Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “DemoDept” в корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

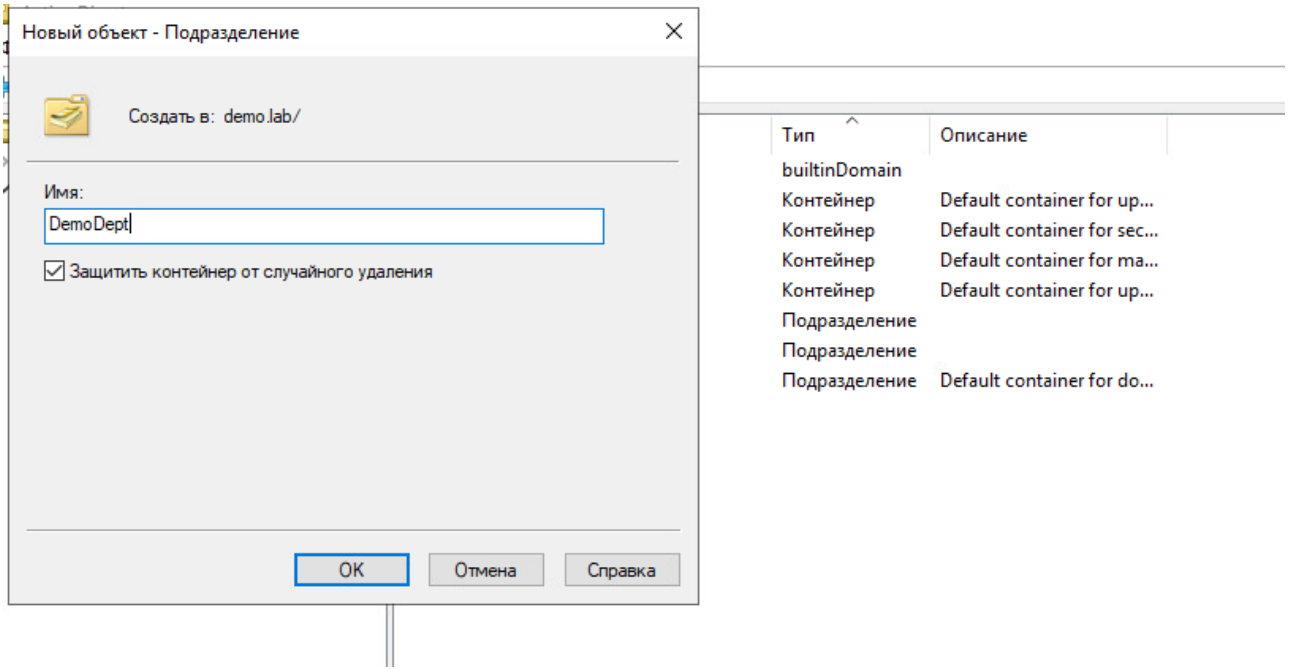

Рисунок 1 – Создание подразделения

Внутри созданного подразделения “DemoDept” необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: iwtm-admin, пароль: xxXX2233, права пользователя домена

Логин: ldap-sync, пароль: xxXX2233, права пользователя домена

Логин: iwdm-root, пароль: xxXX2233, права администратора домена и локального администратора

Логин: user-pc, пароль xxXX2233, права пользователя домена

Логин: user-gp, пароль xxXX2233, права пользователя домена

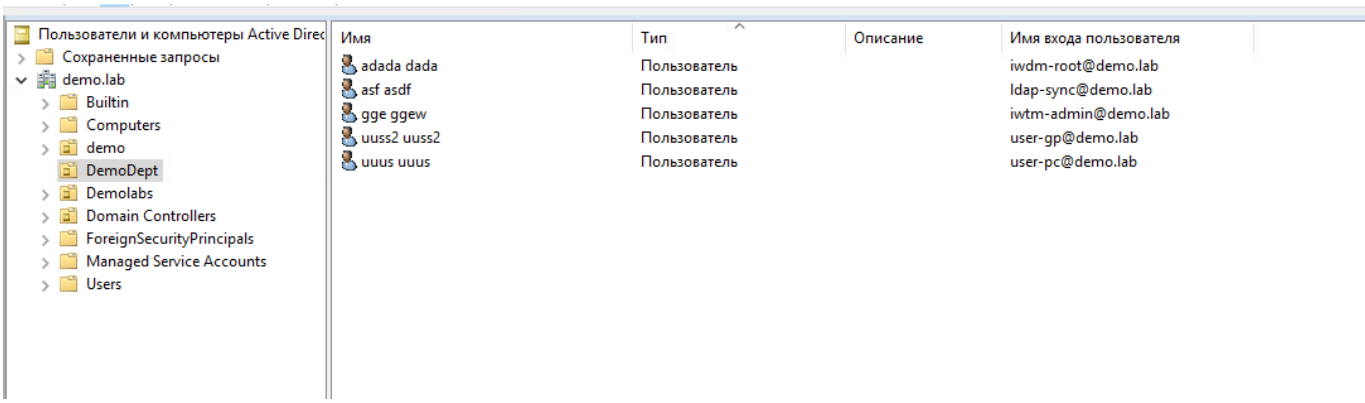

Рисунок 2 – Создание пользователей

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен. Необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случае несовпадений настроить DNS правильно.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

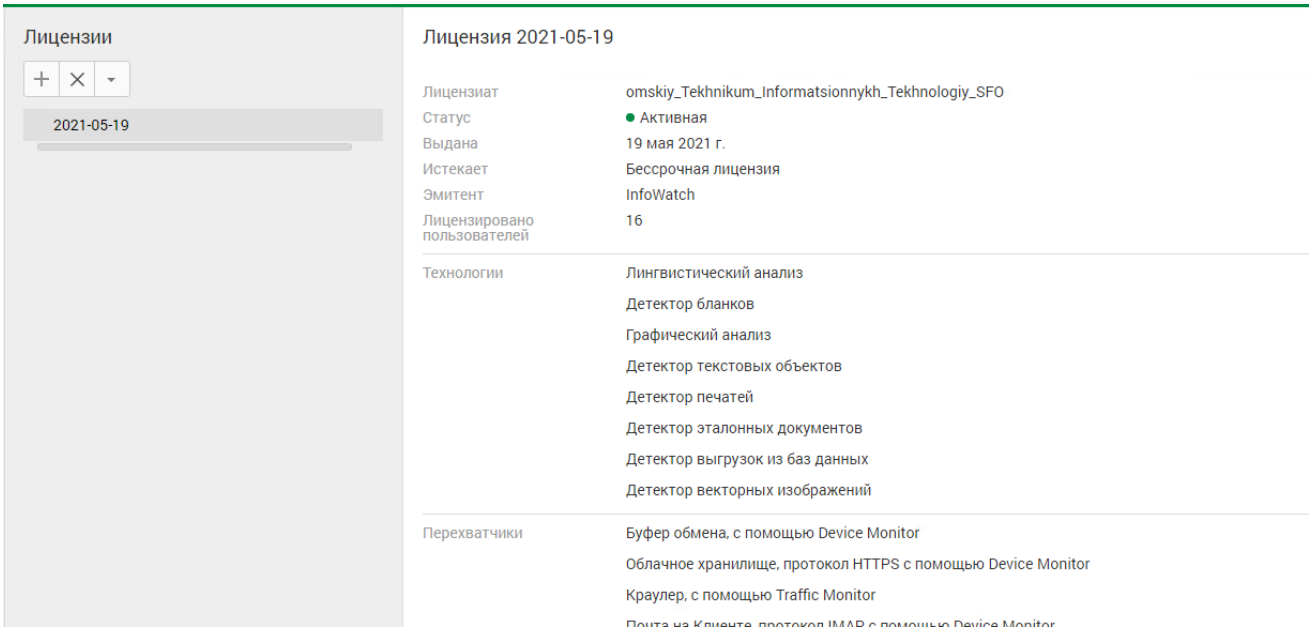

Рисунок 3 – Проверка актуальной лицензии

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя ldap-sync.

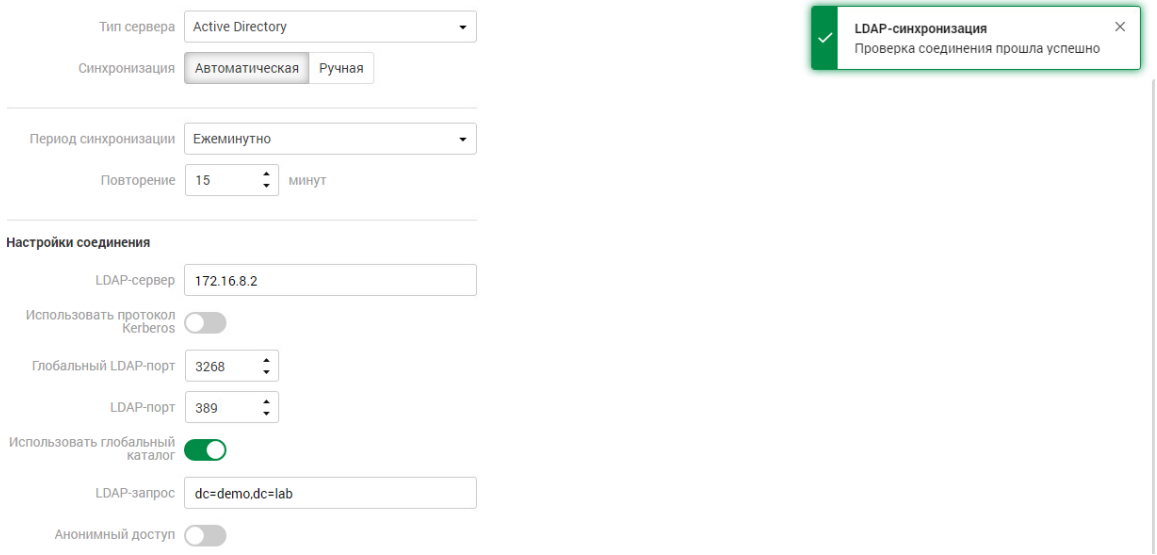

Рисунок 4 – Зашёл на вебморду и синхронизировался с сервером.

Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-admin с полными правами офицера

безопасности и на администрирование системы, полный доступ на все области видимости.

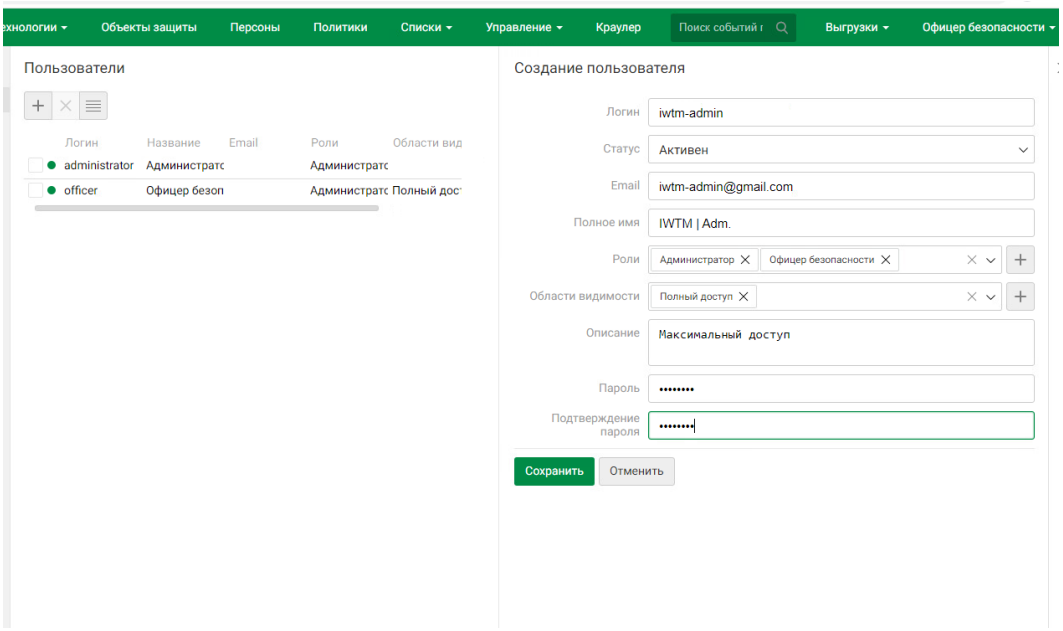

Рисунок 5 – Создание пользователя с фулл правами

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

Рисунок 6 – Создание отчёта на рабочем столе

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя iwdm-root (важно).

