Маска: 255.255.255.248

Веб консоль логин: officer пароль: xxXX1234

### Windows Server (IWDM):

Локальный вход: логин: admin пароль: xxXX1234

IP адрес: 172.16.x.4 Маска: 255.255.255.248

### Windows 10 (Client 1):

Локальный вход: логин: admin пароль: xxXX1234

IP адрес: 172.16.x.5 Маска: 255.255.255.248

Проверка правил передачи через сайт dlptest.com

**ОБЯЗАТЕЛЬНО**

Заполните файл /etc/hosts на виртуальной машине IWTM, в соответствии с дополнительными сведениями.

```
GNU nano 2.3.1      File: /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.3.2   demolab.demo.lab      demolab
172.16.3.3   iwtm.demo.lab           iwtm
172.16.3.4   iwdm.demo.lab           iwdm
172.16.3.5   w10-cli1.demo.lab       w10-cli1
172.16.3.6   w10-cli2.demo.lab       w10-cli2
```

## Модуль 1: Установка и настройка системы

### Описание

Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) одного из интеграторов DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и настроить DLP-систему на отдельном сегменте сети.

В «песочнице» развернут контроллер домена (с каталогом Active Directory), с которым необходимо будет осуществить интеграцию DLP-системы. До настройки системы необходимо подготовить доменных пользователей.

В качестве виртуальной инфраструктуры для пилотного проекта используется среда виртуализации VMware Workstation.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM).

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

Необходимо использовать следующие виртуальные машины:

- Demo (контроллер домена demo.lab)
- IWTM (предустановленный, необходимо настроить)
- Iwdm (Windows Server для IWTM, предустановленный)
- w10-cli1 (ПК первого нарушителя)
- w10-cli2 (ПК второго нарушителя)

Сетевые настройки виртуальных машин указаны в дополнительной карточке заданий.

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

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

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в папке «InfoWatch 6.11.5» на SSD.

Если в задании необходимо сделать скриншот, необходимо называть его по номеру задания, например: Задание\_5\_копирование.png.

## Задание 1: Подготовка Active Directory

**Примечание:** необходимо проверить, что данные пользователи уже не добавлены в Active Directory. Если добавлены, не выполнять повторно.

Для дальнейших работ необходимо создать подразделение организации (Organization Unit) под названием «Office», добавить в него каталоги пользователей и компьютеров (Users и Computers).

**В каталог Users необходимо добавить следующих пользователей:**

- iwdm-admin (права доменного администратора, для машины iwdm)
- db-admin (права доменного администратора, для машины db)
- iwtm-officer (права пользователя домена, для входа в веб-консоль iwtm)
- useroffice-1 (1я машина нарушителя, права пользователя домена, w10-cli1)
- useroffice-2 (2я машина нарушителя, права пользователя домена, w10-cli2)
- ldapsync-user (права пользователя домена, для всех ldap-синхронизаций)

Ваша задача – создать и настроить вышеперечисленных пользователей в соответствии с указанными условиями.

Для всех пользователей необходимо задать пароль xxXX1234

Настройте LDAP-синхронизацию для IWTM с помощью пользователя ldapsync-user.

Для работы с консолью IWTM используйте доменного пользователя iwtm-officer (задать все встроенные роли (officer и administrator) и все области видимости).

Стоит учесть, что после ввода в домен, компьютеры необходимо переносить в ранее созданный каталог Computers (внутри OU «Office»)

В соответствии с политикой компании для обеспечения безопасности компьютеров брандмауэр должен быть активен. Для установки компонентов системы необходимо настроить правила брандмауэра с помощью групповых политик домена.

Зайти пользователями useroffice-1 на машину w10-cli1 и useroffice-2 на машину w10-cli2.

## Решение:

Необходимо зайти на VM demo.lab, перейти в оснастку «Пользователи и компьютеры Active Directory».

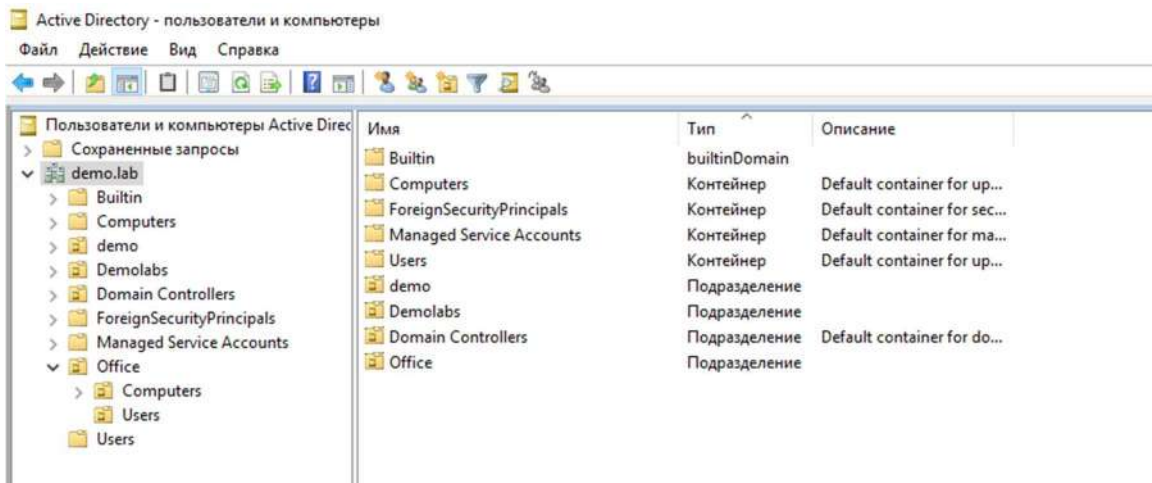


Рисунок 1 - «Оснастка Пользователи и компьютеры»

В открывшейся оснастке необходимо перейти во вкладку demo.lab, правой кнопкой мыши нажать по свободному пространству и выбрать «Создать», после чего выбрать «Подразделение». Согласно заданию, подразделение необходимо назвать «Office». В созданном подразделении нужно создать еще два, по аналогии с предыдущим. Названия: “Computers”, “Users”

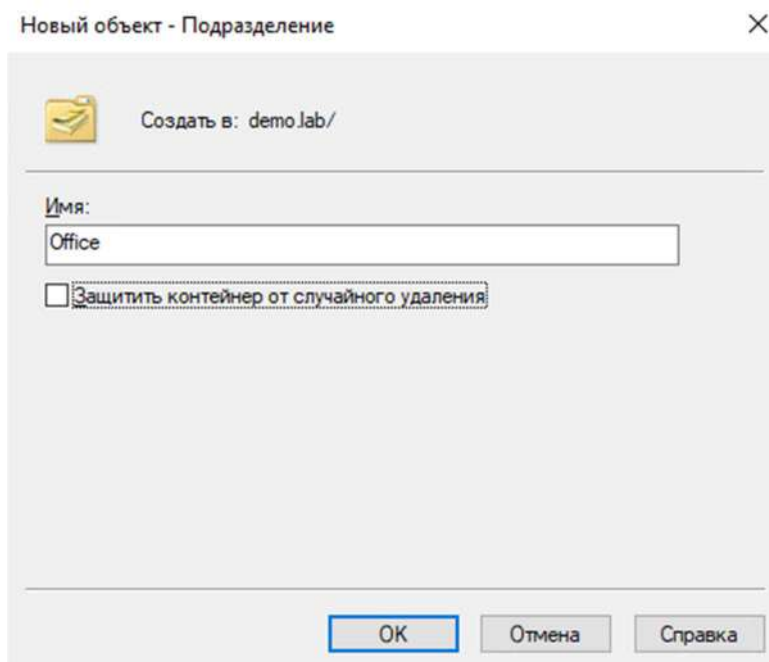


Рисунок 2 - «Создания подразделения»

Затем, необходимо создать пользователей в каталоге Users. Для удобства, советую сначала создать группу «Userss», а затем создавать пользователей.

Для создания группы нужно в подразделении Users кликнуть правой кнопкой мыши, выбрать «Создать» и выбрать «Группа».

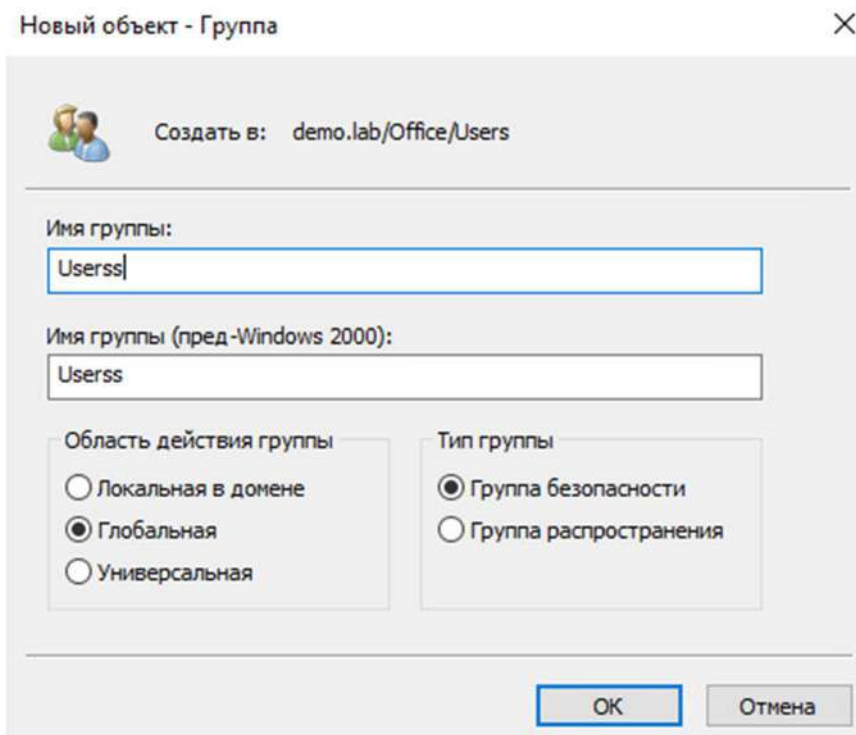
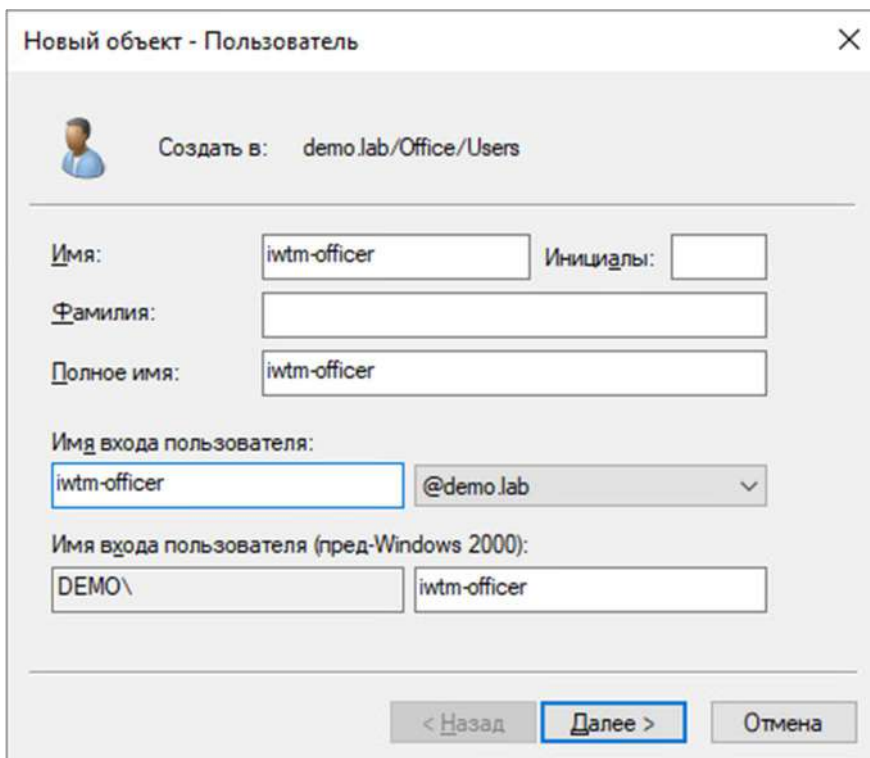


Рисунок 3 – «Создание группы»

После создания группы можно приступать к созданию пользователей. Начнем с пользователей iwtm-officer, iwdm-admin, db-admin. Эти пользователи требуют прав доменного администратора.

Для создания пользователя нужно в подразделении Users кликнуть правой кнопкой мыши, выбрать «Создать» и выбрать «Пользователь». Пароль каждого пользователя должен быть **xxXX1234**. **Все галочки выставлять строго в соответствии с рисунками 4 и 5!**





Новый объект - Пользователь

Создать в: demo.lab/Office/Users

Имя: iwtm-officer Инициалы:

Фамилия:

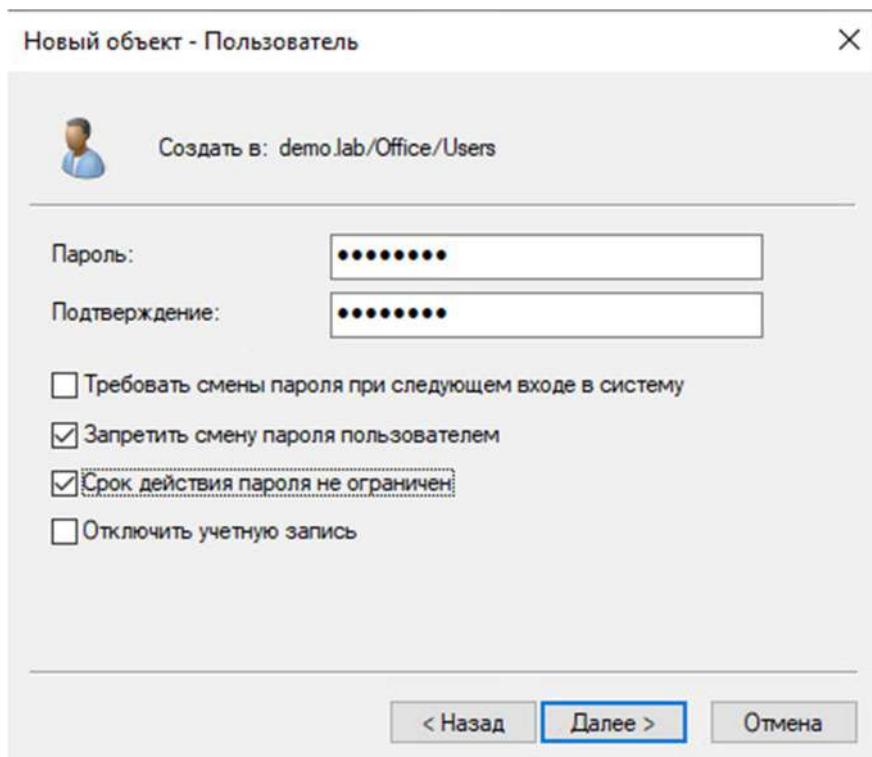
Полное имя: iwtm-officer

Имя входа пользователя: iwtm-officer @demo.lab

Имя входа пользователя (пред-Windows 2000): DEMO\ iwtm-officer

< Назад Далее > Отмена

Рисунок 4 – «Создание пользователя ч.1»



Новый объект - Пользователь

Создать в: demo.lab/Office/Users

Пароль: .....

Подтверждение: .....

☐ Требуется смена пароля при следующем входе в систему

☒ Запретить смену пароля пользователем

☒ Срок действия пароля не ограничен

☐ Отключить учетную запись

< Назад Далее > Отмена

Рисунок 5 – «Создание пользователя ч.2»

По аналогии с пользователем iwtm-officer создайте пользователей db-admin и iwdm-admin. Теперь необходимо предоставить созданным пользователям права доменного администратора. Для этого их необходимо выделить зажатой левой кнопкой мыши, нажать ПКМ на выделенных пользователях и выбрать пункт «Добавить в группу.» В открывшемся окне, необходимо ввести «Domain Admins» («Администраторы домена», если винда русская.) в поле «Введите имена выбираемых объектов».

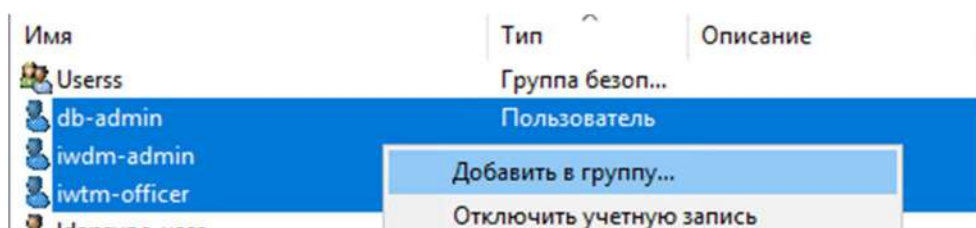


Рисунок 6 – «Добавление пользователей в группу ч.1»

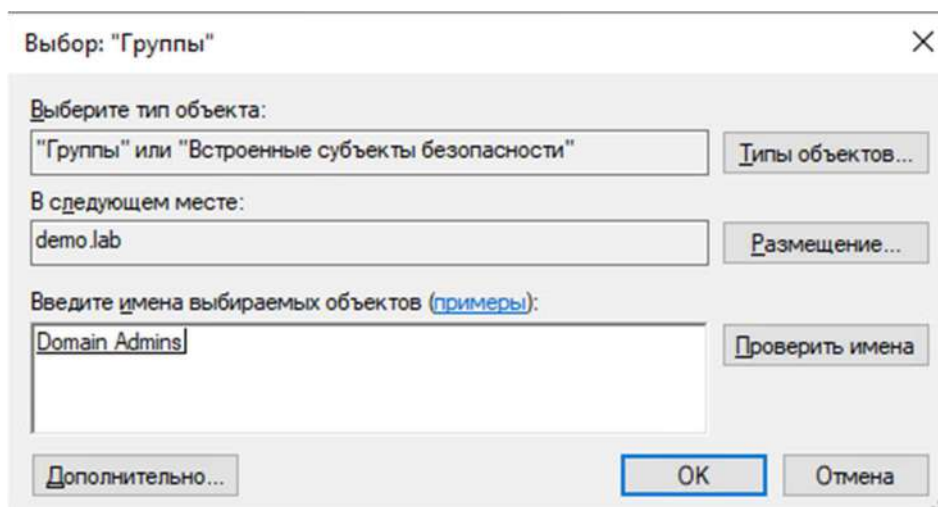


Рисунок 7 – «Добавление пользователей в группу ч.2»

Теперь можно перейти к созданию пользователей useroffice-1, useroffice-2 и ldapsync-user. Делайте это по аналогии с рисунками 4 и 5. **Однако, не добавляйте пользователей в группу Domain Admins (Администраторы домена).**

После создания всех пользователей, можно приступить к настройке LDAP-синхронизации на IWTM. Для настройки LDAP-синхронизации перейдите к WEB-интерфейсу Traffic Monitor. Для этого, в браузере введите в поисковую строку IP-адрес виртуальной машины IWTM (пр. 172.16.10.3).