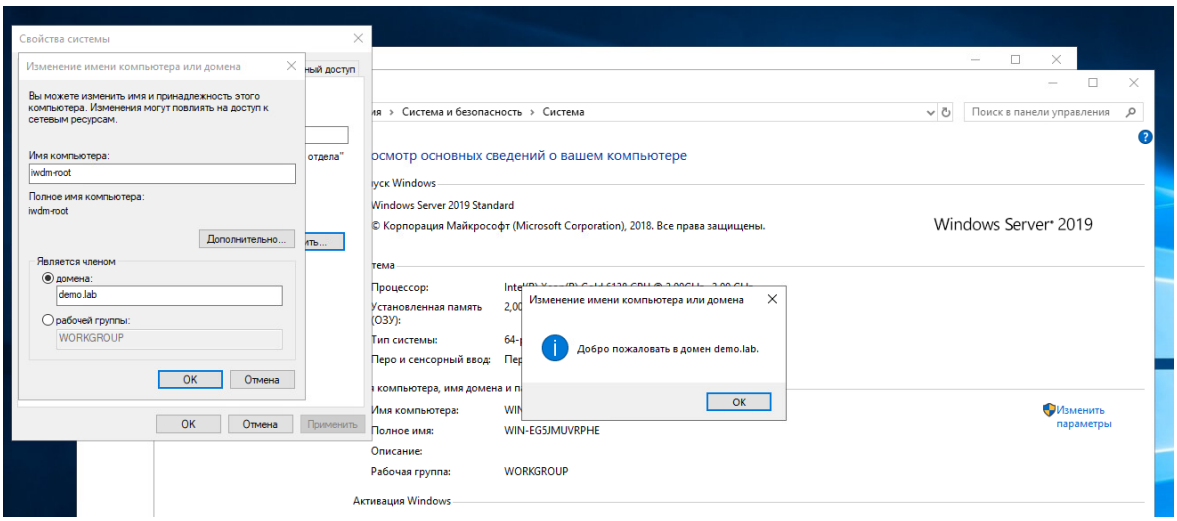

Рисунок 7 – Вход в домен

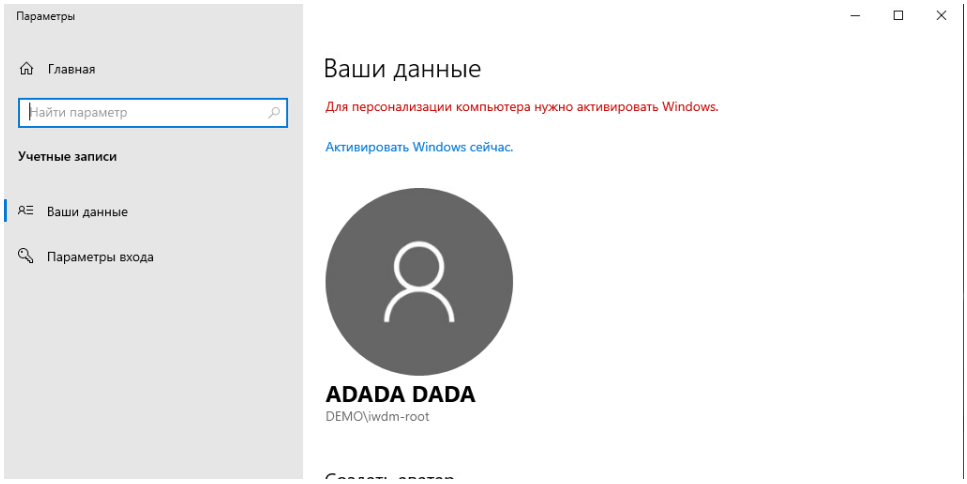

Рисунок 8 – Проверка правильности входа

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

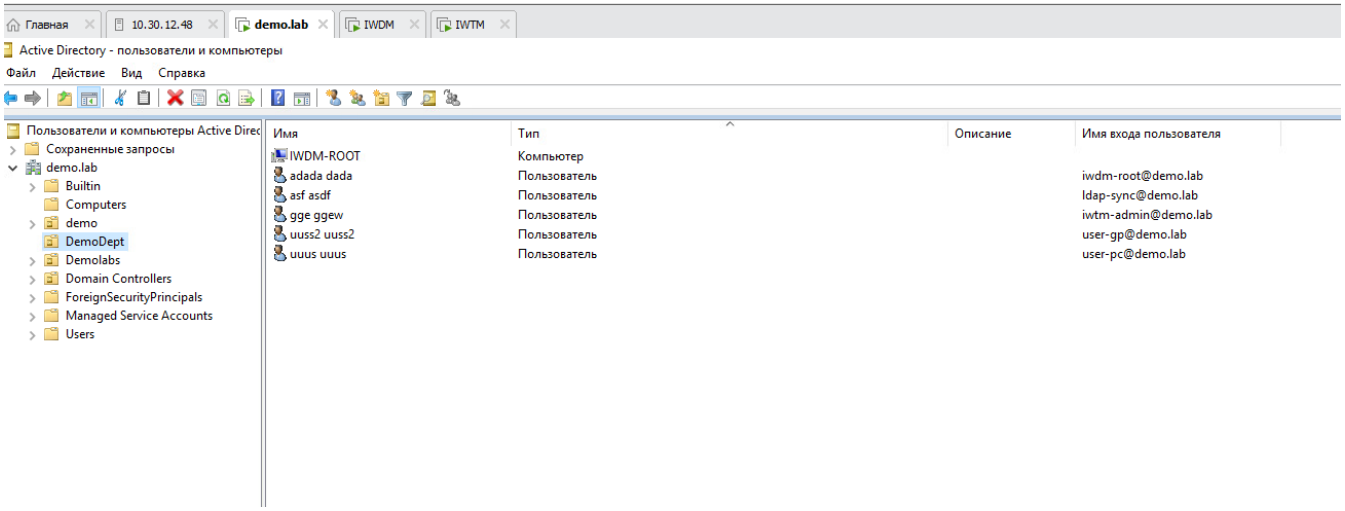

Рисунок 9 – Перенос компьютера в подразделение DemoDept

Установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя xxXX2233.

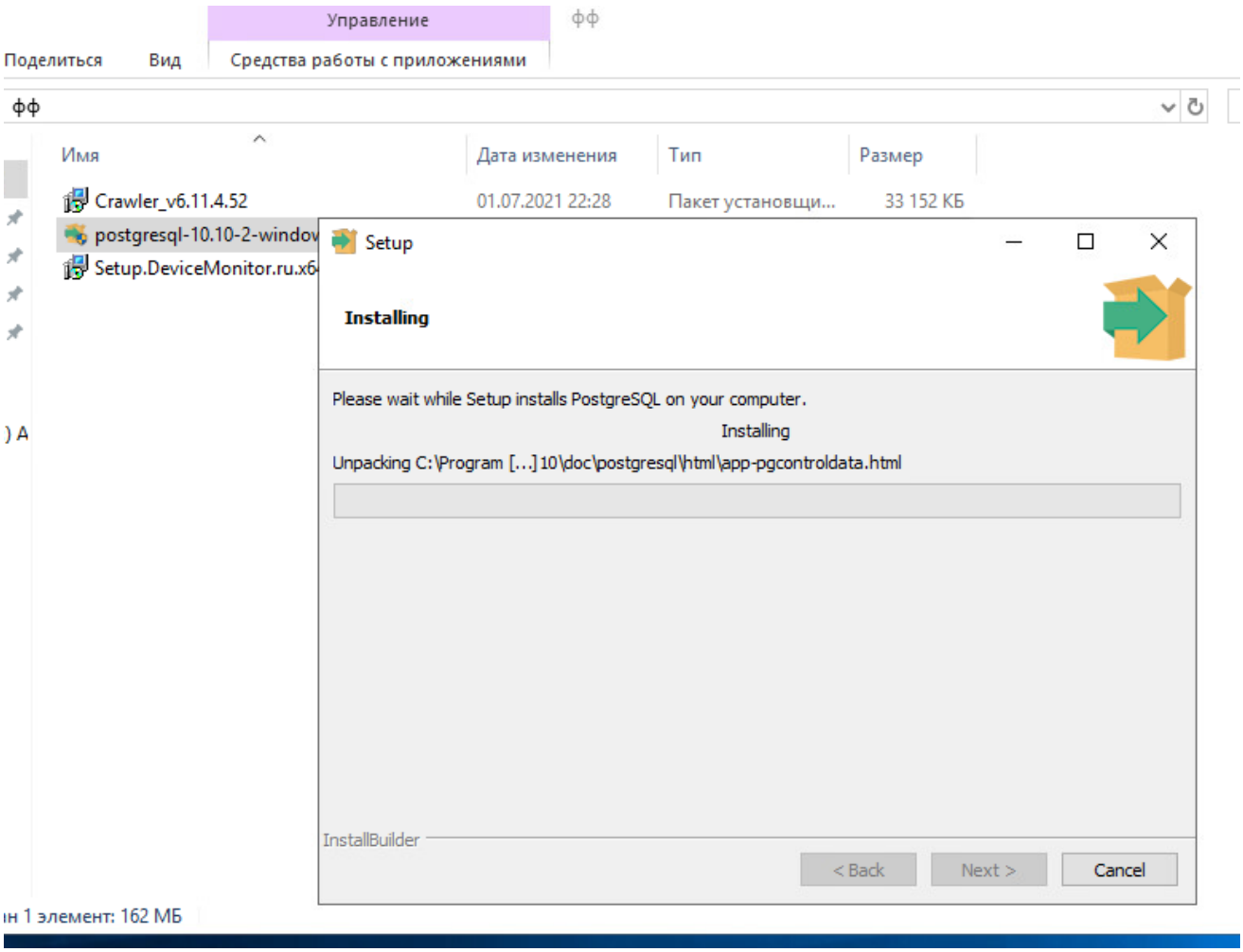

Рисунок 10 – Установка PostgreSQL

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД – рисунки 11-12

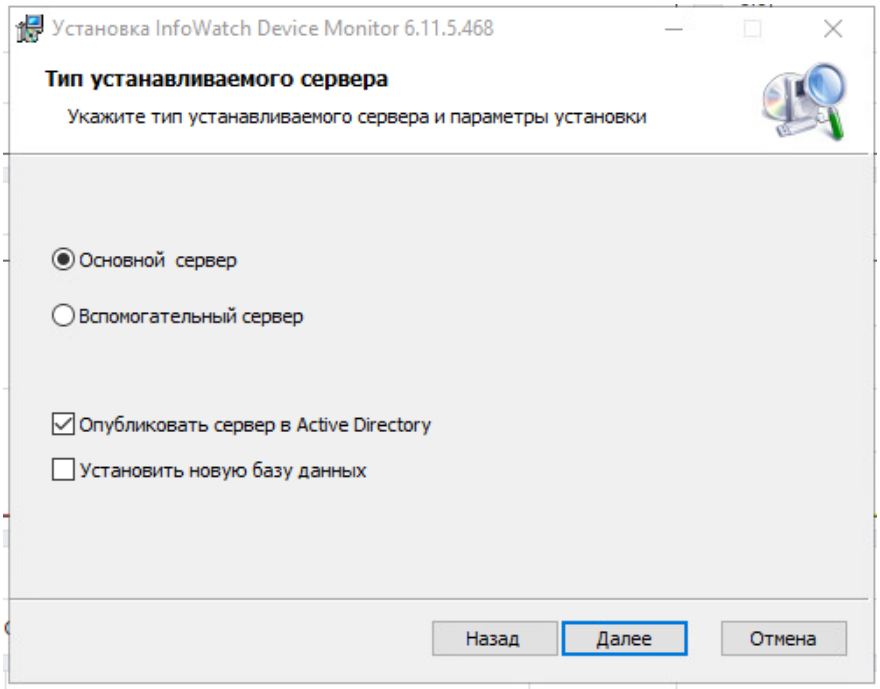

Рисунок 11

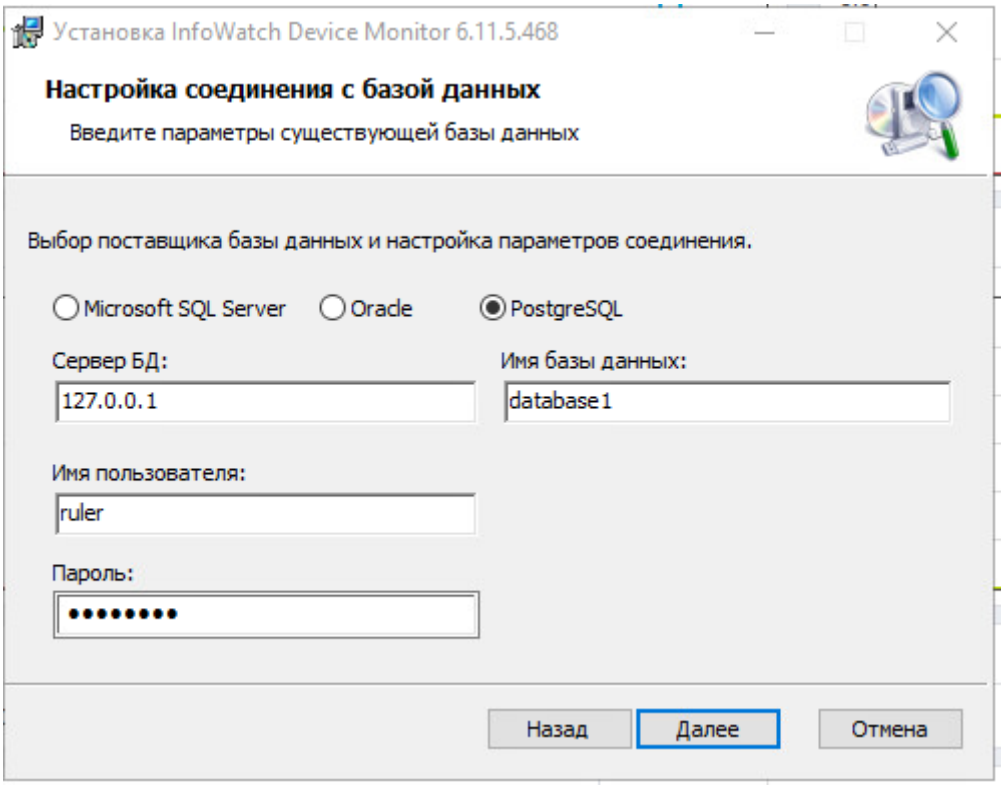

Рисунок 12

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: officer с паролем xxXX2233

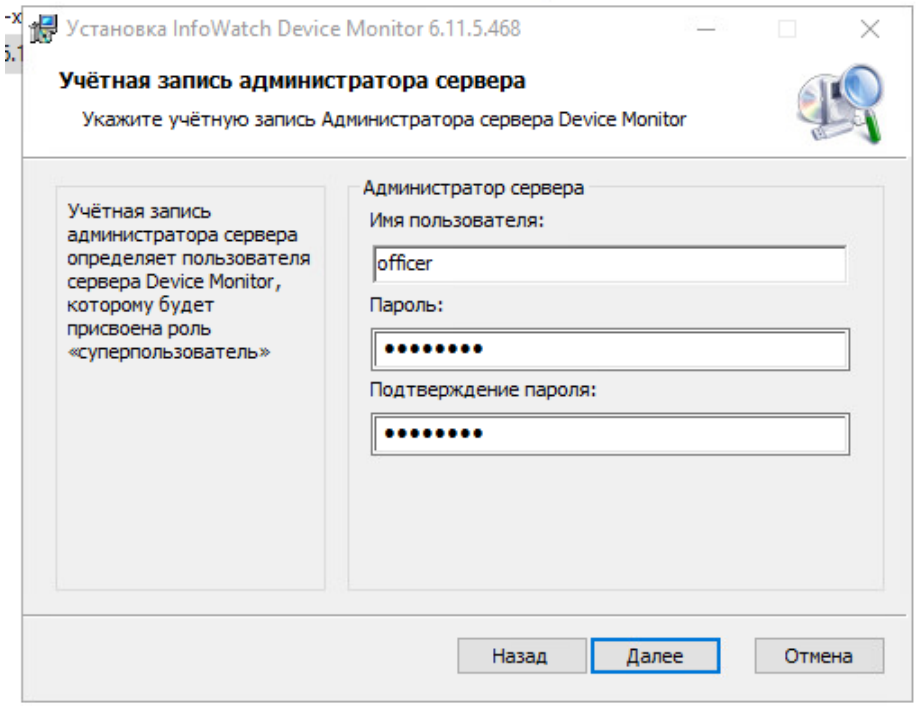

Рисунок 13 – Создание администратора сервера

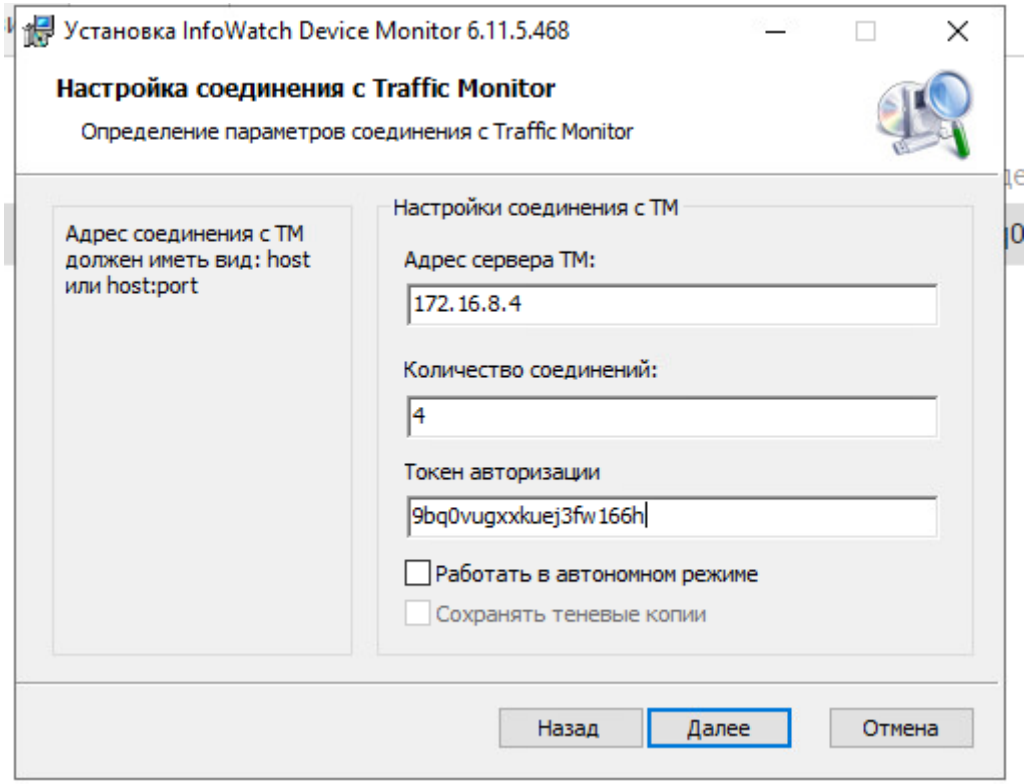

Рисунок 14 – Соединение с DLP-сервером

Синхронизировать каталог пользователей и компьютеров с Active Directory.