Учетные данные для входа в WEB-интерфейс Traffic Monitor:

- логин: officer
- пароль: xxXX1234

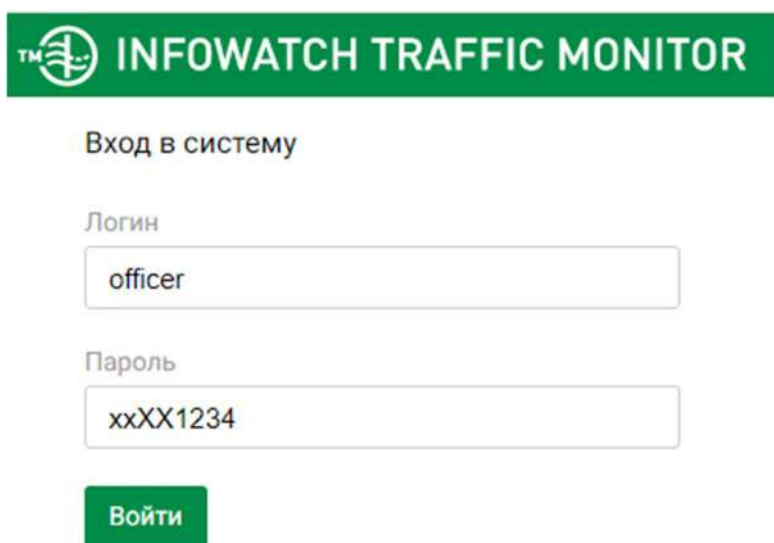


Рисунок 8 – «Вход в Traffic Monitor»

После входа в Web-интерфейс Traffic Monitor, необходимо выбрать пункт «Управление» в панели управления, в верхней части интерфейса, и выбрать подпункт «LDAP-синхронизация».

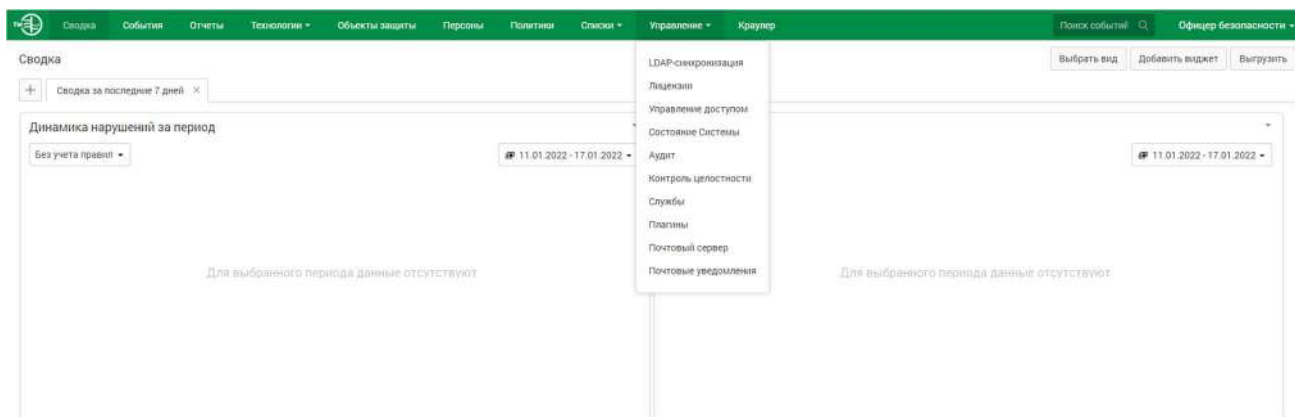


Рисунок 9 – «Переход к настройке LDAP-синхронизации»

В открывшейся вкладке, необходимо выбрать пункт «Создать», отмеченный знаком «+». Теперь, необходимо указать конфигурацию LDAP-синхронизации (Рисунок 10):

- Имя сервера: произвольное (пр. demo.lab),
- Тип сервера: Active Directory,
- Синхронизация: автоматическая,
- Период синхронизации: ежеминутно,
- Повторение: 15 минут,
- LDAP-сервер: IP-адрес виртуальной машины demo.lab (пр. 172.16.1.2),
- Использовать протокол Kerberos: нет,
- Глобальный LDAP-порт: 3268,
- LDAP-порт: 389,
- Использовать глобальный каталог: да,
- LDAP-запрос: DC=DEMO,DC=LAB
- Анонимный доступ: нет,
- Логин: ldapsync-user,
- Пароль: xxXX1234

### Добавление LDAP-сервера

Имя сервера

Тип сервера

Синхронизация ☒ Автоматическая ☐ Ручная

---

Период синхронизации

Повторение  минут

---

### Настройки соединения

LDAP-сервер

Использовать протокол Kerberos ☐

Глобальный LDAP-порт

LDAP-порт

Использовать глобальный каталог ☒

LDAP-запрос

Анонимный доступ ☐

Логин

Пароль

Рисунок 10 – «Конфигурация LDAP-синхронизации»

После настройки LDAP-синхронизации, необходимо добавить нового пользователя, который будет управлять консолью IWTM. Для создания нового пользователя, на знакомой панели управления в верхней части интерфейса веб-консоли Traffic Monitor, перейдите во вкладку «Управление» и выберите пункт «Управление доступом».

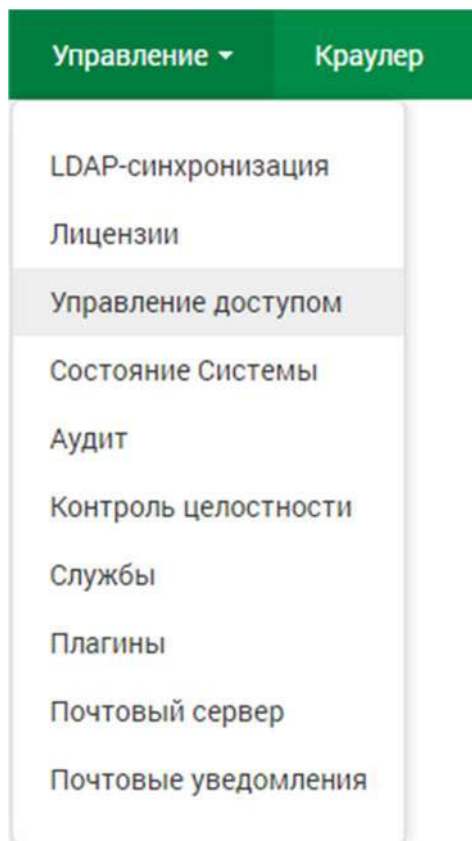


Рисунок 11 – «Управление доступом»

В открывшейся вкладке, необходимо выбрать пункт «Создать», отмеченный знаком «+» и выбрать пункт «Добавить пользователя из LDAP».

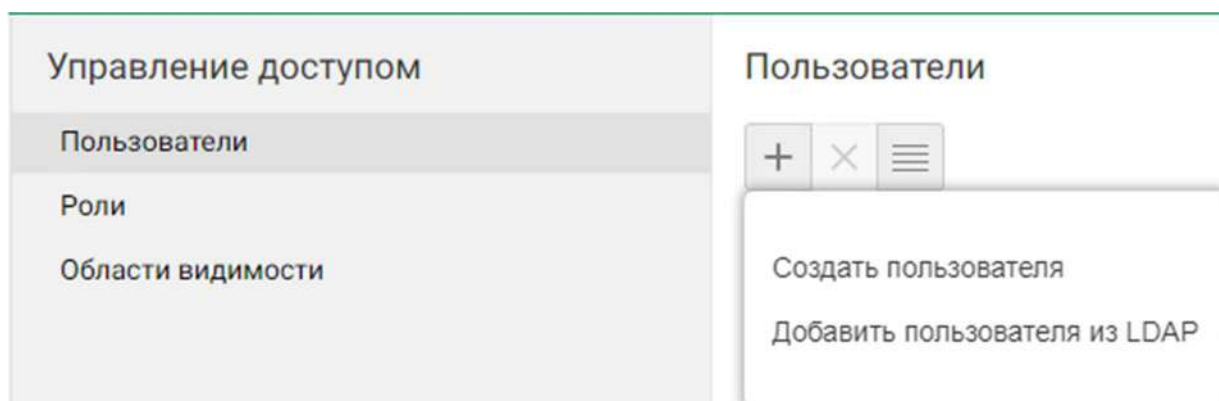


Рисунок 12 – «Добавление пользователя из LDAP ч.1»

Затем, необходимо ввести имя пользователя, который будет выступать администратором консоли, отметить нужного пользователя галочкой и нажать «Сохранить».

Выберите пользователя из LDAP

LDAP-сервер для поиска:

Поиск:

Пользователь	Доменный аккаунт	Адрес сервера	Департамент
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer@DC=DEMO.DC=LAB	172.16.1.2	

Рисунок 13 – «Добавление пользователя из LDAP ч.2»

После чего, необходимо выбрать этого же пользователя для того, чтобы перейти к его настройке. Необходимо указать почту пользователя ([iwtm-officer@demo.lab](mailto:iwtm-officer@demo.lab)), роли (Администратор, Офицер безопасности) и области видимости (Полный доступ, VIP). Нажмите кнопку «Сохранить» для применения настроек.

Пользователи

Логин	Название	Email	Роли	Области видимости	Описание
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer				
<input type="checkbox"/> administrator	Администратор		Администратор		Предустановленная
<input type="checkbox"/> officer	Офицер безопасности		Администратор, Офицер безопасности	Полный доступ	Предустановленная

Редактирование пользователя

Логин:

Статус:

Email:

Полное имя:

Роли:

Области видимости:

Описание:

Создано: 17.01.2022, 03:58 – Изменено: 17.01.2022, 03:58

Рисунок 14 – «Настройка пользователя»

После настройки LDAP-синхронизации, необходимо внести все ПК под управлением ОС Windows в домен Active Directory. Для этого, перейдите на

любой из компьютеров под управлением ОС Windows и откройте «Проводник». В открывшемся окне, в левой панели найдите пункт «Этот компьютер» и кликните на него правой кнопкой мыши, а затем выберите «Свойства».

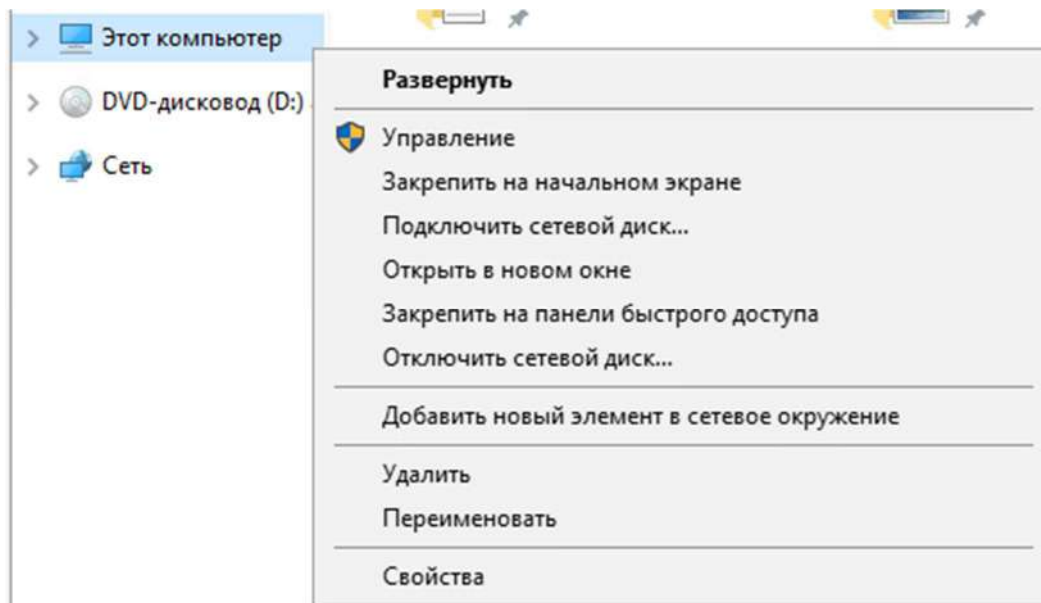


Рисунок 15 – «Переход к свойствам компьютера»

В открывшемся окне найдите подпункт «Имя компьютера, имя домена и параметры рабочей группы» в пункте «Просмотр основных сведений о вашем компьютере» и кликните «Изменить параметры». В открывшемся окне «Свойства системы», на вкладке «Имя компьютера» нажмите кнопку «Изменить».

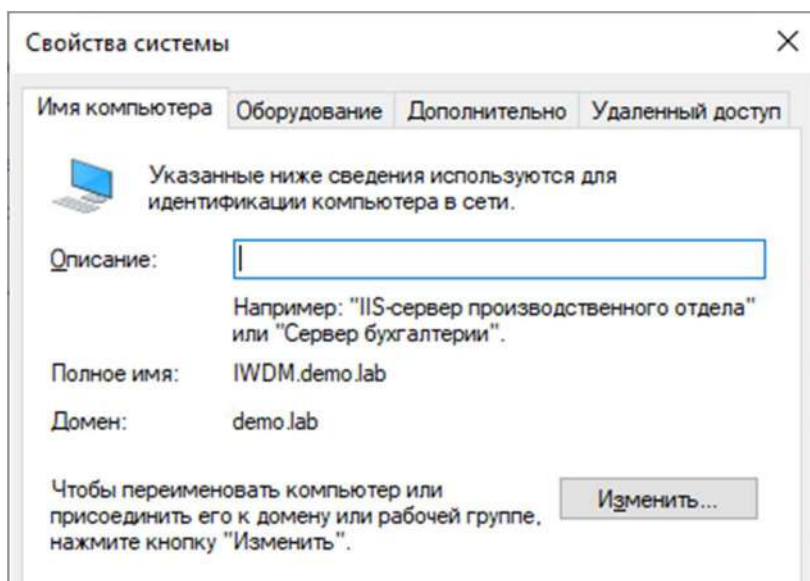


Рисунок 16 – «Добавление ПК в домен demo.lab ч.1»



В открывшемся окне переименуйте компьютер и введите имя домена (demo.lab) в соответствующие поля, после чего нажмите ОК и выполните перезагрузку.

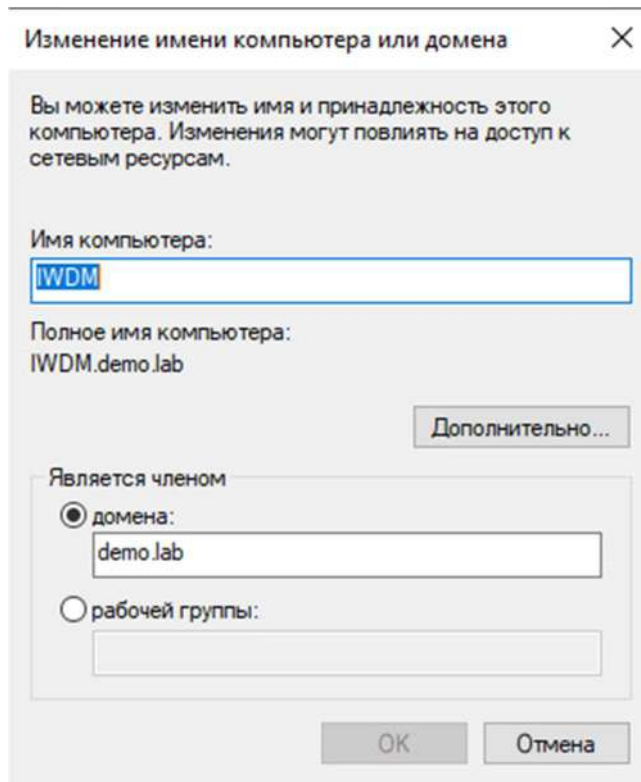


Рисунок 17 – «Добавление ПК в домен demo.lab ч.2»

Остальные компьютеры добавьте в домен по аналогии.

После добавления всех ПК в домен, вернитесь к оснастке «Active Directory Пользователи и компьютеры» на виртуальной машине demo.lab. В этой оснастке необходимо перенести добавленные в домен компьютеры в каталог «Computers» в подразделении «Office».

В открытой оснастке перейдите в каталог «Computers», который находится в корне домена demo.lab, затем выделите компьютеры и перетащите их зажатой левой кнопкой мыши в каталог «Computers» в подразделении «Office» (Рисунок 18).

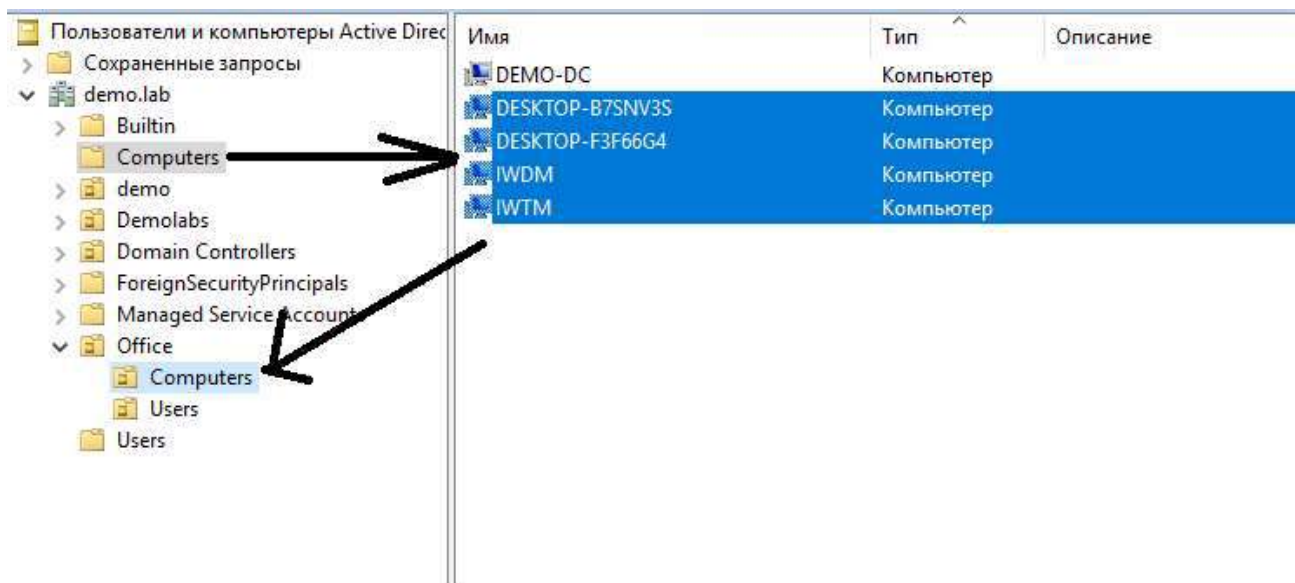


Рисунок 18 – «Перенос ПК в каталог Computers»

**ОПЦИОНАЛЬНО:** для собственного удобства, можно создать записи DNS для каждого устройства. Для этого, зайдите в Пуск → Средства Администрирования → DNS. В открывшейся оснастке выберите единственный сервер и откройте подпапку «Зоны прямого просмотра», а в ней «demo.lab».

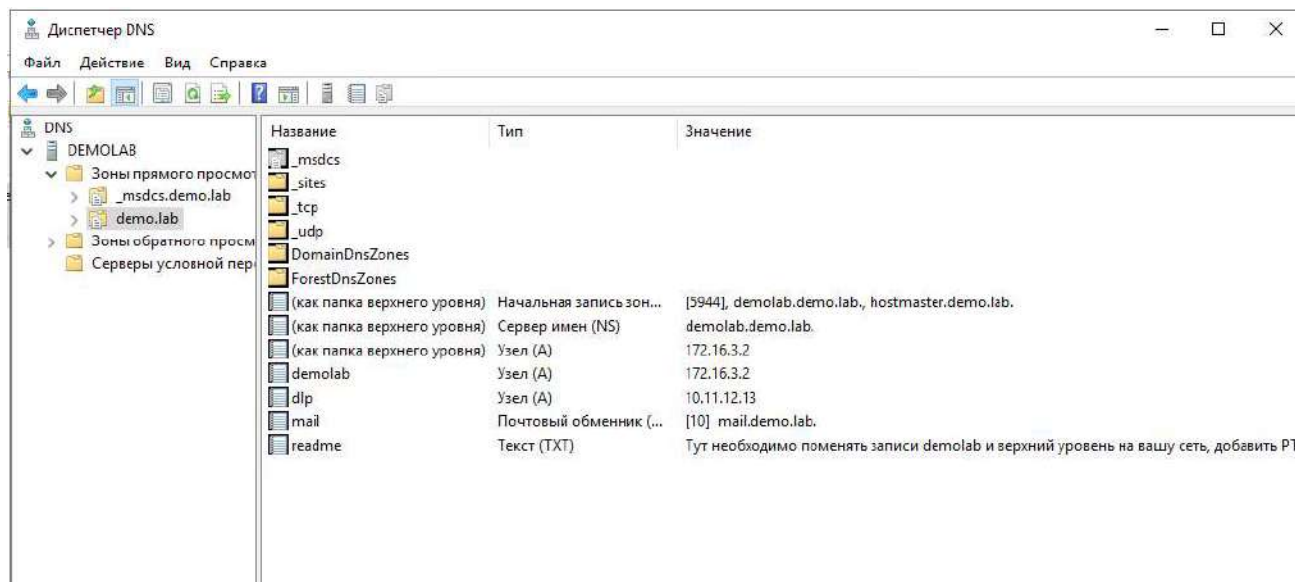
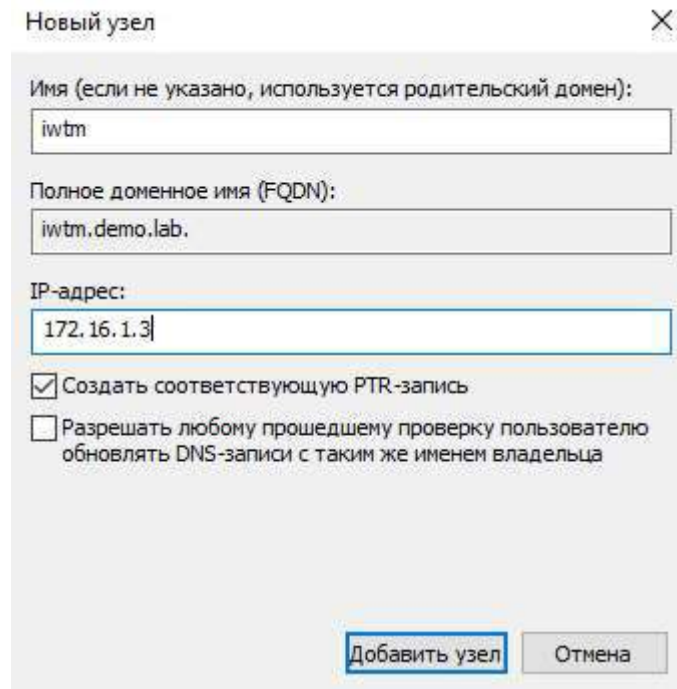


Рисунок 19 – «Зона прямого просмотра demo.lab»

В пустом пространстве нажмите ПКМ и, в открывшемся контекстном меню, выберите «Создать узел (A или AAAA)». При создании нового узла DNS, введите имя устройства и его IP-адрес (прим.: iwtm – 172.16.1.3).



Новый узел

Имя (если не указано, используется родительский домен):  
iwtm

Полное доменное имя (FQDN):  
iwtm.demo.lab.

IP-адрес:  
172.16.1.3

☒ Создать соответствующую PTR-запись

☐ Разрешать любому прошедшему проверку пользователю обновлять DNS-записи с таким же именем владельца

Добавить узел Отмена

Рисунок 20 – «Создание узла»

## Задание 2: Развертывание InfoWatch Crawler

Для контроля общих сетевых ресурсов в организации необходимо развернуть следующие сетевые компоненты InfoWatch Traffic Monitor на машину IWDM: Crawler Server и Crawler Scanner.

После установки InfoWatch Crawler необходимо создать задачу на ежедневное сканирование сетевых ресурсов (папки share\_iwtm, share\_iwdm). Предварительно требуется создать общие сетевые папки:

1. На виртуальной машине IWTM создать папку «share\_iwtm» с правами чтения и записи для всех пользователей домена
2. На виртуальной машине IWDM создать папку «share\_iwdm» с правами чтения и записи для всех пользователей домена

*Зафиксировать создание и выполнение скриншотом.*

Чтобы установить Crawler – перейдите к виртуальной машине IWDM (виртуальная машина для Device Monitor). Перейдите в проводник (может быть на рабочем столе одного из пользователей) и найдите установочный файл Crawler (Crawler\_v6\*.exe), после чего откройте его.

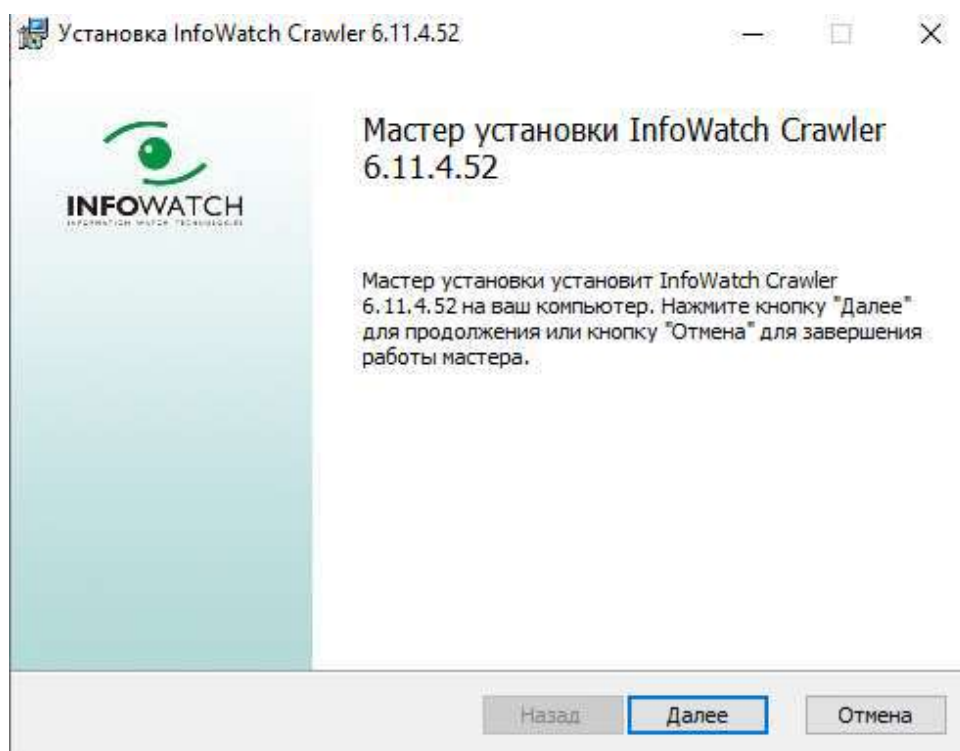


Рисунок 21 – «Установка Crawler»

Соглашайтесь со всем подряд, до пункта «Настройка базы данных».

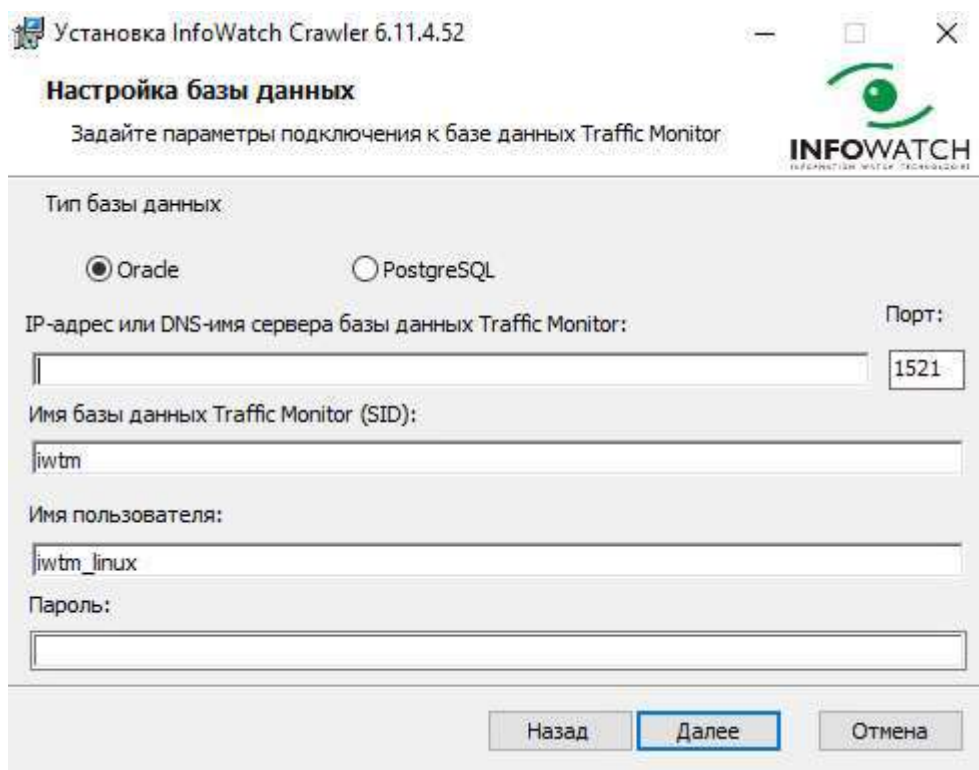


Рисунок 22 – «Настройка базы данных»

Заполните соответствующую информацию:

- Тип базы данных: PostgreSQL
- IP-адрес или DNS-имя сервера базы данных ТМ: 172.16.1.3 (или iwtm, если настроено DNS)
- Имя базы данных ТМ (SID): postgres
- Имя пользователя: iwtm
- Пароль: xxXX1234

После заполнения информации о БД, будет необходимо заполнить информацию о Traffic Monitor.

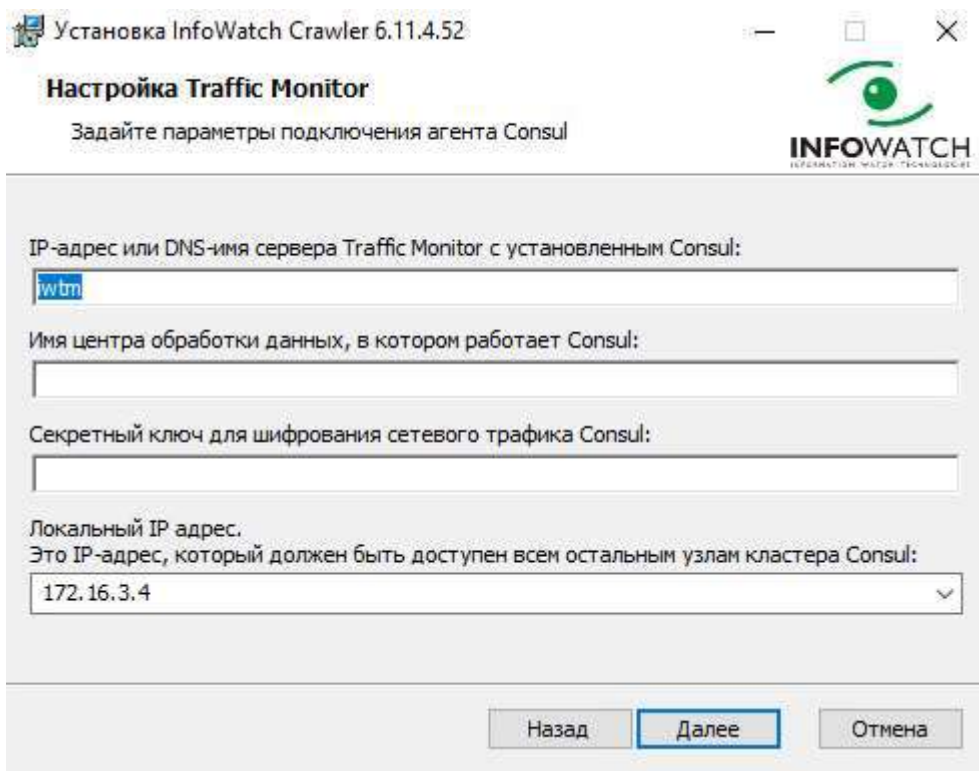


Рисунок 23 – «Настройка Traffic Monitor»

Агент Consul устанавливается вместе с Traffic Monitor по умолчанию. Для получения имени центра обработки данных и секретного ключа шифрования, вам необходимо подключиться к IWTM с помощью SSH. Для этого, откройте командную строку (Windows + R → cmd) и ввести команду `ssh root@172.16.1.3` (или `ssh root@iwtm`, если настроен DNS), ввести пароль пользователя root от виртуальной машины IWTM.

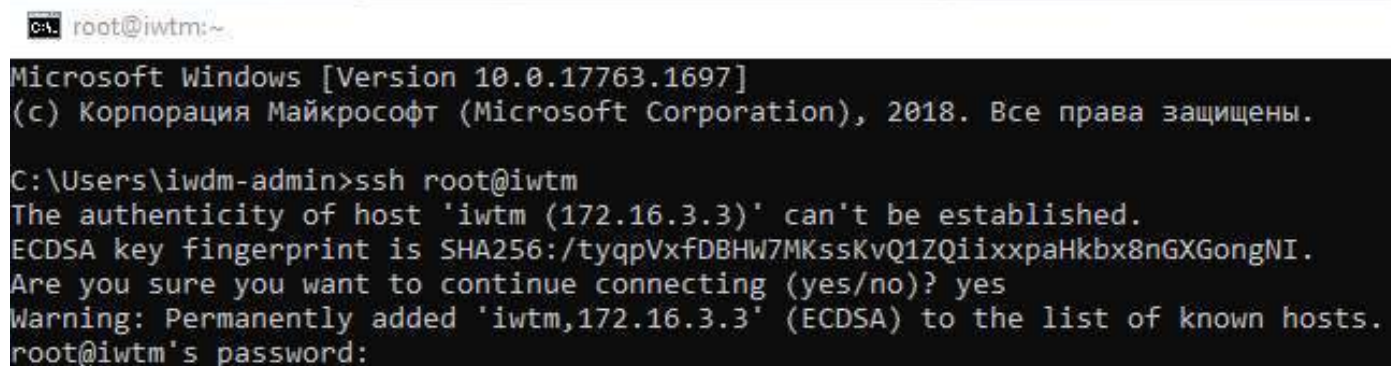


Рисунок 24 – «Подключение к IWTM»