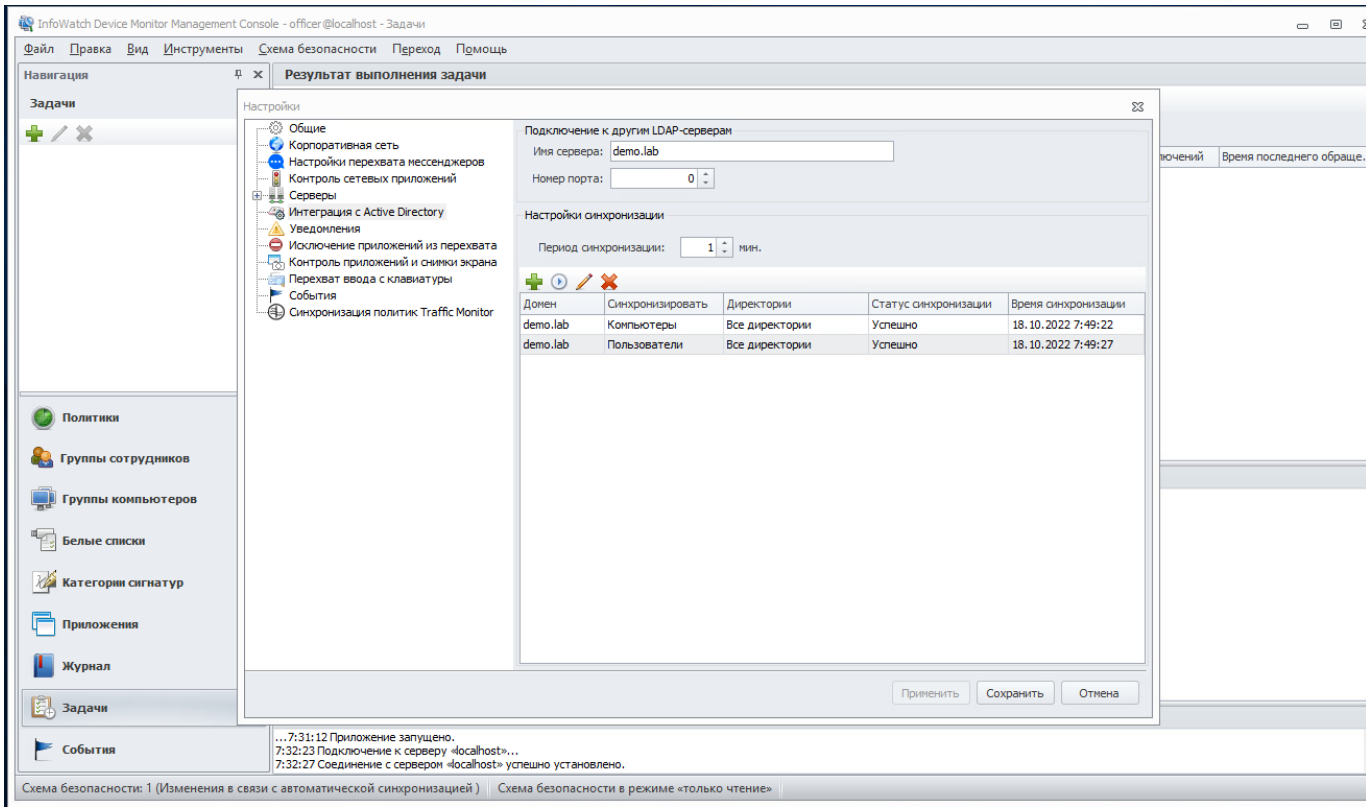

Рисунок 15 – Синхронизация контактов

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

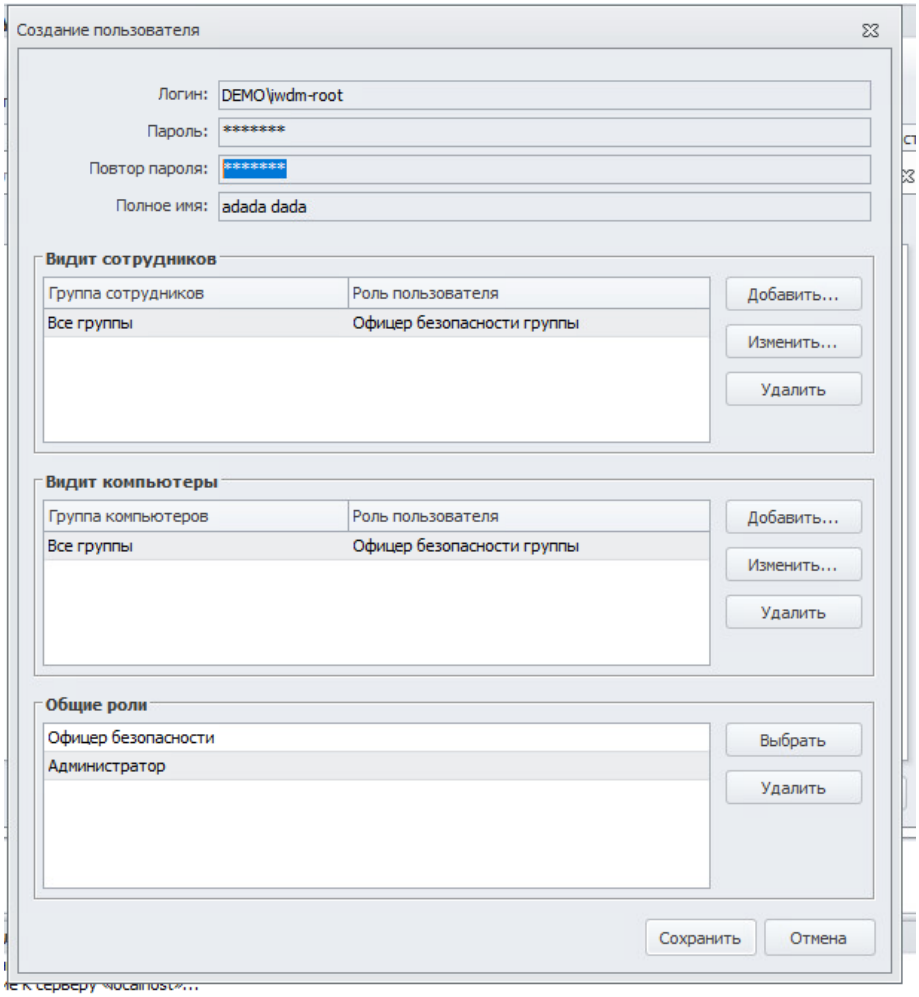

Рисунок 16 – Настройка входа от доменного пользователя

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

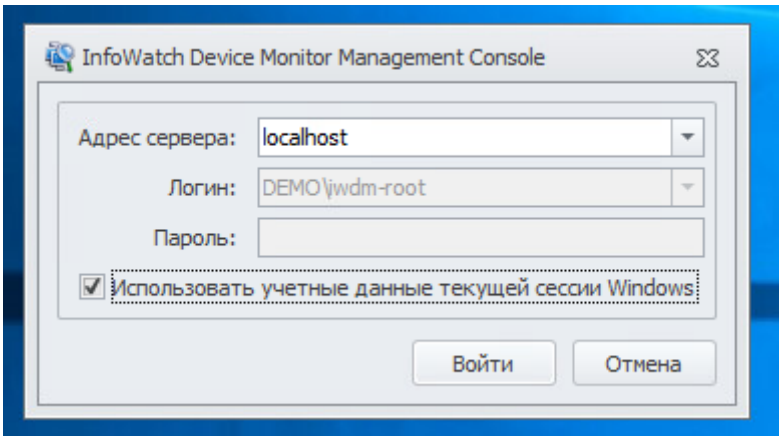

Рисунок 17 – Проверка успешного входа без пароля под idwm-root

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

Задание 4: Установка агента мониторинга на машине нарушителя

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

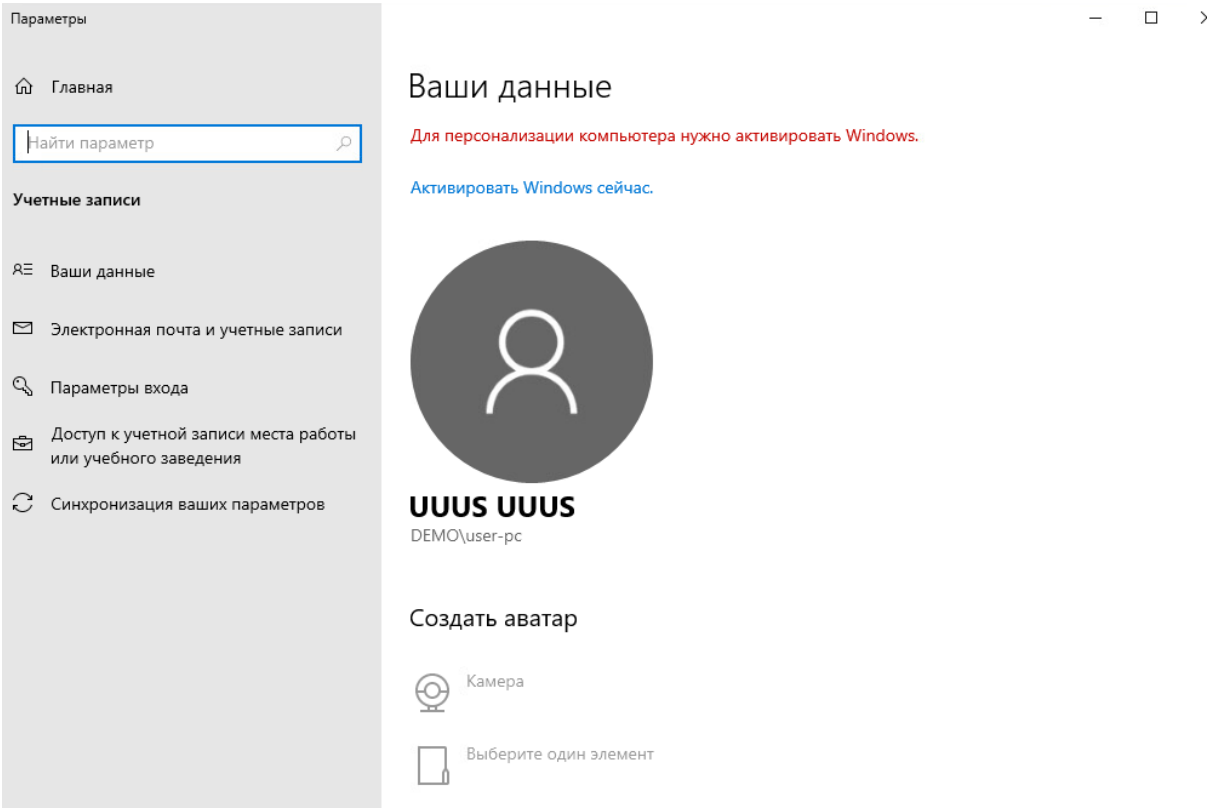

Рисунок 18 – Ввод первого клиента в домен

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-gp.

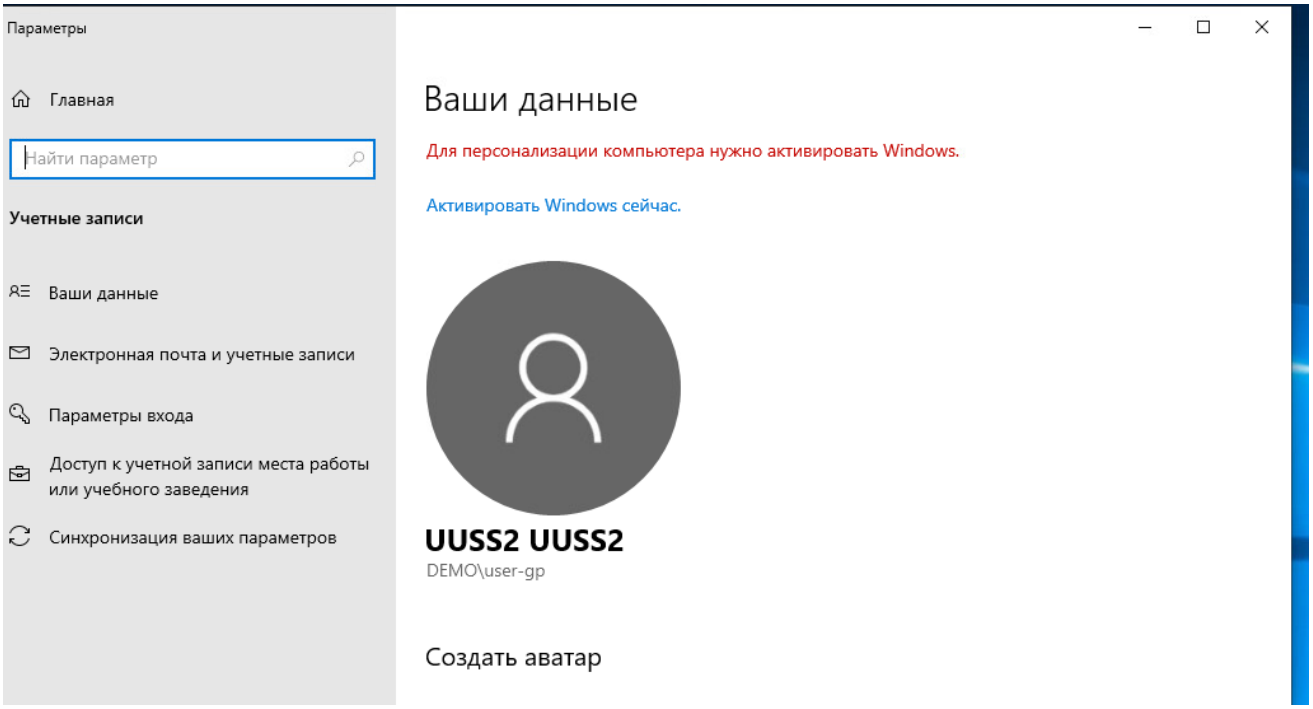

Рисунок 19 – Ввод второго клиента в домен

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “DemoDept” на домене.

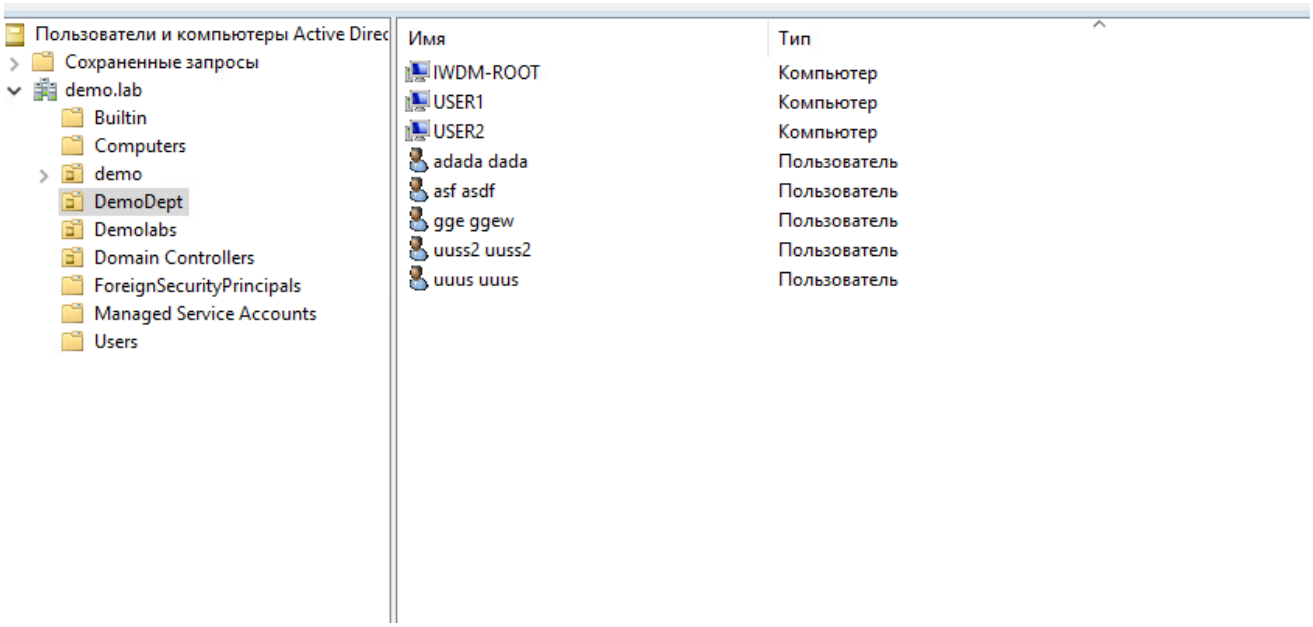

Рисунок 20 – Перенос компьютеров в подразделение

Установить агент мониторинга:

На машину 1 (user-pc) с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания и переноса любым способом пакета установки является некорректным выполнением задания

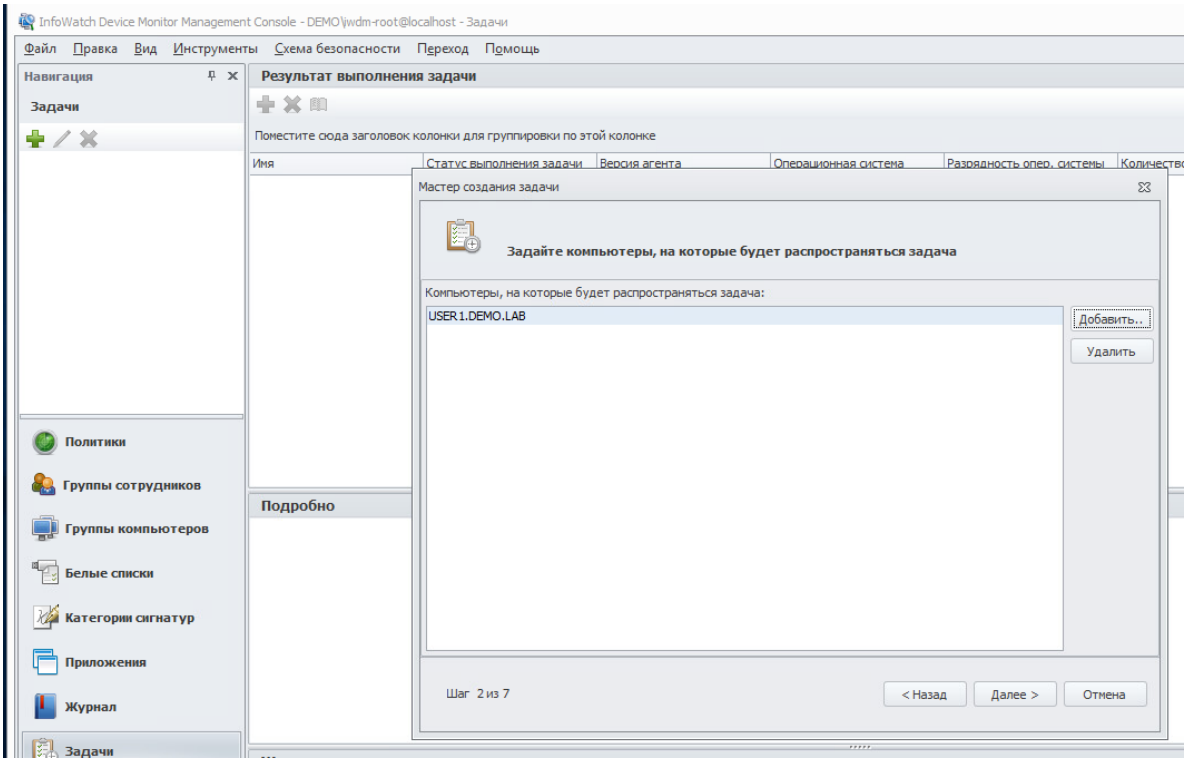

Рисунок 21 – Создание задачи первичного распространения

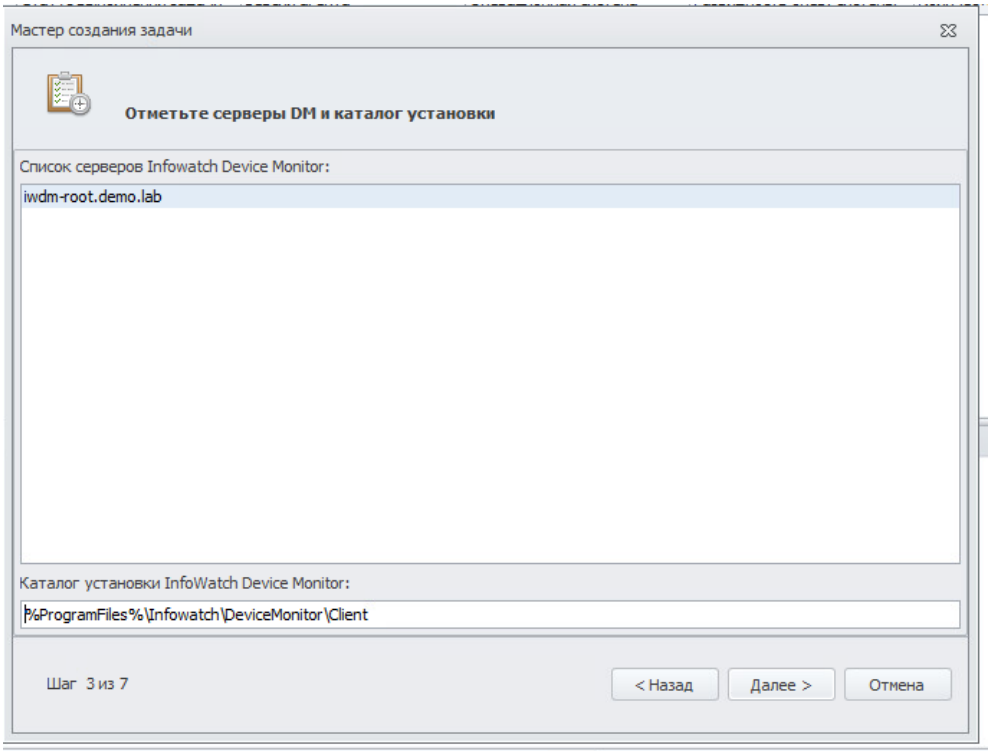

Рисунок 22 – Выбор каталога установки DeviceMonitor

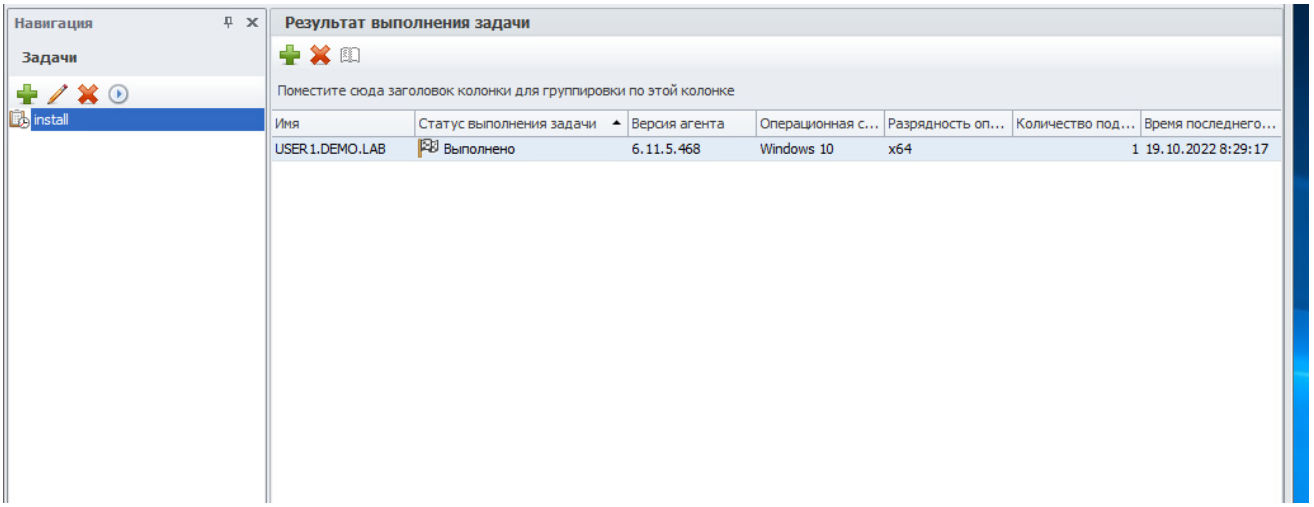

Рисунок 23 – Проверка успешной установки

На машину 2 (user-gp) с помощью групповых политик домена. Допускается как удаленная установка созданного вручную пакета, так и с помощью удаленной установки компонента Deploy Agent с последующей установкой через задачи сервера агентского мониторинга.

Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания

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

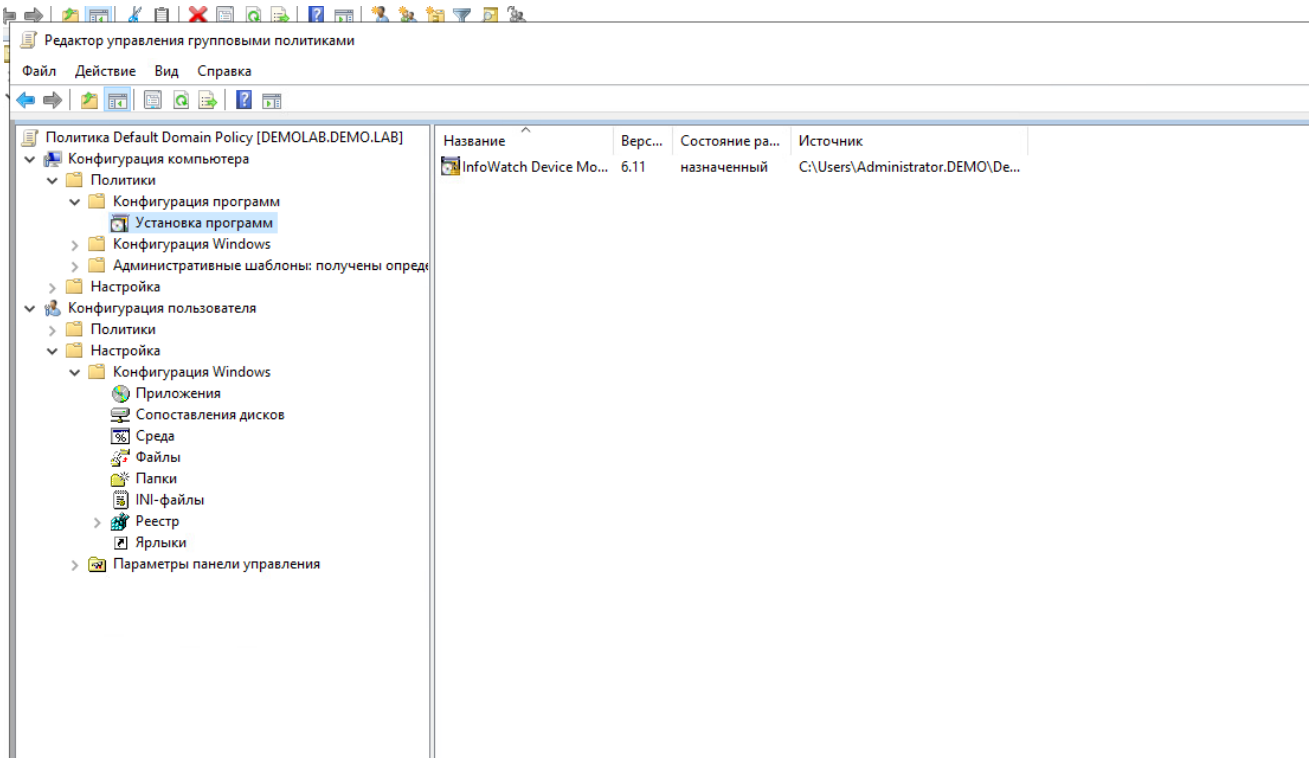

Рисунок 24 – Создание общего пакета установки

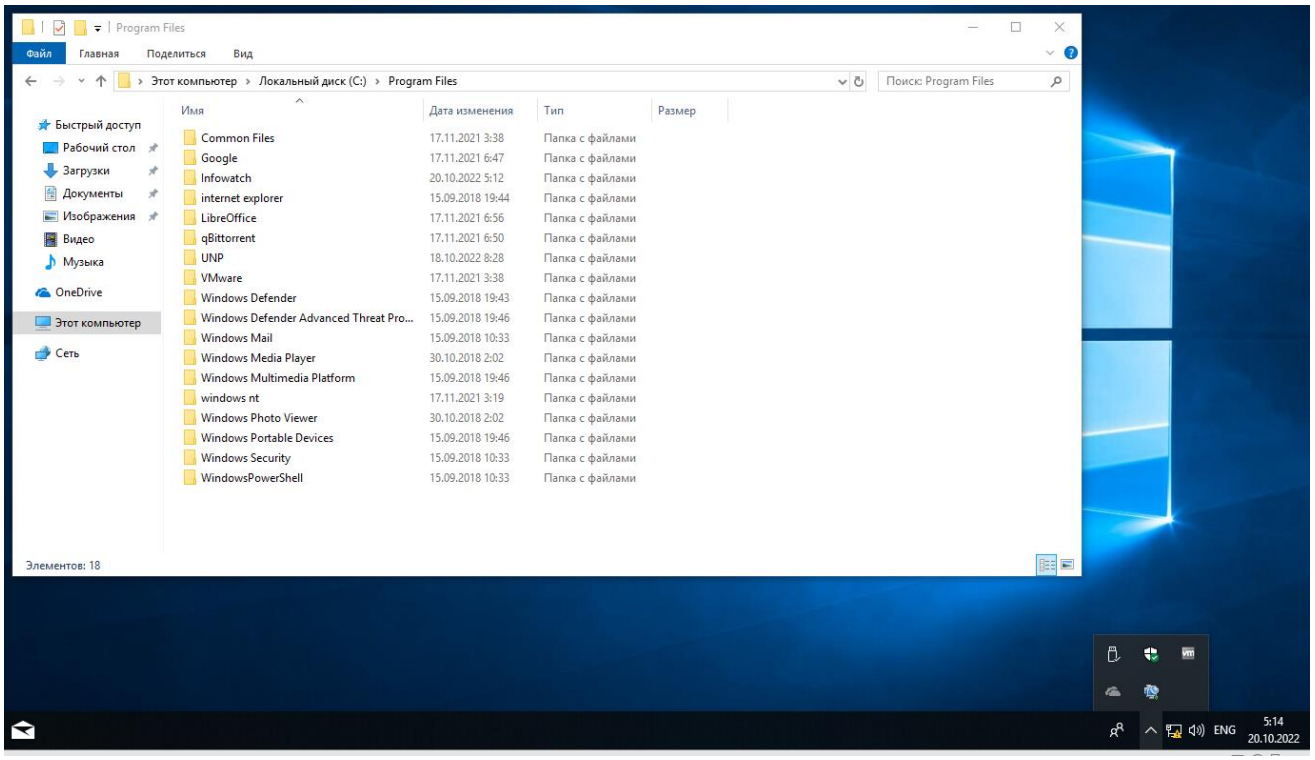

Рисунок 25 – Проверка, что установилось

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

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

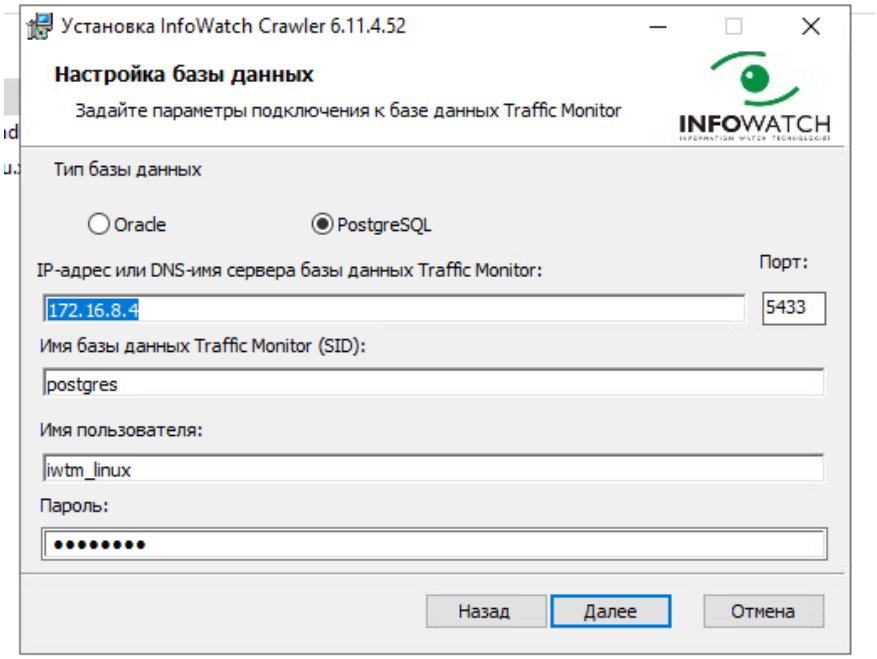

Рисунок 26 – Начальное окно установки Crawler

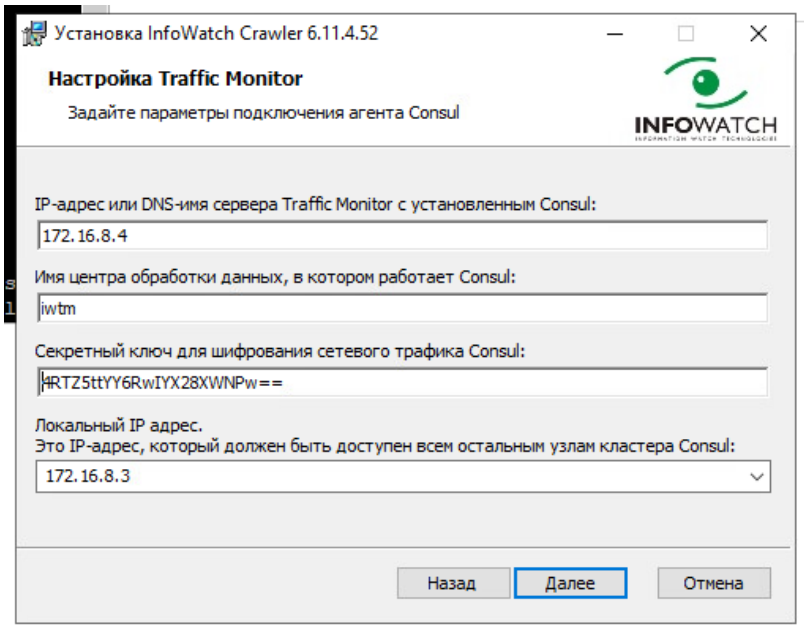

Рисунок 27 - Параметры подключения агента Consul

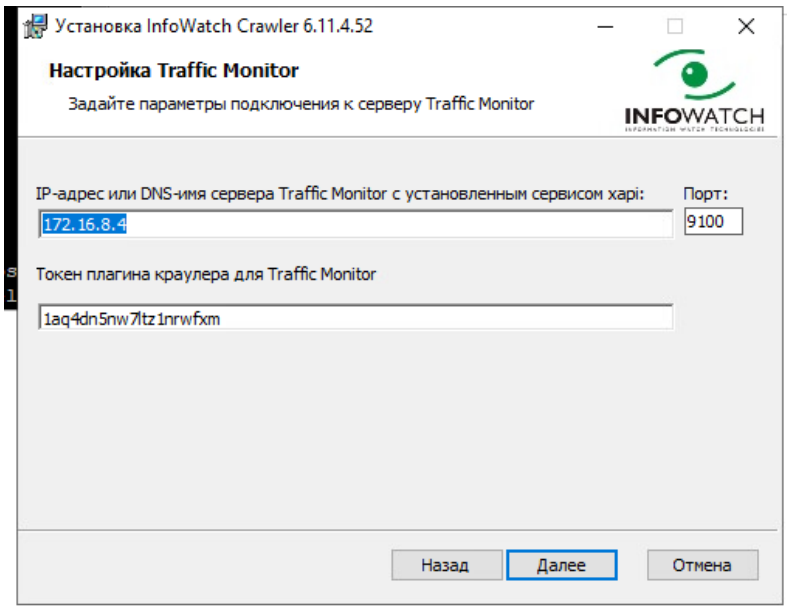

Рисунок 28 – Параметры подключения к серверу Traffic Monitor

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

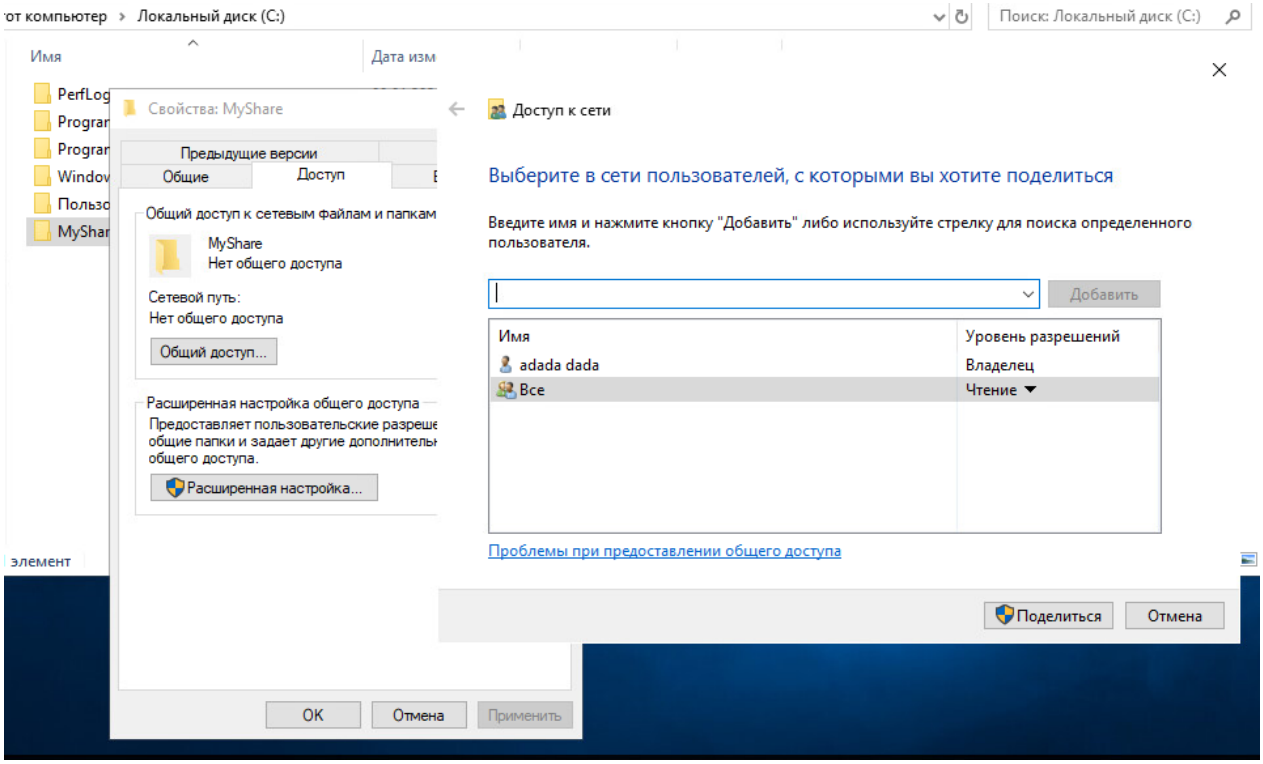