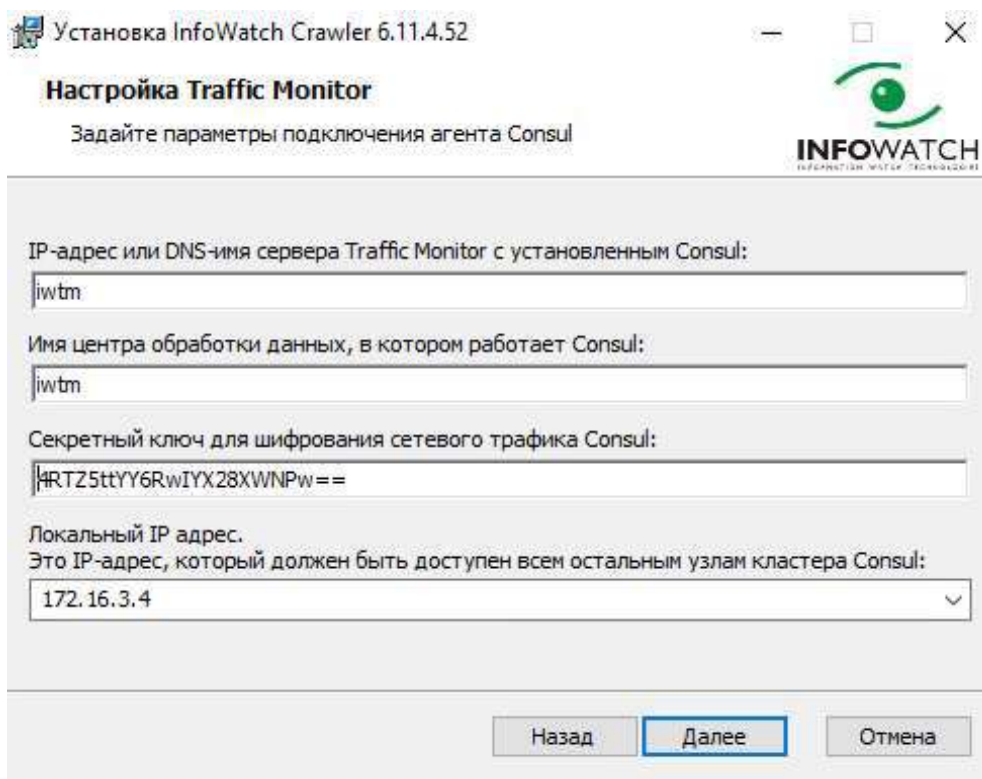
Подключившись к IWTM, вам необходимо открыть файл конфигурации службы Consul (/opt/iw/tm5/etc/consul/consul.json) и скопировать оттуда имя ЦОД



и ключ шифрования. Для того, чтобы прочитать содержимое файла, введите команду **cat /opt/iw/tm5/etc/consul/consul.json**, вывод данной команды покажет имя ЦОД (значения поля **datacenter**) и секретный ключ (значение поля **encrypt**). Скопируйте эти значения и вставьте (без кавычек) в окно установки Crawler и нажмите «Далее».

```
[root@iwtm ~]# cat /opt/iw/tm5/etc/consul/consul.json
{
  "bootstrap_expect": 1,
  "client_addr": "127.0.0.1",
  "data_dir": "/opt/iw/tm5/var/consul",
  "datacenter": "iwtm",
  "disable_update_check": true,
  "enable_syslog": true,
  "encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",
  "leave_on_terminate": false,
  "log_level": "WARN",
  "rejoin_after_leave": true,
  "server": true,
  "skip_leave_on_interrupt": true
}
```

Рисунок 25 – «Конфигурационный файл Consul»



Установка InfoWatch Crawler 6.11.4.52

**Настройка Traffic Monitor**

Задайте параметры подключения агента Consul

IP-адрес или DNS-имя сервера Traffic Monitor с установленным Consul:

Имя центра обработки данных, в котором работает Consul:

Секретный ключ для шифрования сетевого трафика Consul:

Локальный IP адрес.  
Это IP-адрес, который должен быть доступен всем остальным узлам кластера Consul:

Назад **Далее** Отмена

Рисунок 26 – «Заполненная информация о Traffic Monitor»

Следующее, что нужно сделать, задать параметры подключения к серверу

Traffic Monitor. Для этого необходимо найти токен плагина краулера, который располагается в веб-интерфейсе IWTM. Войдите, с ранее созданной учетной записью iwtm-officer, и во вкладке «Управление» на верхней панели, перейдите к пункту «Плагины».

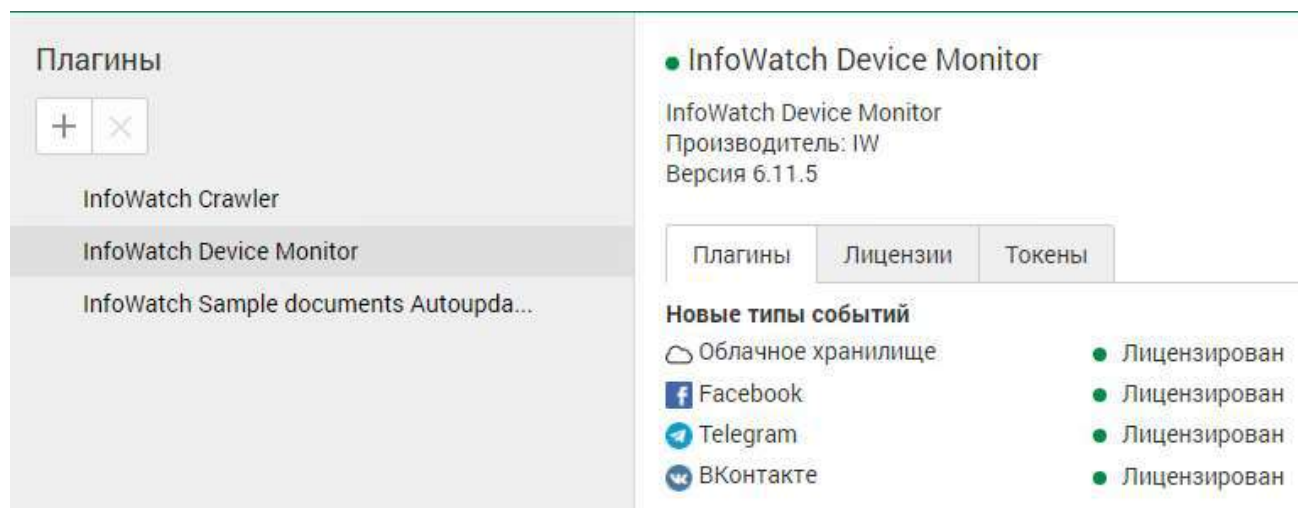


Рисунок 27 – «Плагины Traffic Monitor»

Найдите плагин «InfoWatch Crawler» и перейдите ко вкладке «Токены» внутри. Скопируйте (с помощью кнопки «Скопировать токен». Выделить токен у вас не получится.) содержание активного токена и вставьте в окно установщика Crawler.

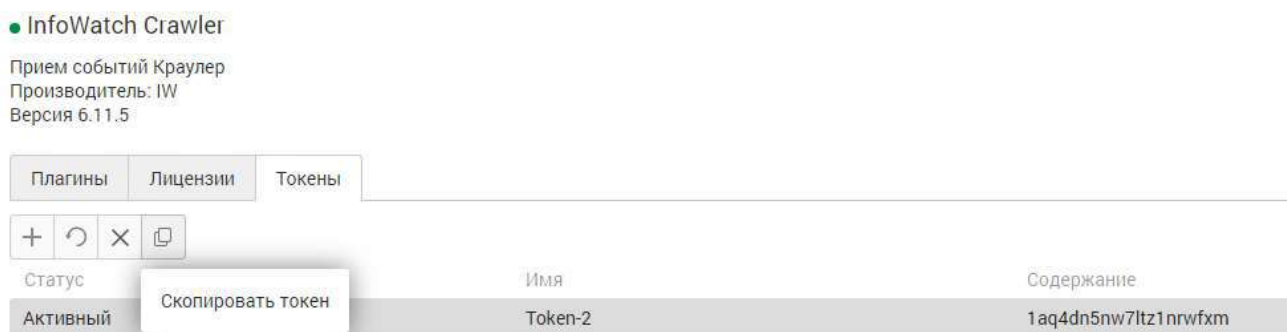


Рисунок 28 – «Токен Crawler»



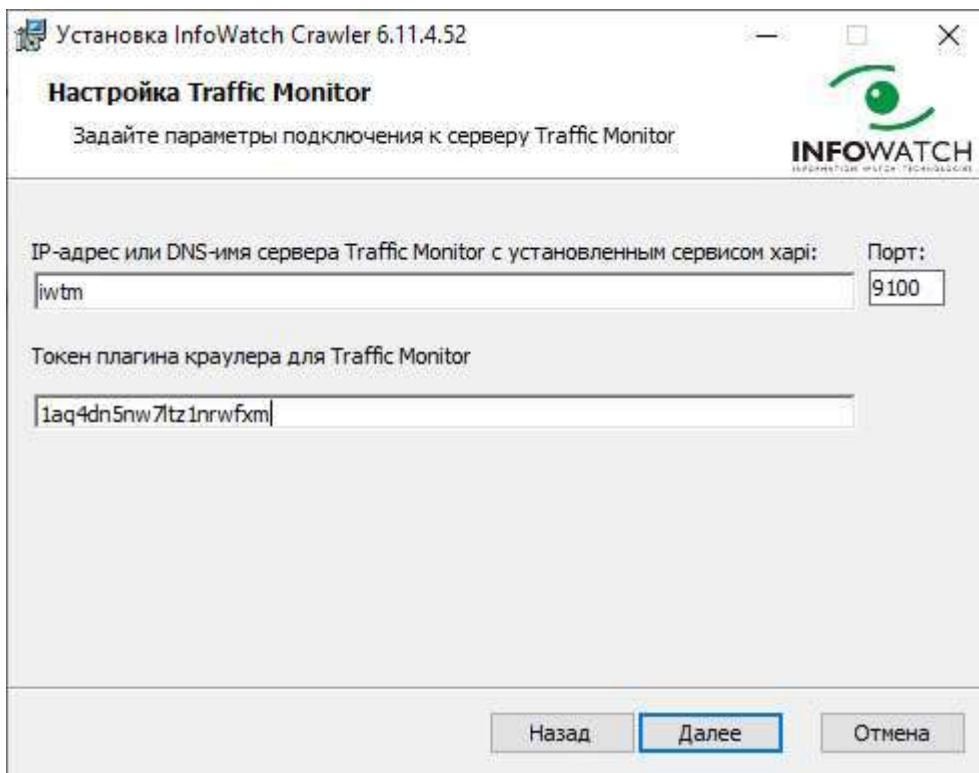


Рисунок 29 – «Заполненная информация о подключении к серверу ТМ»

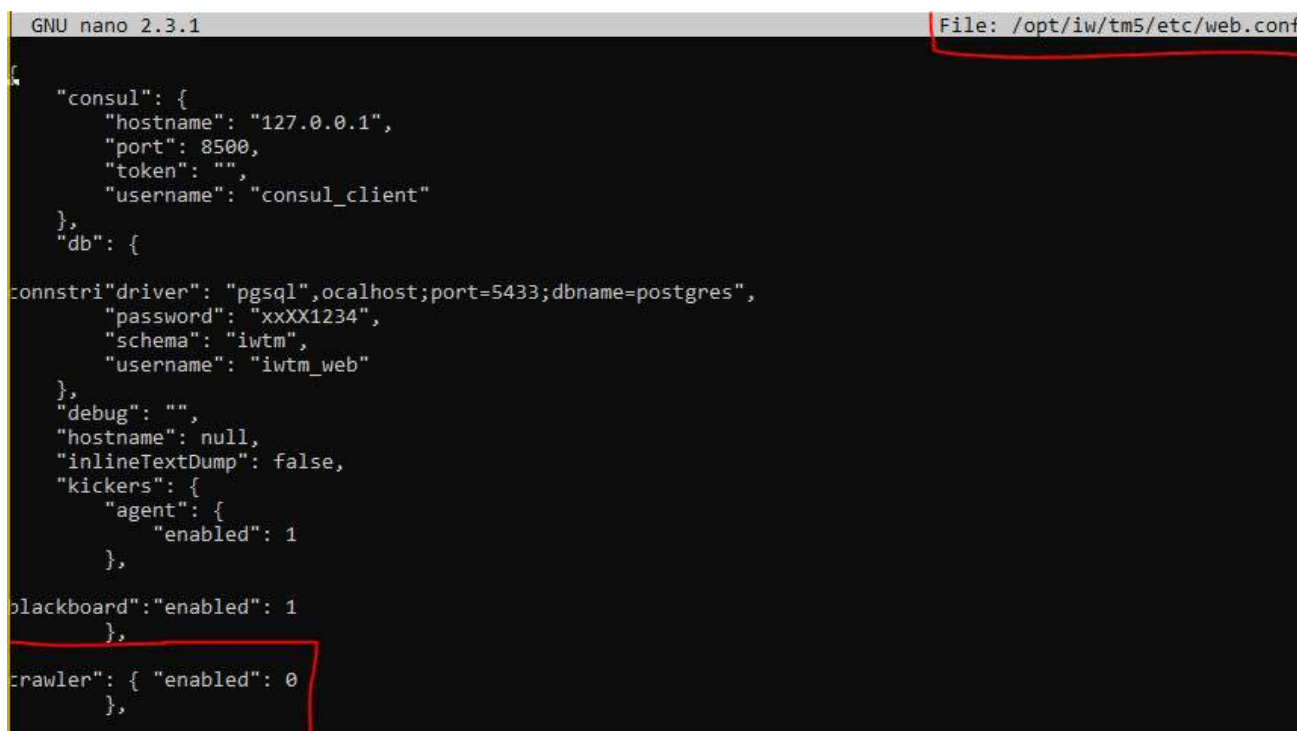
Затем, будет предложено выбрать параметры учетной записи для сервиса сканера – выбирайте «Локальная система». Далее соглашайтесь со всем, до конца установки. Crawler установлен, однако зайдя в веб-интерфейс, вы его не увидите. Чтобы заставить Crawler полноценно функционировать, откройте порты 6556 и 1337, необходимые для работы Crawler. Можете делать это любым способом, но быстрее всего это можно сделать через Powershell: откройте Powershell с правами администратора и введите следующие команды:

```
New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 1337"
-DisplayName "Crawler 1337" -Profile Any -Protocol TCP -LocalPort 1337
```

```
New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 6556"
-DisplayName "Crawler 6556" -Profile Any -Protocol TCP -LocalPort 6556
```

После открытия портов, вновь подключитесь к виртуальной машине IWТМ (ssh root@iwtm) и перейдите к конфигурационному файлу /opt/iw/tm5/etc/web.conf. Откройте файл любым текстовым редактором, например

nano (прим.: nano /opt/iw/tm5/etc/web.conf) и, попадая в редактор, измените значение параметра «enabled» с «0» на «1» в параметрах «crawler».



```
GNU nano 2.3.1 File: /opt/iw/tm5/etc/web.conf
{
  "consul": {
    "hostname": "127.0.0.1",
    "port": 8500,
    "token": "",
    "username": "consul_client"
  },
  "db": {
    "driver": "pgsql",
    "connstr": "host=localhost;port=5433;dbname=postgres",
    "password": "xxXX1234",
    "schema": "iwtm",
    "username": "iwtm_web"
  },
  "debug": "",
  "hostname": null,
  "inlineTextDump": false,
  "kickers": {
    "agent": {
      "enabled": 1
    }
  },
  "blackboard": {
    "enabled": 1
  },
  "crawler": {
    "enabled": 0
  }
}
```

Рисунок 30 – «Параметры crawler в web.conf»

Теперь необходимо создать две общие папки, которые будет сканировать Crawler. Для того, чтобы создать общую папку на виртуальной машине IWTM, перейдите в терминал и установите пакет samba, с помощью команды **yum install samba**. После установки samba, создайте папку «share\_iwtm» в корне файловой системы(/) с помощью команды **mkdir /share\_iwtm**. Теперь, отредактируйте права группы с помощью команд **chown -R nobody:nobody /share\_iwtm** и **chmod -R 0755 /share\_iwtm**. Затем, перейдите к конфигурационному файлу samba и перейдите к его редактированию (**nano /etc/samba/smb.conf**).

Приведите файл smb.conf к такому виду:

```
[global]
    map to guest = Bad User

[share_iwtm]
    path = /share_iwtm
    read only = no
    guest ok = yes
    guest only = yes
```

Рисунок 31 – «Содержимое файла /etc/samba/smb.conf»

Теперь, необходимо перезапустить службу SMB и NMB. Сделайте это, с помощью команда **systemctl restart smb** и **systemctl restart nmb**. Отныне, сетевая папка на IWTM настроена и работоспособна, однако, зайти на нее с Windows-машин вы пока не можете, для этого необходимо создать GPO, позволяющее заходить в гостевые общие папки. Это будет сделано в следующем шаге.

Теперь, нужно создать общую папку на IWDWM. Это делается на порядок легче и быстрее. Создайте папку **share\_iwdm** в корне диска C:, затем перейдите к свойствам созданной папки и выберите вкладку «Доступ» (рис. 32). Нажмите «Общий доступ» и выберите пользователей в сети, с которыми нужно поделиться папкой, в нашем случае, это группа – Domain Users (Пользователи домена, если русская винда), затем нажмите «Поделиться» (рис. 33). Готово.

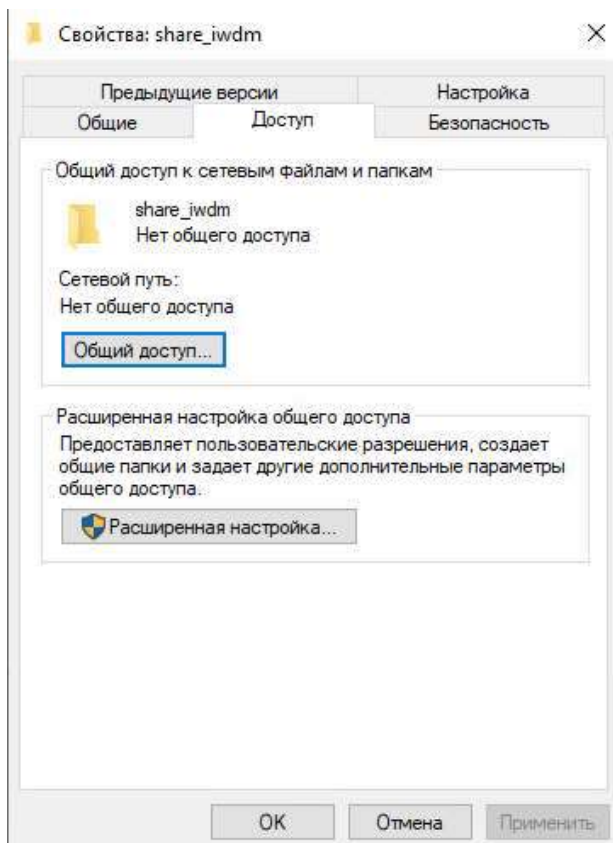


Рисунок 32 – «Доступ к share\_iwdm»

← Доступ к сети

Выберите в сети пользователей, с которыми вы хотите поделиться

Введите имя и нажмите кнопку "Добавить" либо используйте стрелку для поиска определенного пользователя.