Рисунок 29 – Создание папки и распространение прав

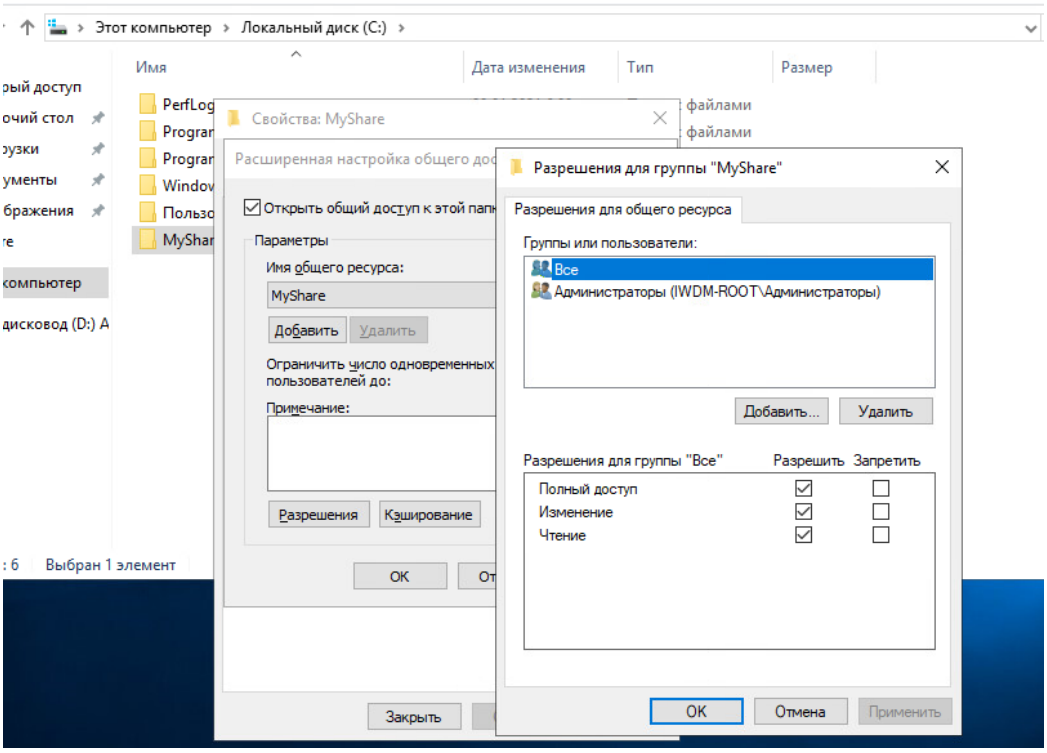

Рисунок 30 – Проверка распространения разрешений общего доступа

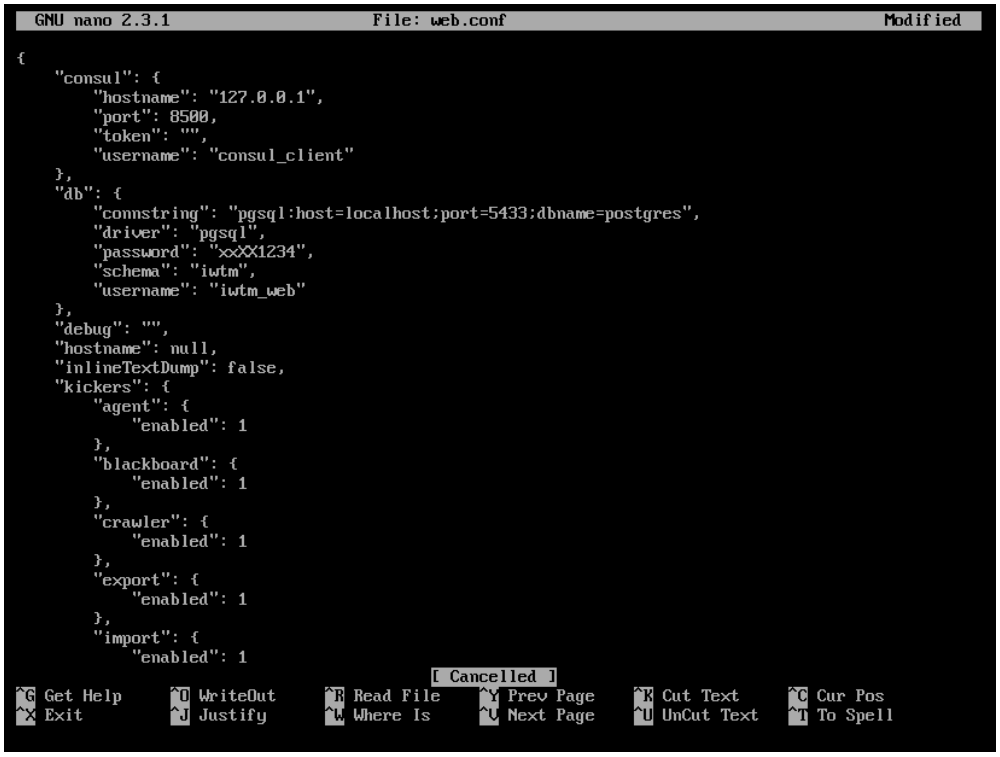

Рисунок 31 – Активация динамического обновления веб-консоли iwtm

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

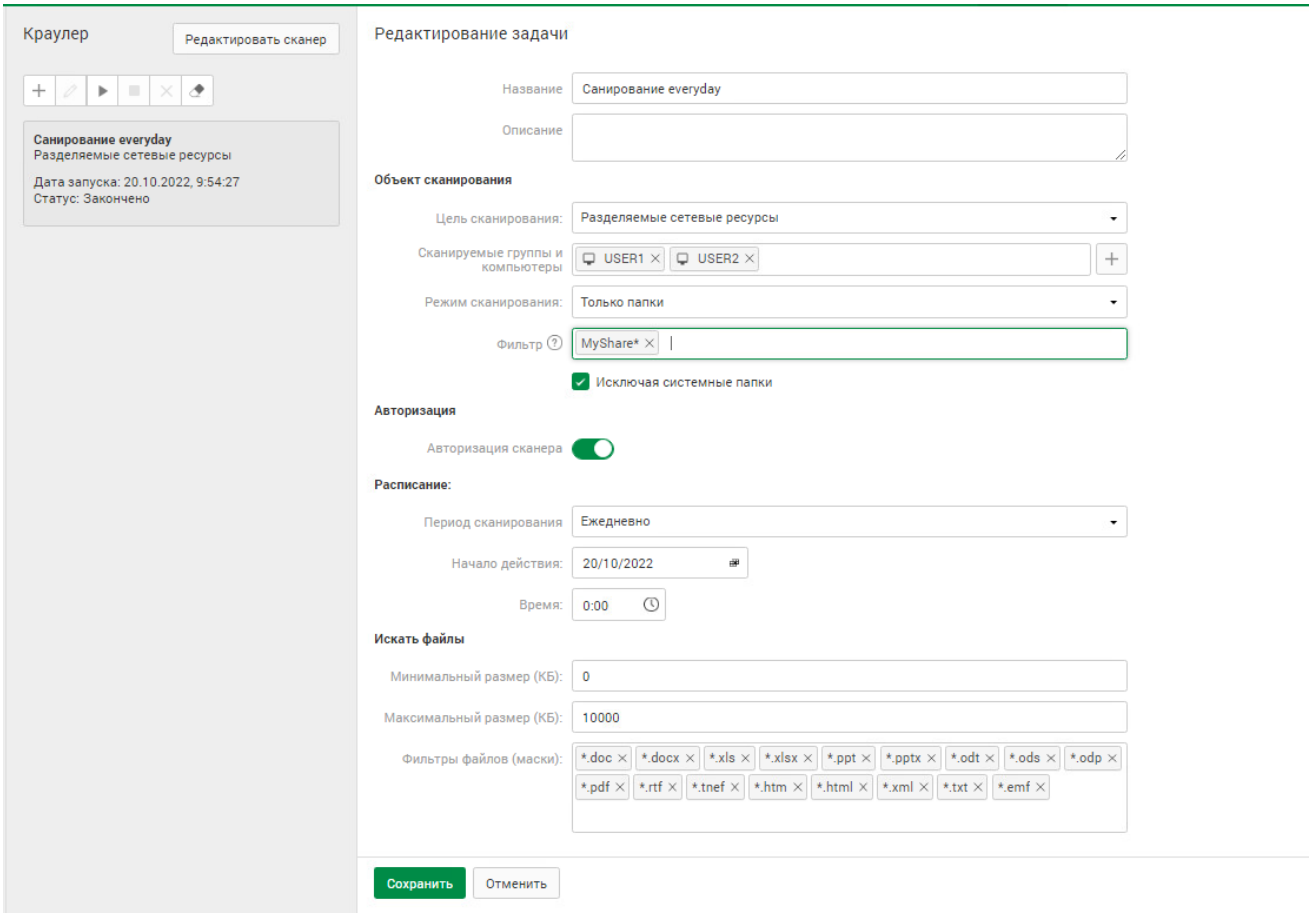

Рисунок 32 – Настройки создаваемой задачи

Зафиксировать выполнение задания скриншотом настройки и работоспособности в WEB-консоли.

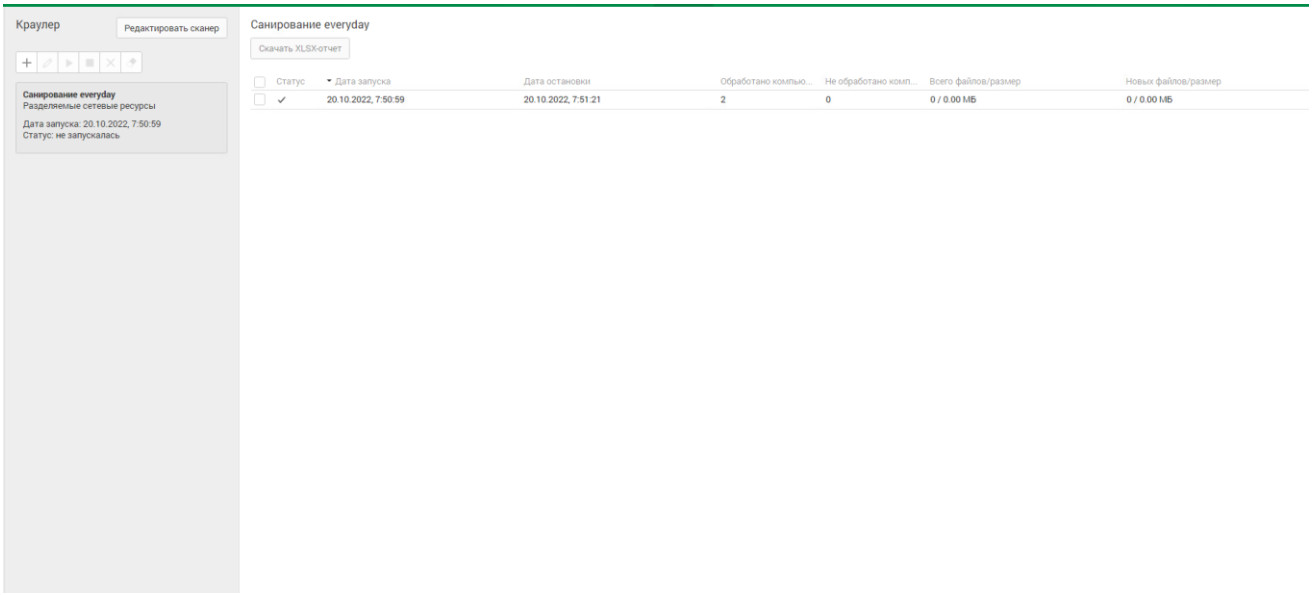

Рисунок 33 – Проверка работоспособности задачи сканирования

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих термин «Демо экзамен» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «ДЭ».