Имя	Уровень разрешений
Domain Users	Чтение и запись ▼
iwdm-admin	Владелец

[Проблемы при предоставлении общего доступа](#)

Поделиться

Отмена

Рисунок 33 – «Доступ к share\_iwdm»

После создания двух общих папок, необходимо создать операцию сканирования краулера. Вернитесь к веб-интерфейсу Traffic Monitor и перейдите ко вкладке «Краулер» в верхней части окна. С помощью кнопки «+» (Создать задачу), создайте новую задачу сканирования.

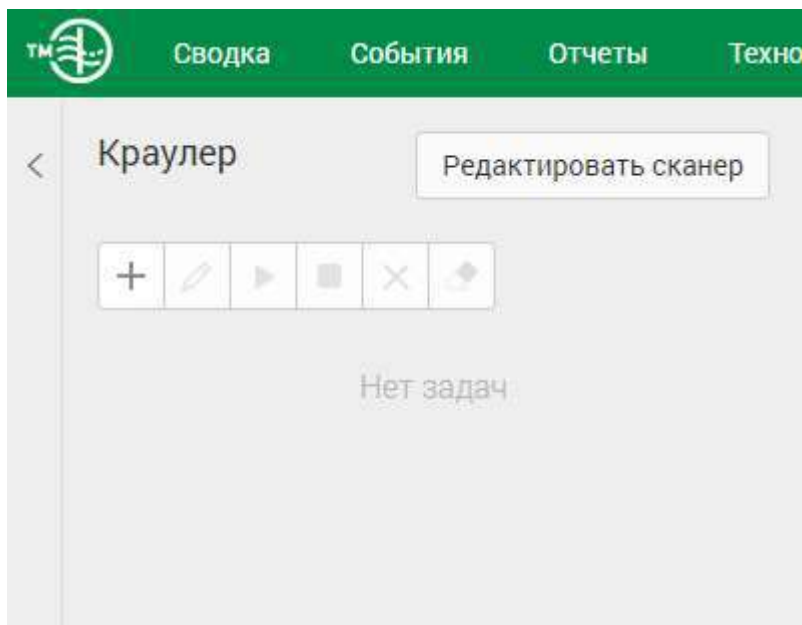


Рисунок 34 – «Краулер»

Далее, заполните параметры:

- Название: произвольное;
- Описание: произвольное;
- Цель сканирования: разделяемые сетевые ресурсы;
- Сканируемые группы и компьютеры: iwtm, iwdm;
- Режим сканирования: все папки;
- Авторизация сканера: да;
- Период сканирования: ежедневно;
- Время: 00:00.

Больше ничего менять не нужно. Создайте два любых текстовых файла в папках share\_iwtm и share\_iwdm, для проверки работы Crawler. Затем вернитесь в веб-интерфейс и запустите задачу сканирования. Готово.

## Модуль 5: Технологии агентского мониторинга

### Задание 1

Необходимо применить групповые политики Windows для OU «Office».

#### **Групповая политика 1:**

- Минимальная длина пароля должна составлять 7 символов;
  - Срок жизни пароля должен составлять 192 дня;
- Выполнение задания подтвердить скриншотами.

#### **Групповая политика 2:**

- Отключить возможность локального входа для пользователей iwtm-officer и Idapsync-user с помощью групповых политик
- Выполнение задания подтвердить скриншотами.

#### **Групповая политика 3:**

- С помощью редактора групповой политики запретить показ анимации при входе в систему. Выполнение задания подтвердить скриншотами.

#### **Групповая политика 4:**

- С помощью редактора групповой политики настройте запрет запуска msinfo32.exe. Выполнение задания подтвердить скриншотами.

#### **Групповая политика 5:**

- С помощью редактора групповой политики ограничить доступ к панели управления. Выполнение задания подтвердить скриншотами.

Для создания и редактирования групповых политик перейдите к виртуальной машине demolab (контроллер домена) и откройте оснастку «Управление групповой политикой» (Пуск → Средства Администрирования Windows → Управление групповой политикой). В открывшейся оснастке выберите лес, перейдите в подпапку «домены» и выберите соответствующий домен.

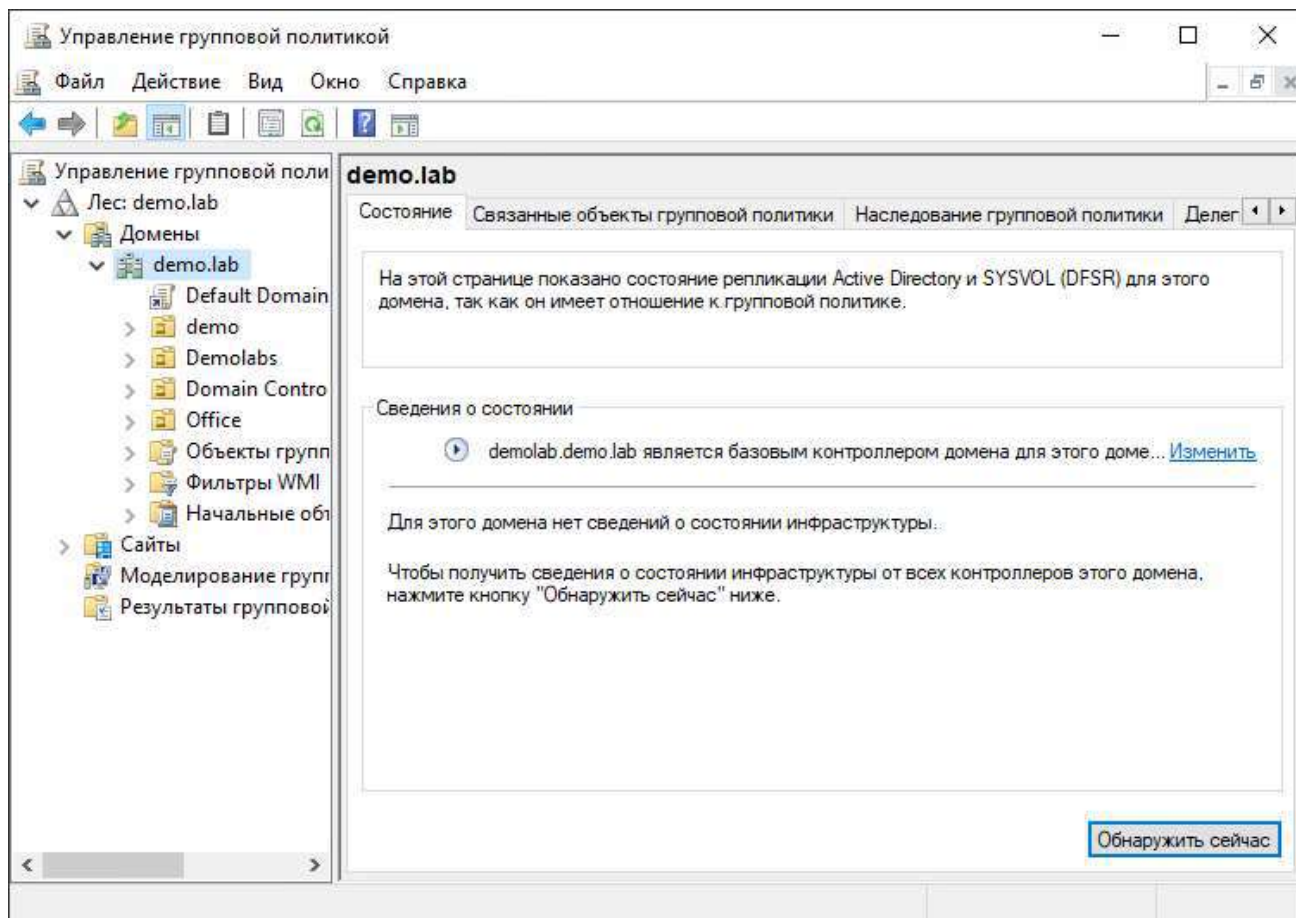


Рисунок 35 – «Управление групповыми политиками»

Кликните ПКМ по домену, чтобы открыть контекстное меню и выберите «Создать объект групповой политики в этом домене и связать его...» (рис. 36), назовите объект произвольным именем (прим.: Office). Затем сразу отредактируйте фильтры безопасности созданной политики. Для этого откройте созданный объект политики, удалите «Прошедшие проверку» (рис. 37) и добавьте группу «Domain Computers» (Компьютеры домена, если русская винда) и, созданную ранее, группу Office (рис. 38).



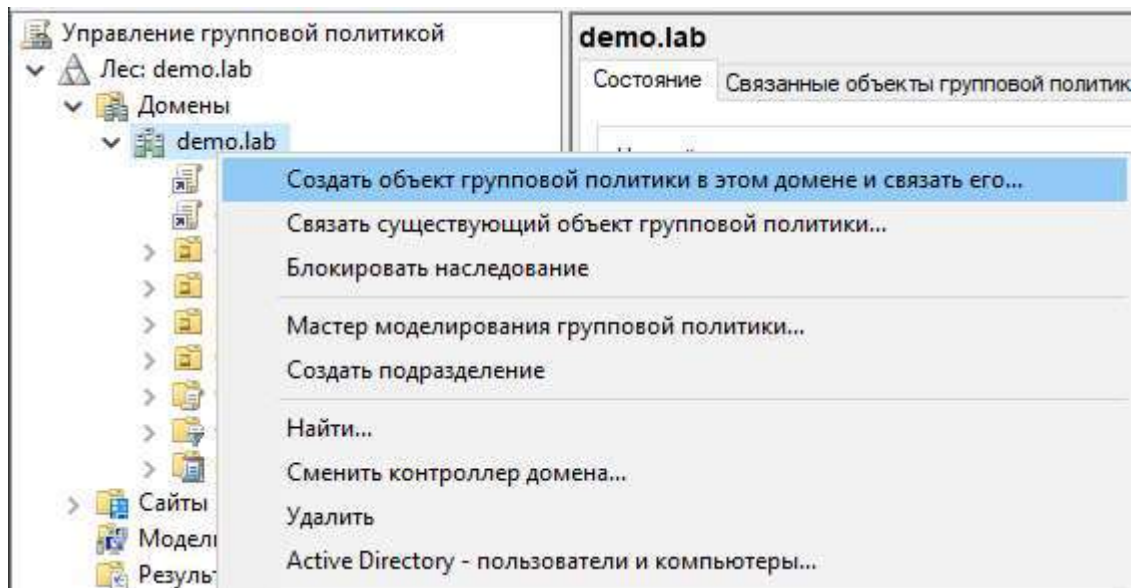


Рисунок 36 – «Создание объекта группой политики»

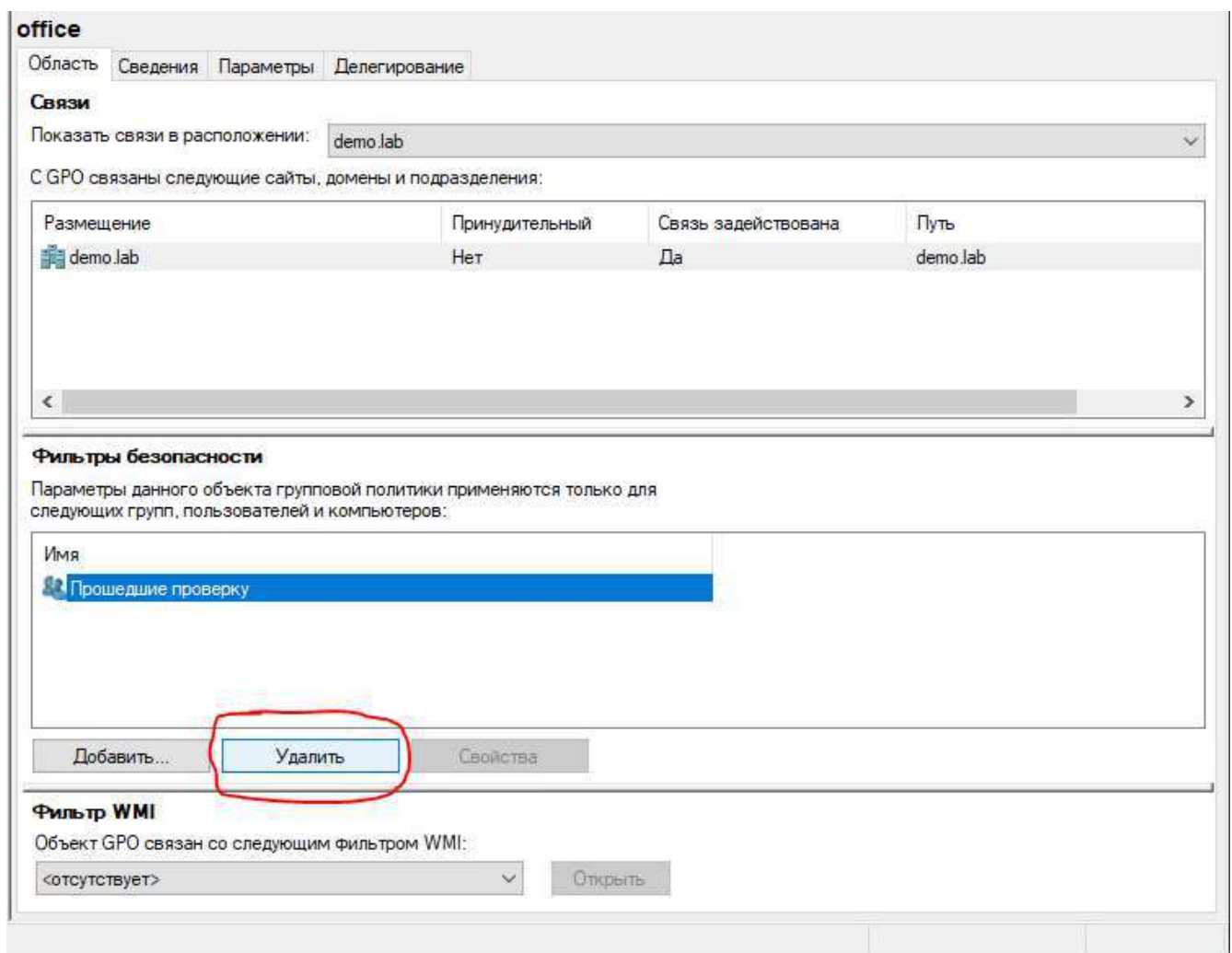


Рисунок 37 – «Редактирование фильтров безопасности»



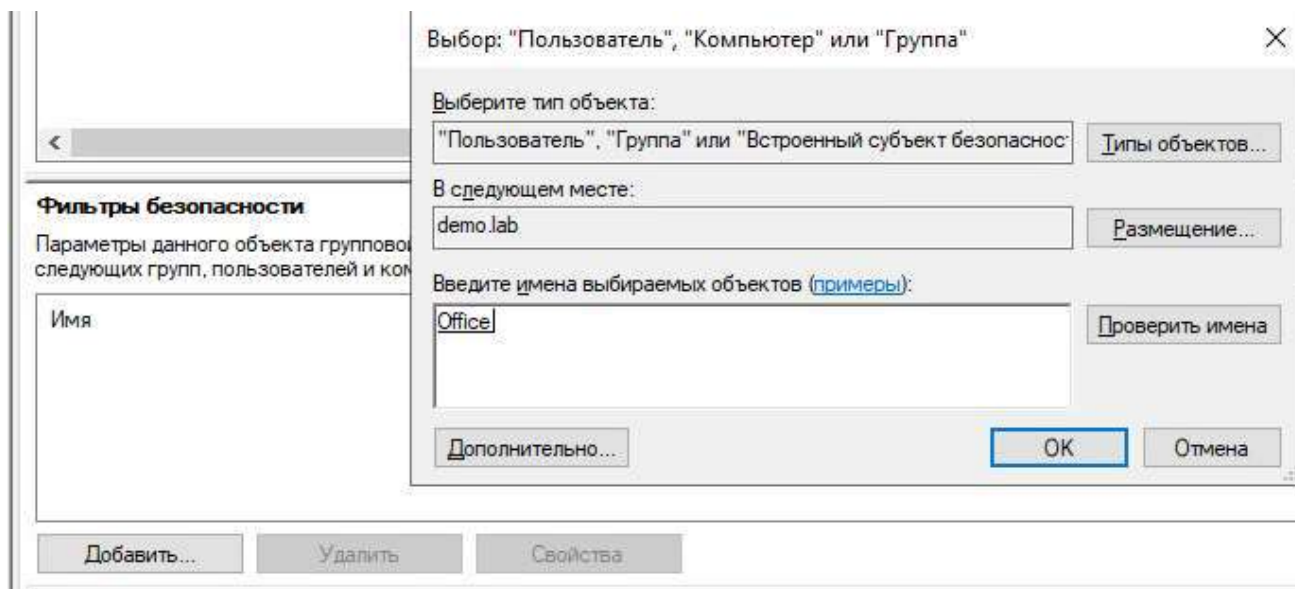


Рисунок 38 – «Добавление фильтров безопасности»

Чтобы перейти к редактированию объекта групповой политики, кликните на нем ПКМ и, в контекстном меню, выберите «Изменить», после чего откроется редактор управления групповыми политиками. Интерфейс интуитивно понятен, проблем возникнуть не должно:

- Политика 1:
  - Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политика паролей → Максимальный срок действия пароля = 192 дн. + Минимальная длина пароля = 7 зн.
- Политика 2:
  - Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя → Запретить локальный вход = DEMO\iwtm-officer, DEMO\ldapsync-user
- Политика 3:
  - Конфигурация компьютера → Политики → Административные шаблоны → Система → Вход в систему → Показать анимацию при первом входе в систему = Отключено.
- Политика 4:

- Конфигурация пользователя → Политики → Административные шаблоны → Система → Не запускать указанные приложения Windows → msinfo32.exe
- Политика 5:
  - Конфигурация пользователя → Политики → Административные шаблоны → Панель управления → Запретить доступ к панели управления = включено.
- Политика 6 (чтобы работала общая папка IWTM, это обязательно):
  - Конфигурация компьютера → Политики → Административные шаблоны → Сеть → Рабочая станция Lanman → включить небезопасные гостевые входы = Включено.

## Задание 2

Используйте для входа в консоль IWDM доменного пользователя **iwdm-admin**.

Задать максимальные права пользователя на работу в консоли IWDM.

*Проверить работоспособность, зафиксировать настройку и выполнение скриншотом запущенной консоли.*

## Задание 3

Необходимо создать новые политики (кроме политики на устройства по умолчанию),

### **Политика 1:**

Название: «**Отдел 1**»

Группа компьютеров: Виртуальная машина пользователя **userofficer-1**

### **Политика 2:**

Название: «**Отдел 2**»

Группа компьютеров: Виртуальная машина пользователя **userofficer-2**

*Зафиксировать выполнение скриншотами.*

Перед началом работы с консолью Device Monitor необходимо установить службы Device Monitor и СУБД PostgreSQL, для этого перейдите к виртуальной машине IWDM (ВМ для работы в Device Monitor) и обнаружьте установочный файл, на подобии с Crawler, СУБД PostgreSQL (postgresql-\*-windows-x64) и запустите его. Возможно, до запуска самой программы установки PostgreSQL, установятся дополнительные компоненты.



Рисунок 39 – «Установка PostgreSQL»

Соглашайтесь со всем подряд ничего не меняя, до этапа создания пароля. В качестве пароля введите произвольный пароль, **однако крайне рекомендую поставить стандартный пароль – xxXX1234**. Далее, начиная с сетевого порта, ничего не меняйте, до конца установки. В конце установки уберите галочку с пункта «Launch Stack Builder at exit?» и закройте установочный файл. Последнее, что нужно сделать для работы БД – отредактировать файл подключений pg\_hba.conf. Перейдите к папке C:\Program Files\PostgreSQL\10\data и найдите файл pg\_hba.conf – откройте его с помощью приложения Блокнот.

В открывшейся файл добавьте строку «host all all 0.0.0.0/0», в секцию «IPv4 local connections».

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# IPv4 local connections:					
host	all		all	127.0.0.1/32	md5
host	all		all	0.0.0.0/0	md5
# IPv6 local connections:					
host	all		all	:::1/128	md5
# Allow replication connections from localhost, by a user with the					
# replication privilege.					
host	replication		all	127.0.0.1/32	md5
host	replication		all	:::1/128	md5

Рисунок 40 – «Редактирование pg\_hba.conf»

Найдите и запустите установочный файл Device Monitor (Setup.Device.Monitor.ru.\*).

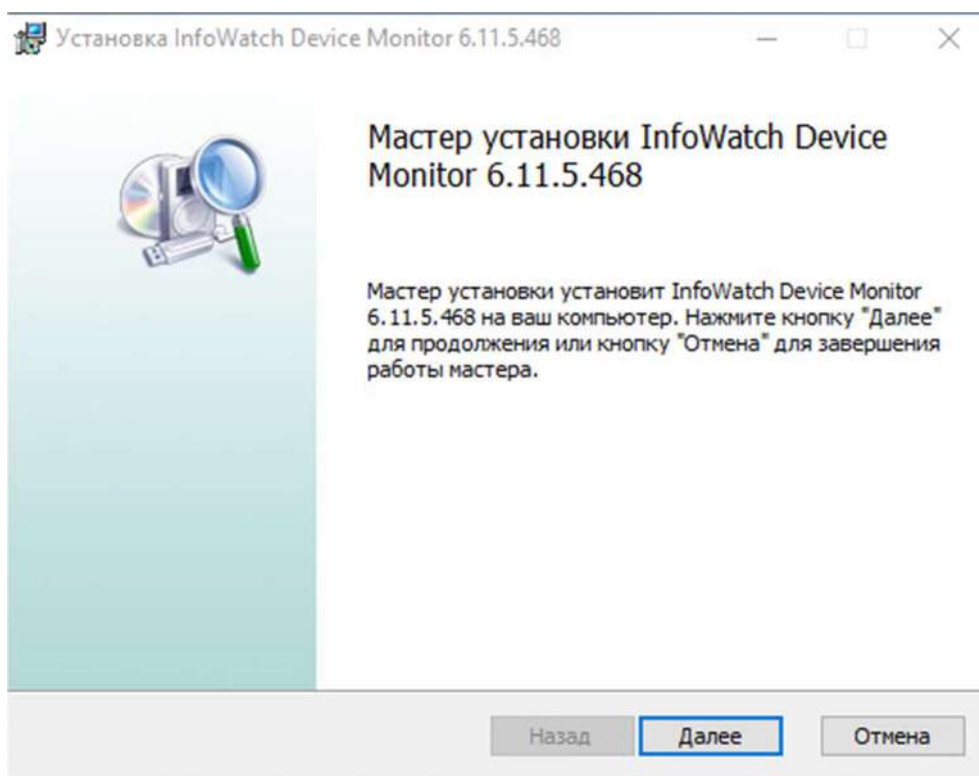


Рисунок 40 – «Установка Device Monitor»

Примите лицензионное соглашение, и, на этапе выборочной установки, выберите оба компонента (сервер и консоль управления). Перейдите к следующему этапу установки, названному «Тип устанавливаемого сервера»,

выберите тип сервера, и отметьте галочками пункты «Опубликовать сервер в Active Directory» и «Установить новую базу данных». Далее, выберите базу данных – PostgreSQL, и, перейдя к следующему этапу, введите параметры подключения к БД (рис. 40), с ранее созданным паролем.

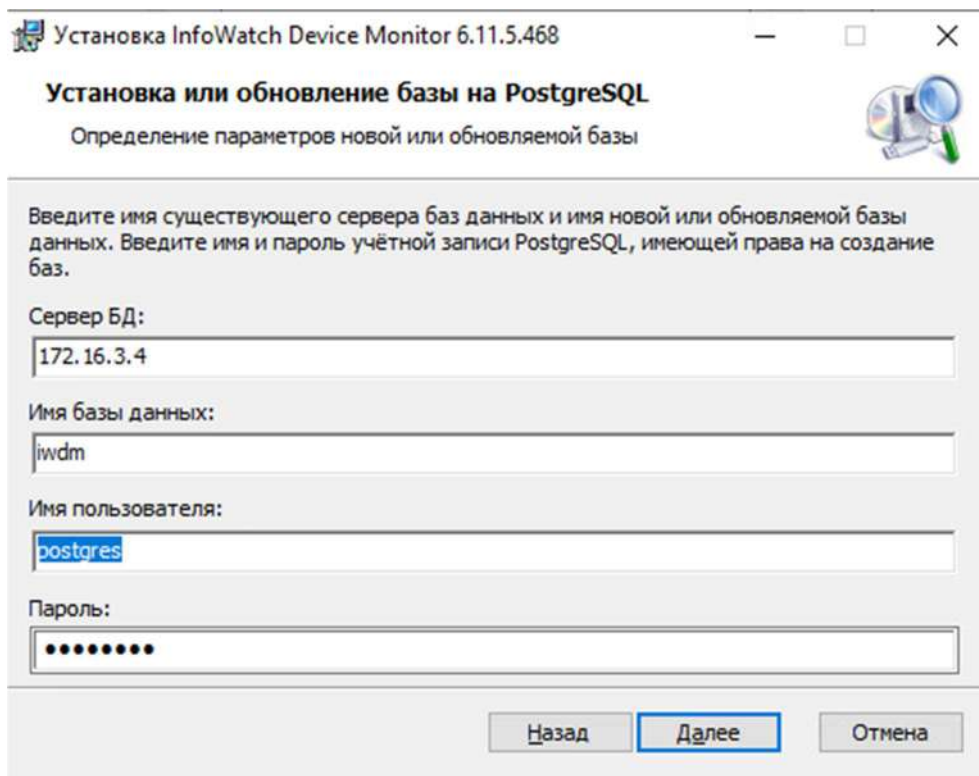


Рисунок 41 – «Параметры подключения к БД»

Соглашайтесь со всем подряд до пункта «Настройки защищенного канала». На этом пункте также согласитесь, ничего не изменяя, однако вам будет предложено сохранить ключ защищенного канала, для этого откроется окно проводника. Сохраните ключ с произвольным именем в любом месте. Продвигайтесь по установке далее, ничего не меняя. Дойдя до пункта «Учетная запись Администратора» - укажите имя администратора (admin), и пароль (xxXX1234). Затем, настройте соединение с Traffic Monitor (рис. 42), укажите адрес (iwtm) и токен авторизации (возьмите его из веб-интерфейса IWTM). Нажмите далее и установите Device Monitor. По окончании установки на рабочем столе появится ярлык «Консоль управления», для начала работы с IWDM – откройте его и войдите в консоль (адрес – localhost, логин – admin, пароль – xxXX1234).

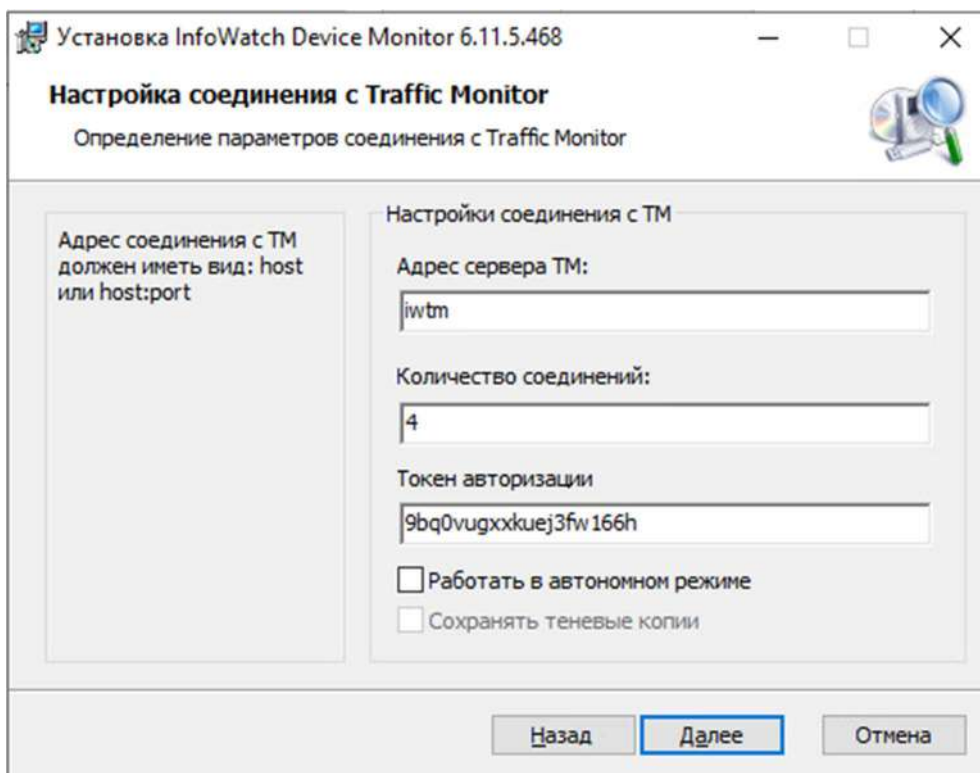


Рисунок 42 – «Параметры подключения к Traffic Monitor»

Перейдите ко вкладке «Инструменты» и откройте «Пользователи консоли и роли».

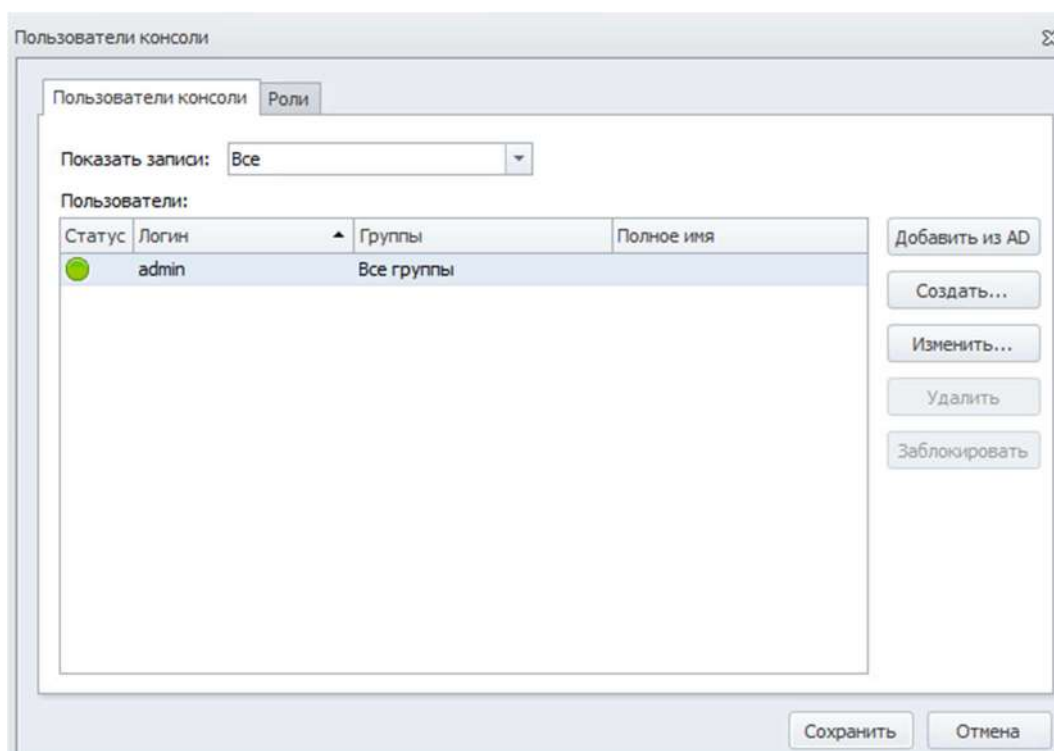


Рисунок 43 – «Пользователи консоли»

В открывшемся окне нажмите кнопку «Добавить из AD», после чего, в поле «Выберите добавляемого пользователя» введите «iwdm-admin» и нажмите «Сохранить», затем откроется дополнительное окно для управления ролями пользователя (рис. 44). Во всех доступных полях добавьте все, что только можно, ведь пользователь должен иметь максимальные права. Ваша задача сделать так, как на (рис. 45). Затем сохраните и вернитесь к настройкам. Найдите пункт «Интеграция с Active Directory», откройте его и создайте новое подключение:

- Имя домена: demo.lab;
- Синхронизировать: Компьютеры;
- Синхронизируемые директории: Все директории.

Более ничего не меняйте и сохраните подключение. Создайте второе подключение по аналогии с первым, но в пункте «Синхронизировать», выберите «Пользователи»



Создание пользователя

Логин: DEMO\jwdm-admin

Пароль: \*\*\*\*\*

Повтор пароля: \*\*\*\*\*

Полное имя: jwdm-admin

Видит сотрудников

Группа сотрудников	Роль пользователя

Добавить...  
Изменить...  
Удалить

Видит компьютеры

Группа компьютеров	Роль пользователя

Добавить...  
Изменить...  
Удалить

Общие роли

--

Выбрать  
Удалить

Сохранить

Отмена

Рисунок 44 – «Пользователи консоли»

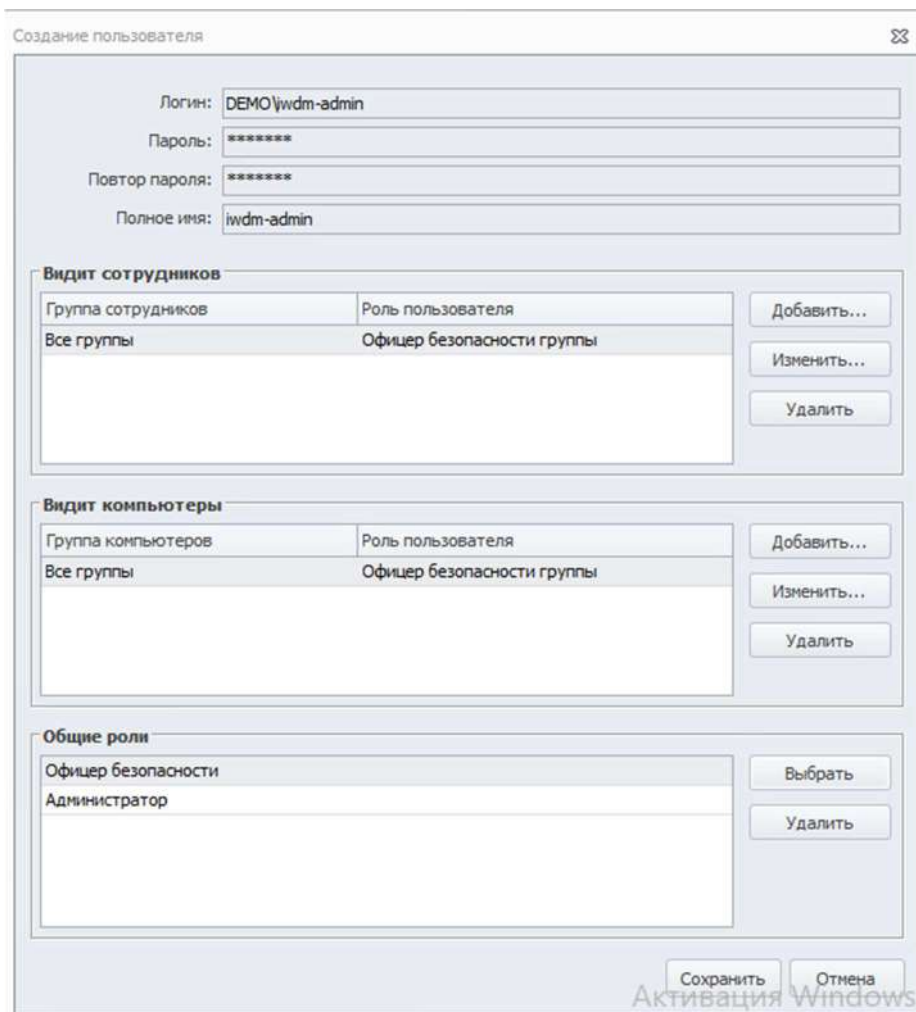


Рисунок 45 – «Пользователи консоли, как должно быть»

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).

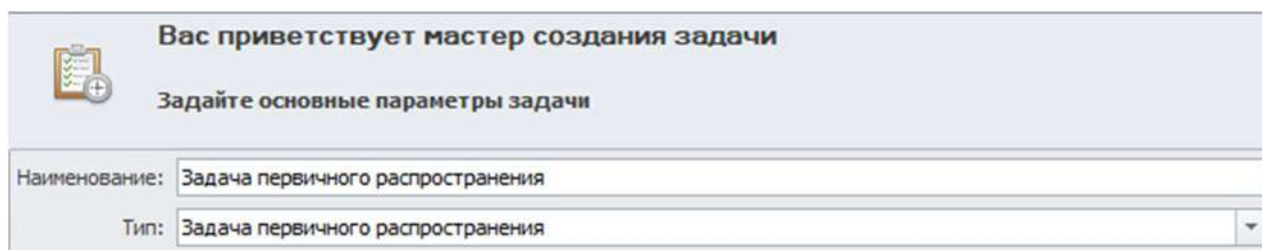


Рисунок 46 – «Шаг 1»

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.

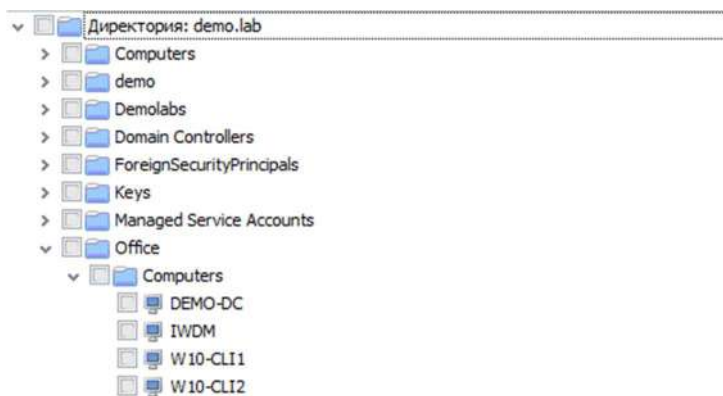


Рисунок 47 – «Добавление компьютеров»

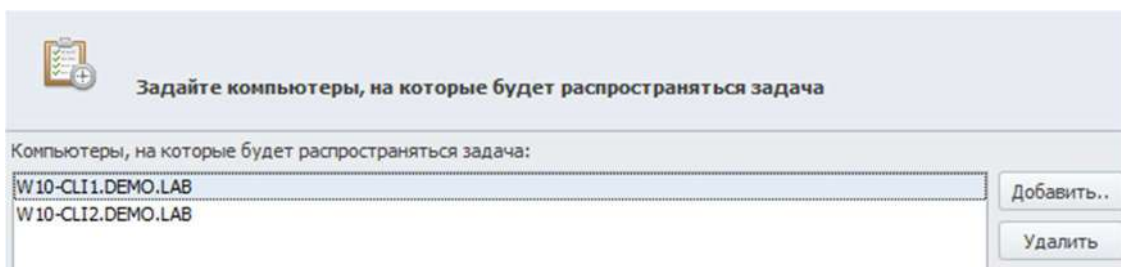
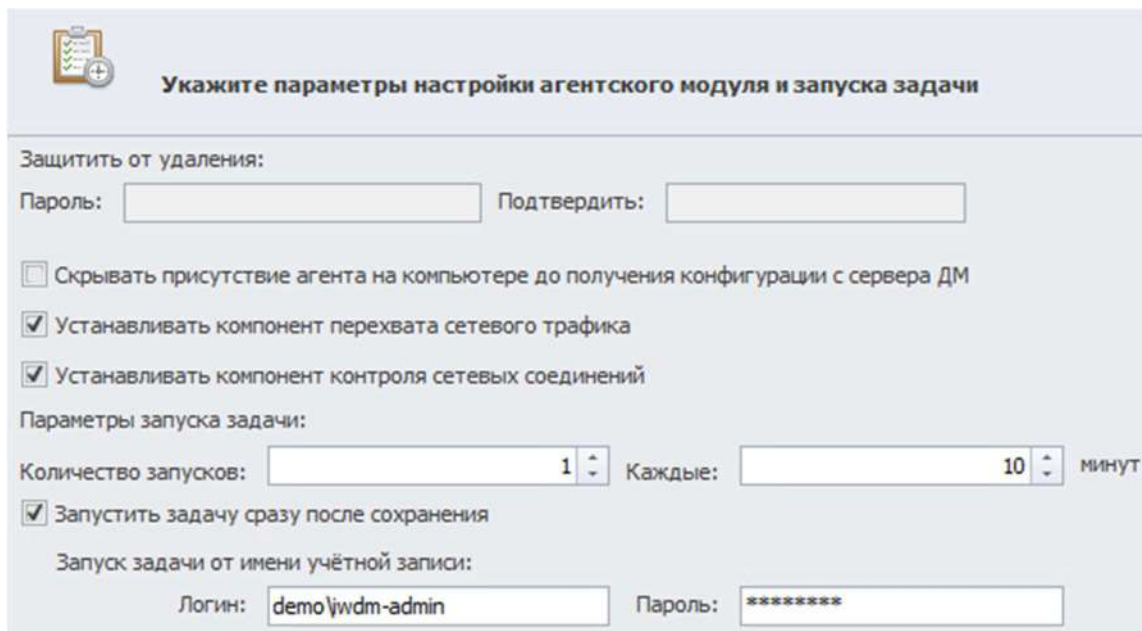


Рисунок 48 – «Шаг 2»

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:

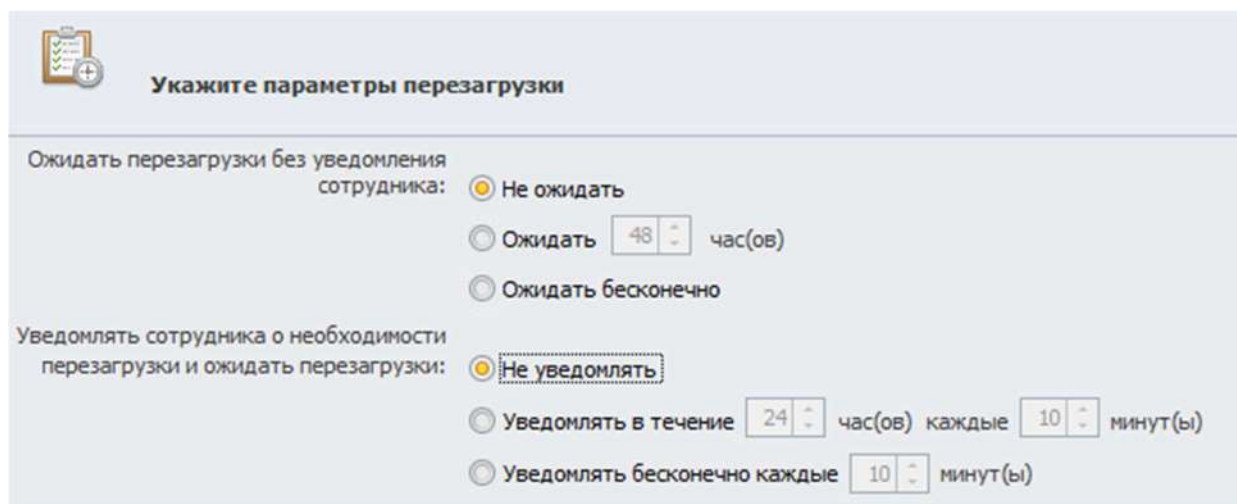
Количество запусков:  Каждые:  минут

☒ 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

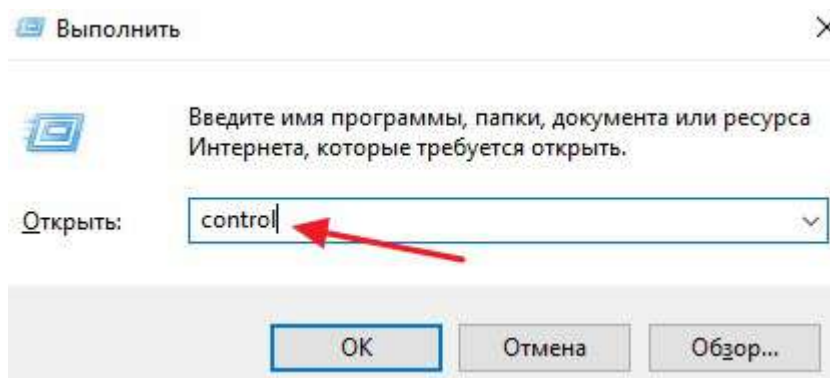


Рисунок 51 – «Запуск панели управления»

Настройка параметров компьютера

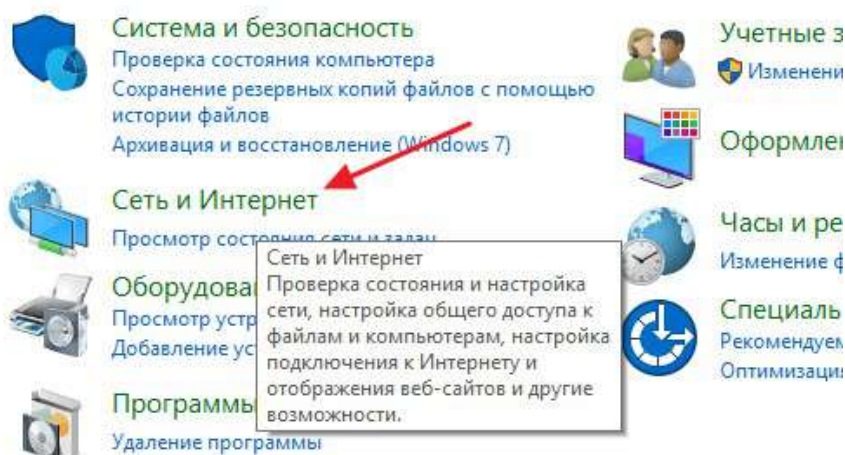
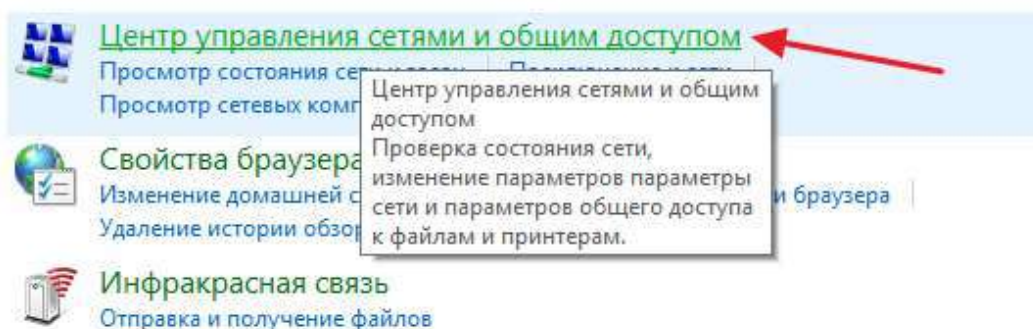


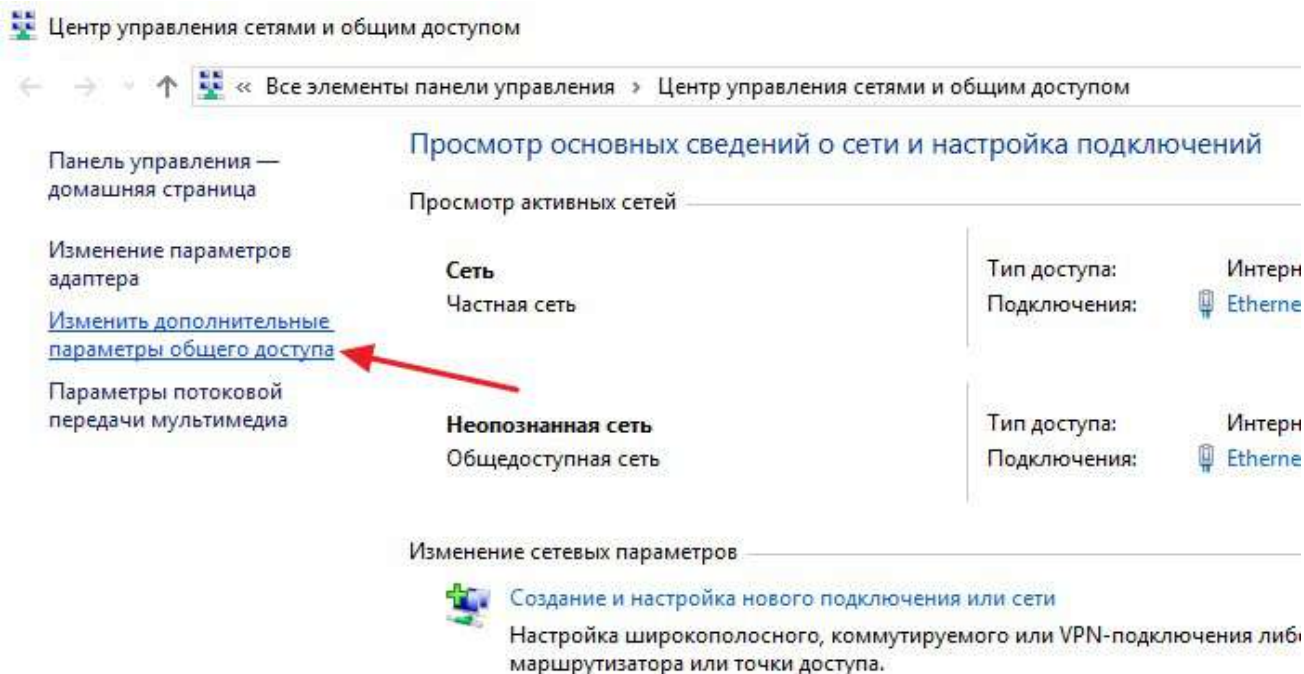
Рисунок 52 – «Сеть и Интернет»





### 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).

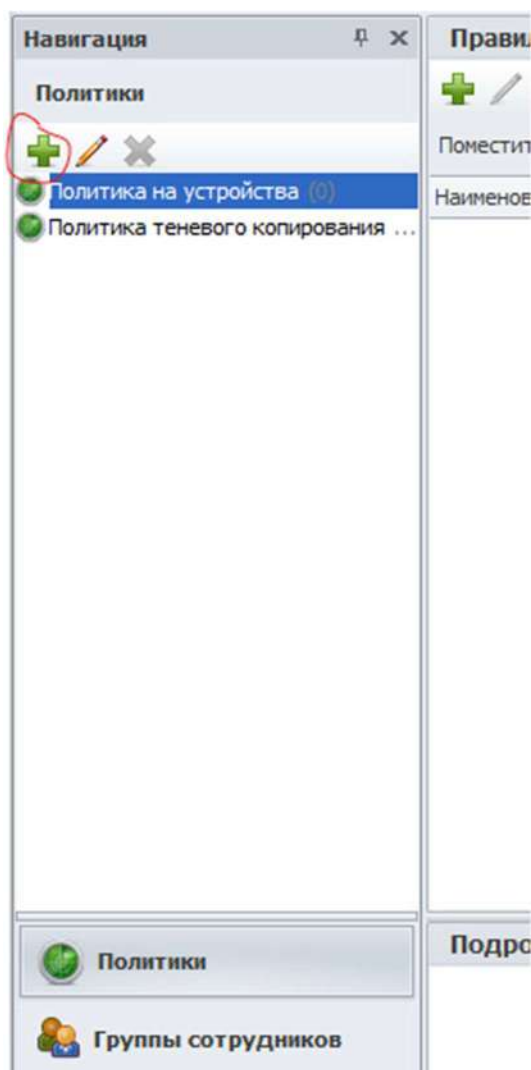


Рисунок 55 - «Создание политики»

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.

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-cl11. 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 «scal.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.

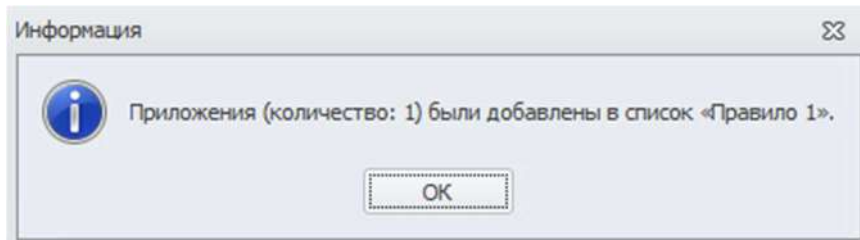
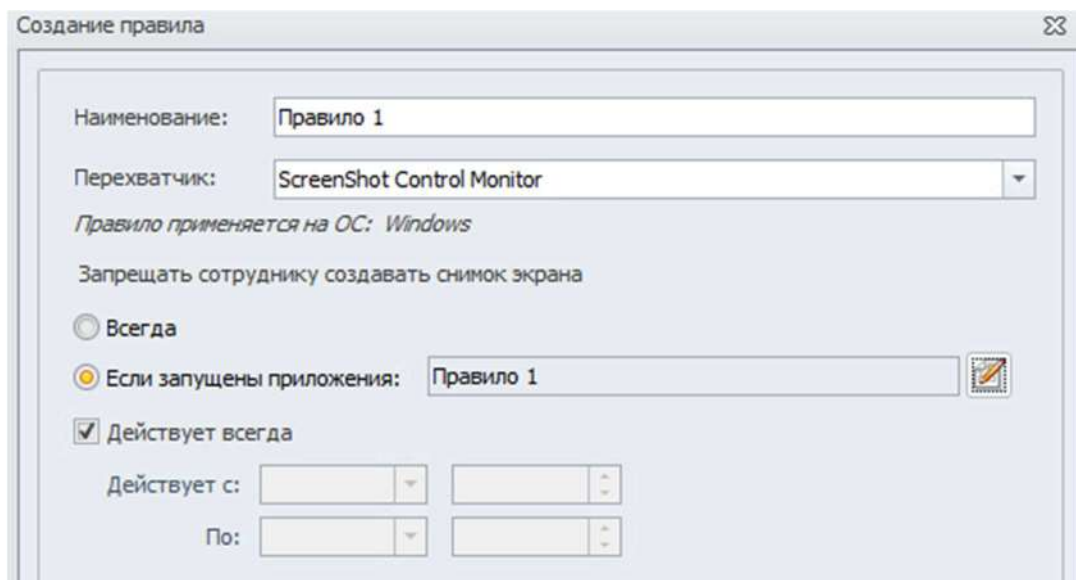


Рисунок 59 – «Успешное добавление приложения»

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:

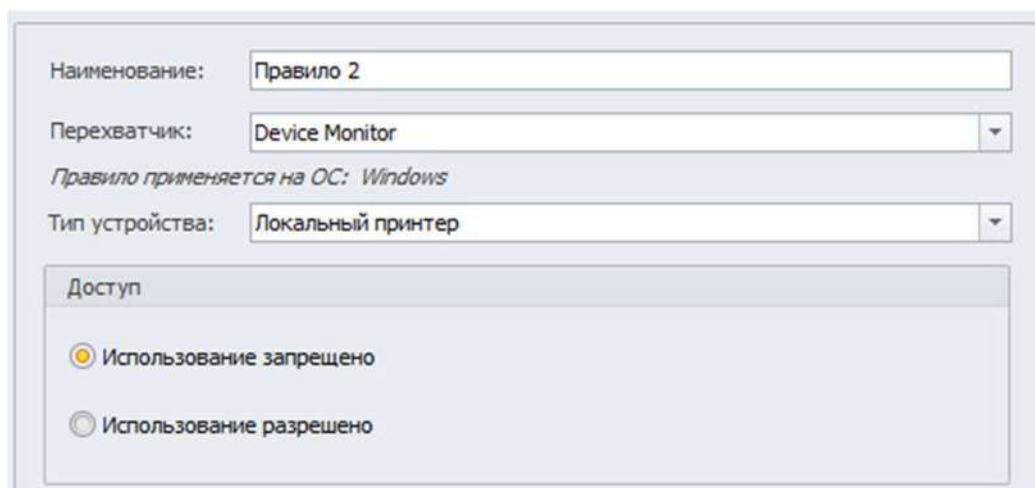
☒ Действует всегда

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).

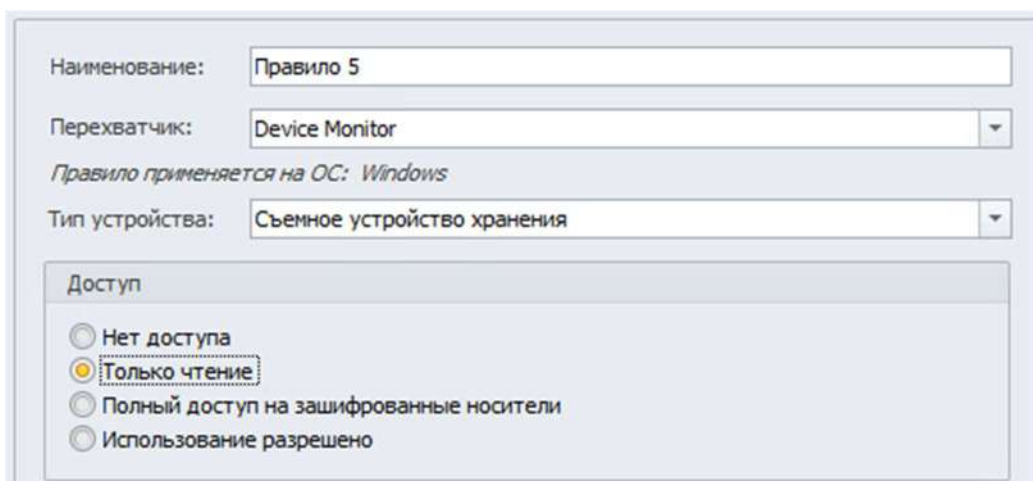
*Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.*

### 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*

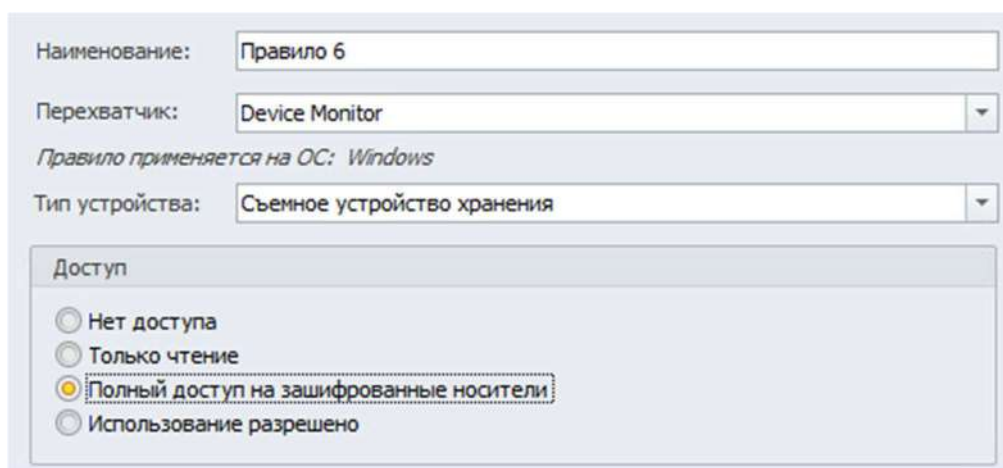
Тип устройства:

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).

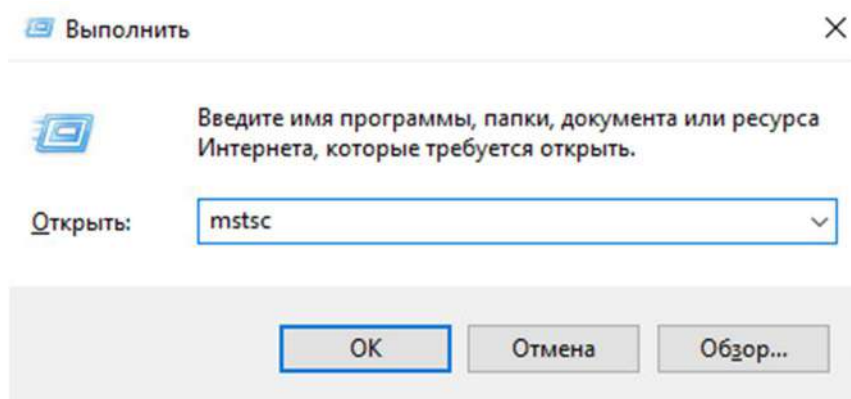


Рисунок 66 – «Открытие подключение к удаленному рабочему столу»

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.

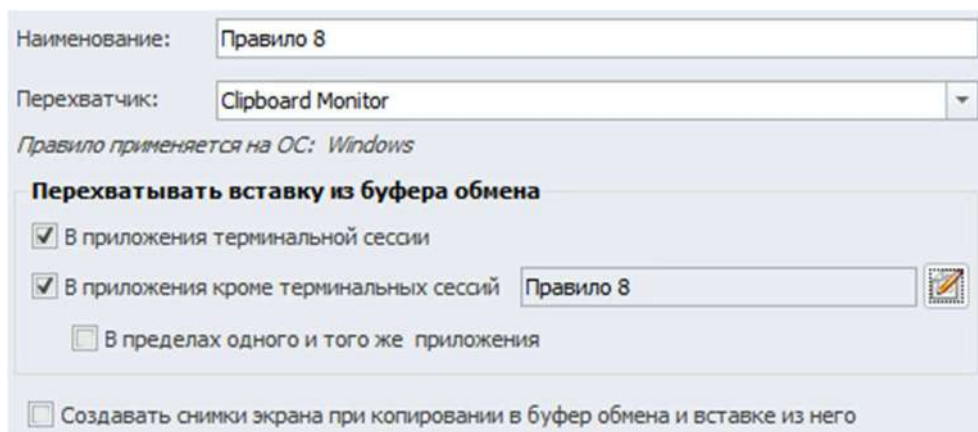


Рисунок 69 - «Правило 8»

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 штат 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».

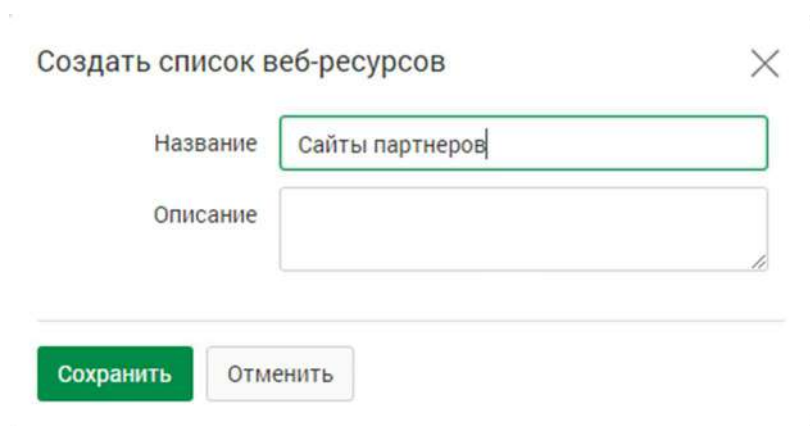


Рисунок 72 – «Создание список веб-ресурсов»

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

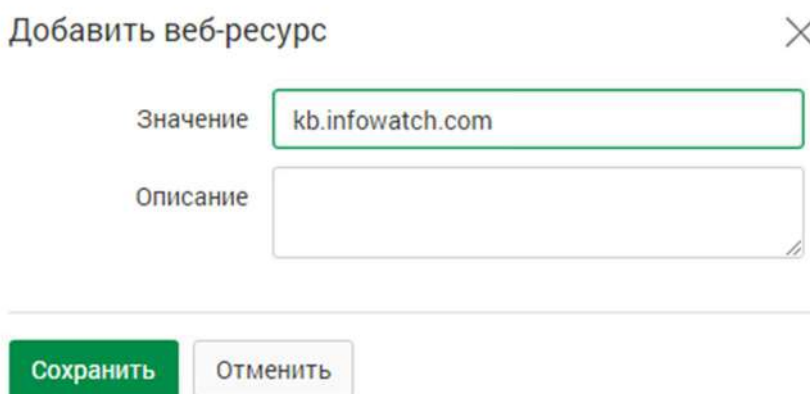


Рисунок 73 – «добавление веб-ресурсов»

## 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».

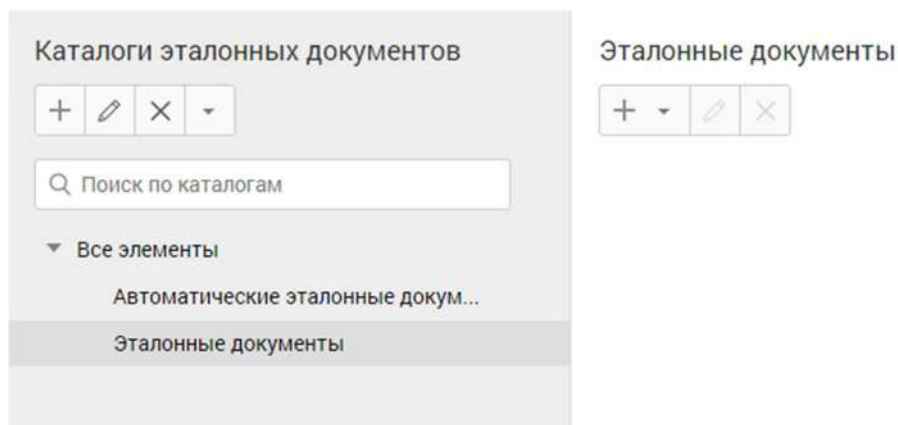


Рисунок 75 – «Эталонные документы»

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%.

**Создать** ✕

Название

Порог цитируемости для текстовых данных

10 %

Порог цитируемости для бинарных данных

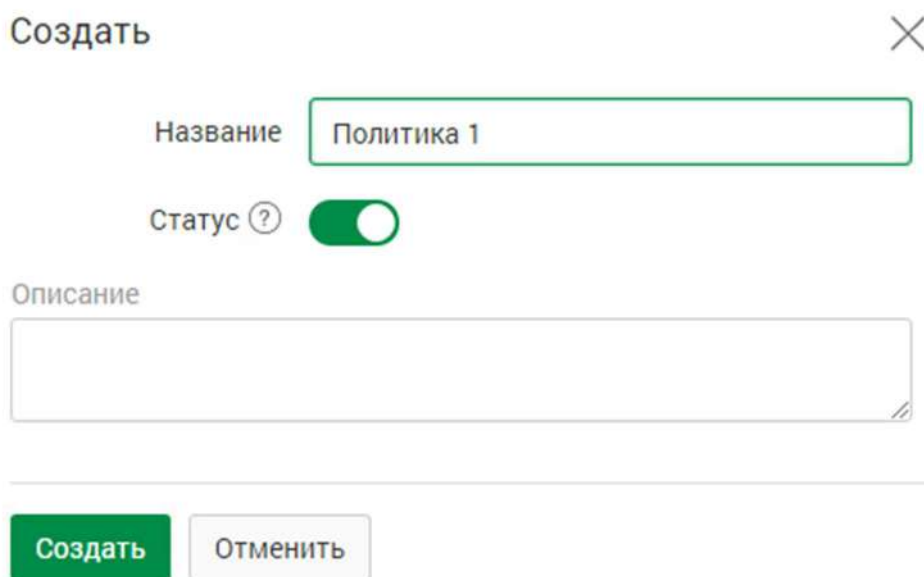
50 %

Описание

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).



The image shows a 'Создать' (Create) dialog box with a close button (X) in the top right corner. Inside the dialog, there is a label 'Название' (Name) followed by a text input field containing 'Политика 1'. Below this is a label 'Статус' (Status) with a question mark icon and a green toggle switch that is currently turned on. Underneath is a label 'Описание' (Description) followed by a large empty text area. At the bottom of the dialog, there are two buttons: a green 'Создать' (Create) button and a grey 'Отменить' (Cancel) button.

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.

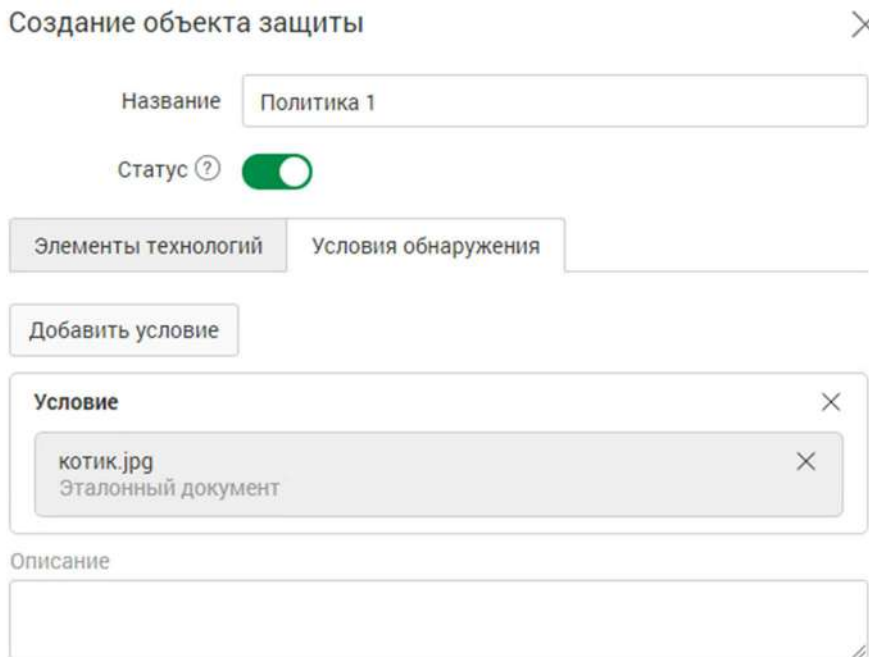


Рисунок 79 – «Создание объекта защиты»

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».

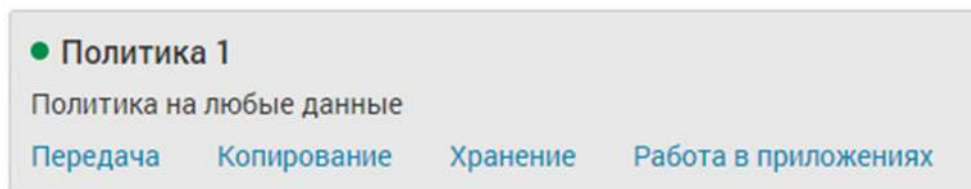


Рисунок 80 – «Политика 1»

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...

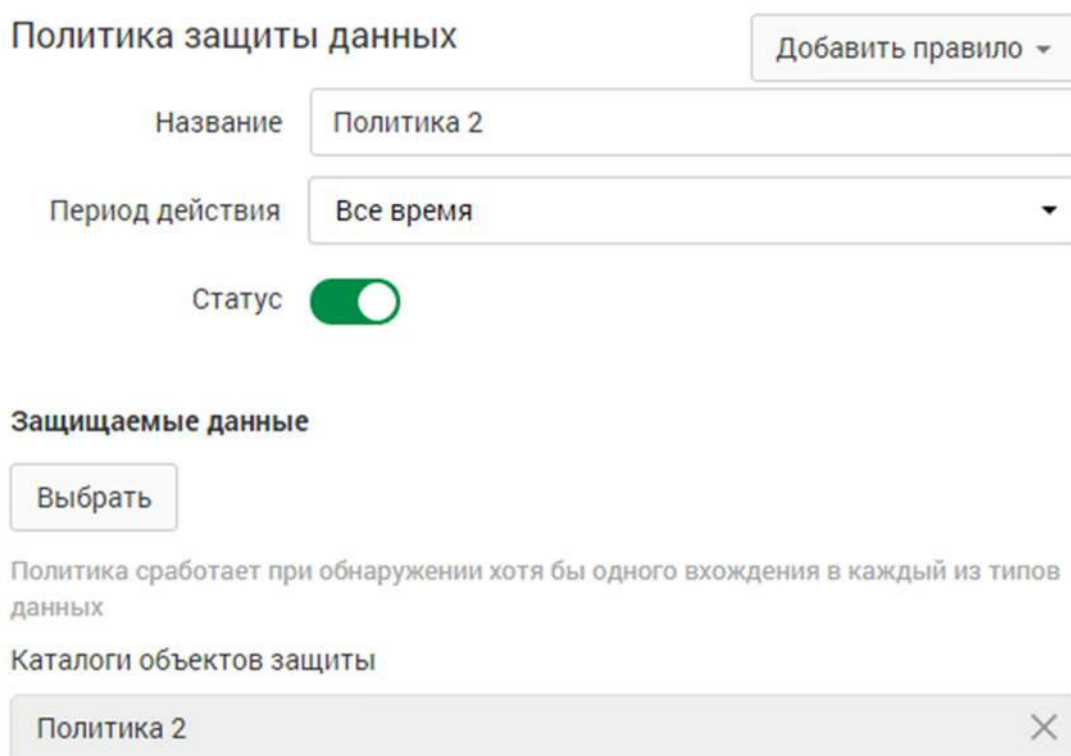
10

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**

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

## Действия при срабатывании правила

Отправить почтовое уведомление <sup>?</sup>	<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»