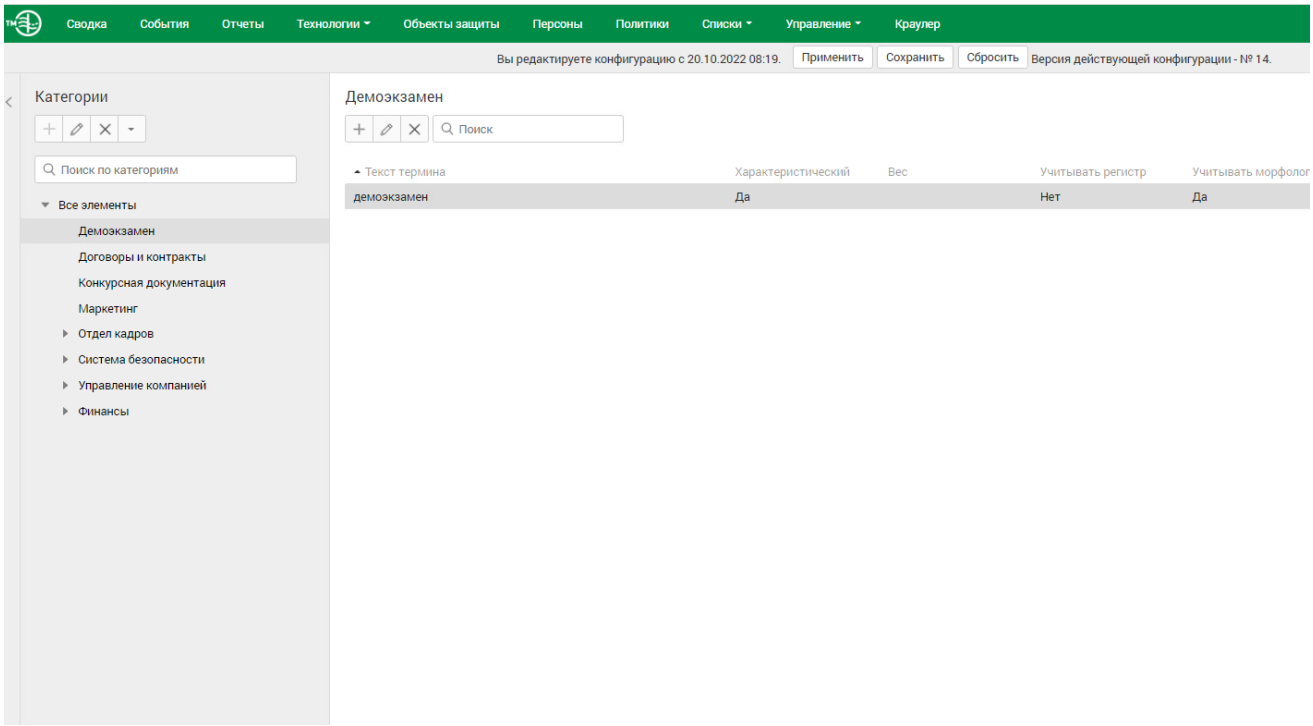

Рисунок 34 – Создание термина

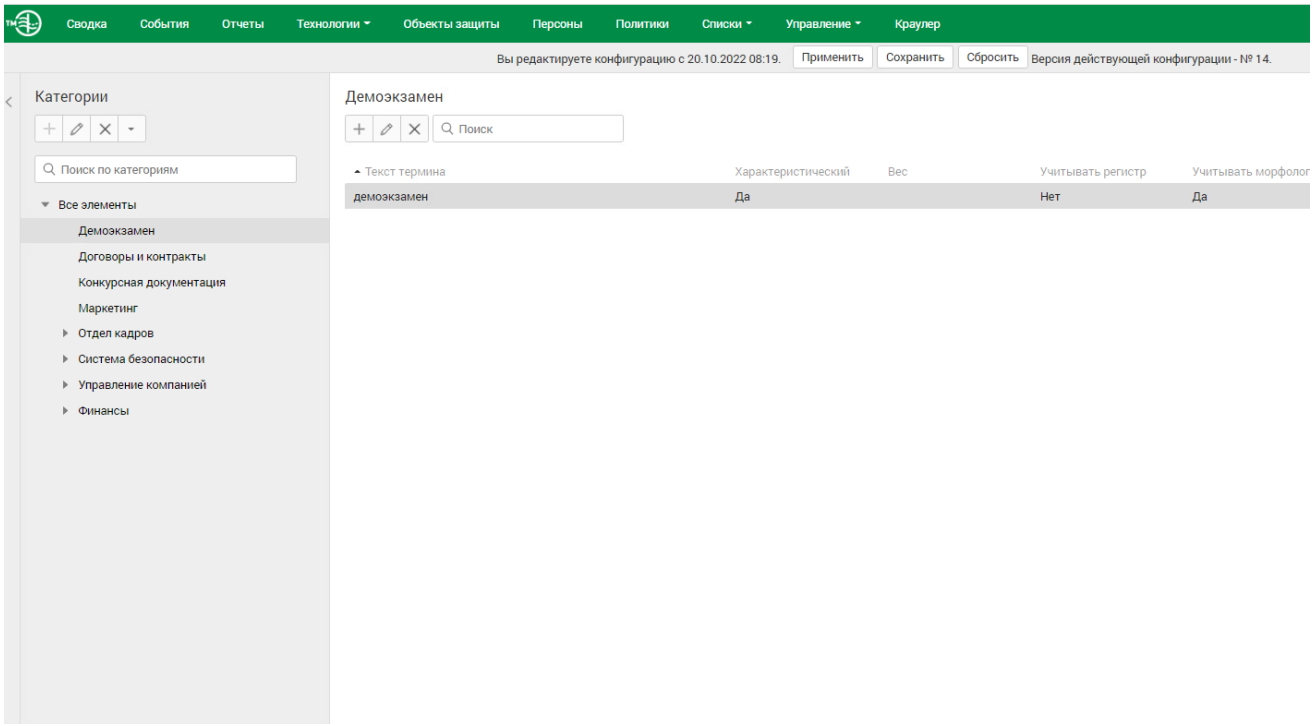

Рисунок 35 – Создание объекта защиты

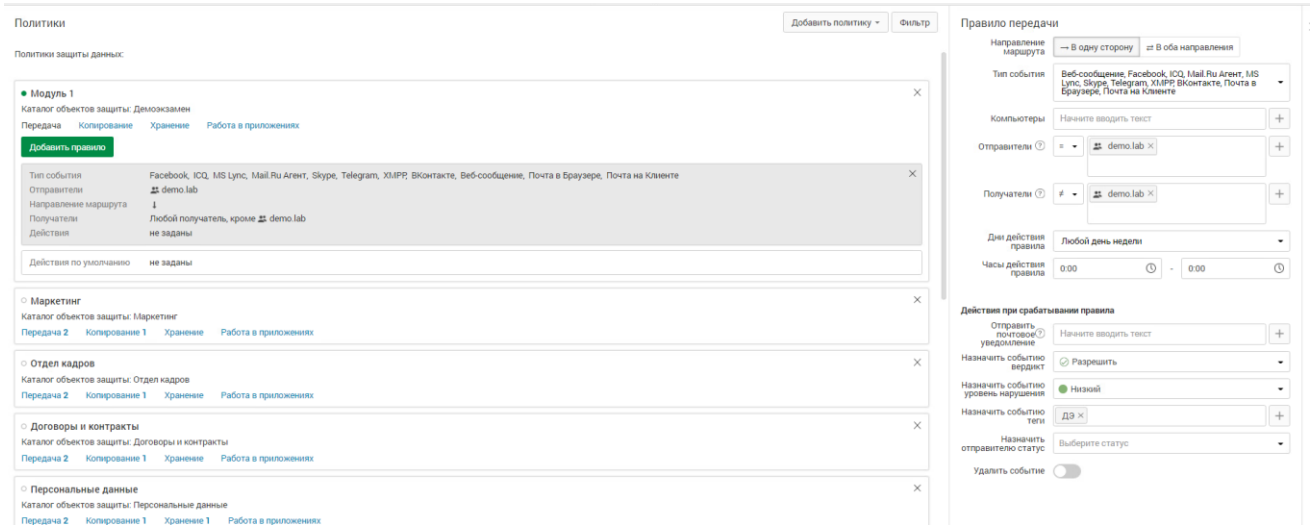

Рисунок 36 – Настройки правила передачи

По такому же принципу (рисунок 36) сделал правила для остальных действий с файлами (копирование, хранение, работа в приложении)

Для отработки правил через сервер агентского мониторинга необходимо создавать правила в отдельной политике «Модуль 1». После отработки политик необходимо оставить политику и открепить ее от групп компьютеров или выключить правила, но не удалять.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

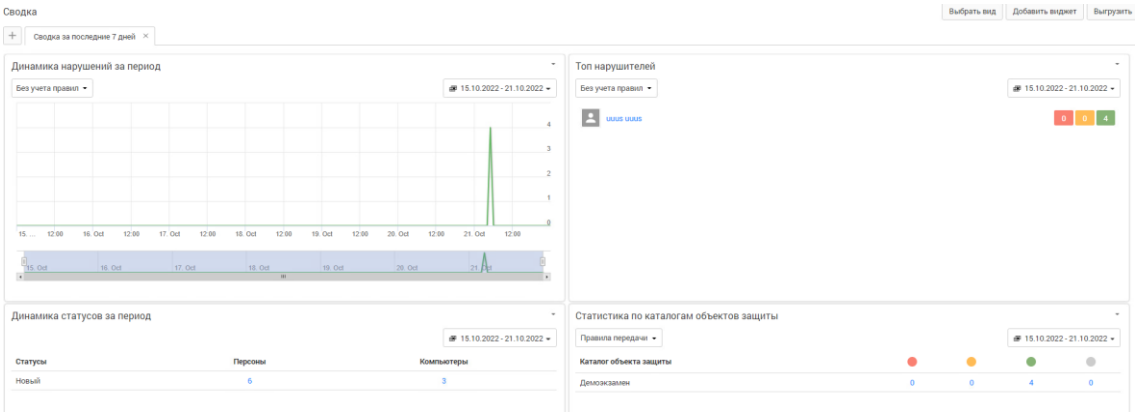

Рисунок 37 – Отображение нарушения правила передачи

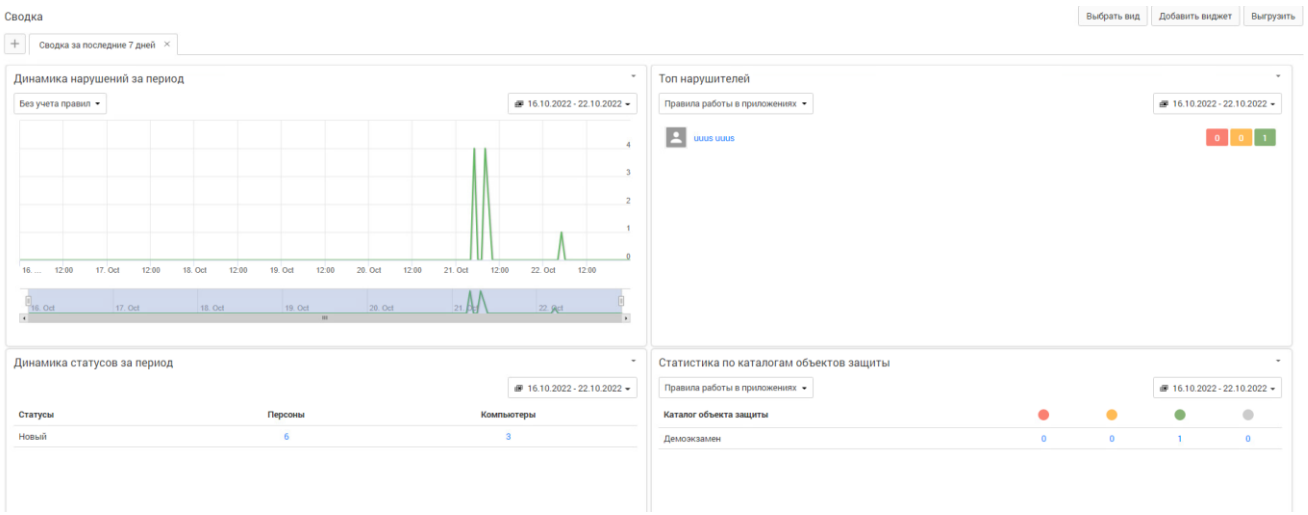

Рисунок 38 – Отображение нарушения правила буфера обмена

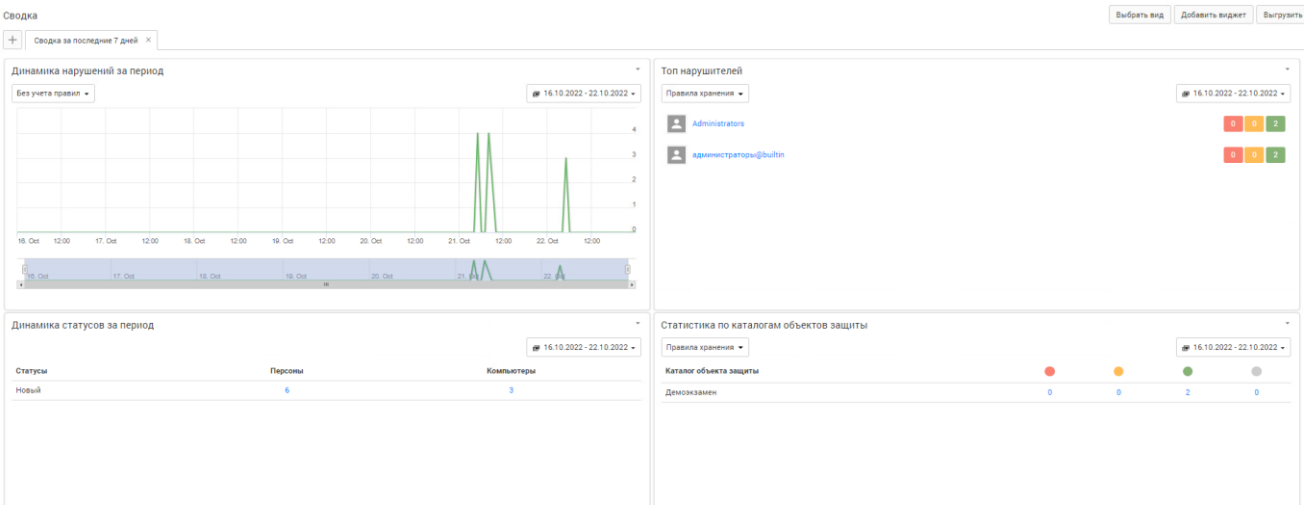

Рисунок 39 – Отображение нарушения правила хранения

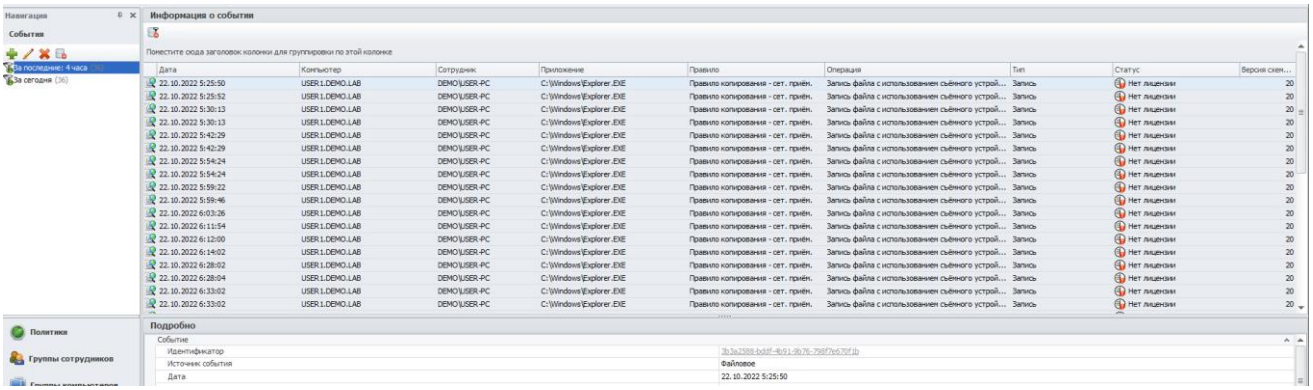

Рисунок 40 – Отображение нарушения правила копирования

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена), настроив конструктор выборки вручную.
Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

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

Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата

Дополнительная информация сертификатов должна включать в себя:

- Страна: RU
- Город: StPetersburg
- Компания (и иные дополнительные поля): demolab
- Отдел: Admins
- Почтовый адрес: из домена demo.lab
- Пароли ключей (если применимо): xxXX2233

Остальные поля заполняются самостоятельно.
После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корнФевой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли IWTM.
В случае невозможности это сделать, установить сертификат на машину домена и отобразить это в отчете.

Перед началом создания сертификатов, я установил на доменный компьютер центр сертификации и настроил его (это нужно для указания центра сертификации, при создании сертификатов).

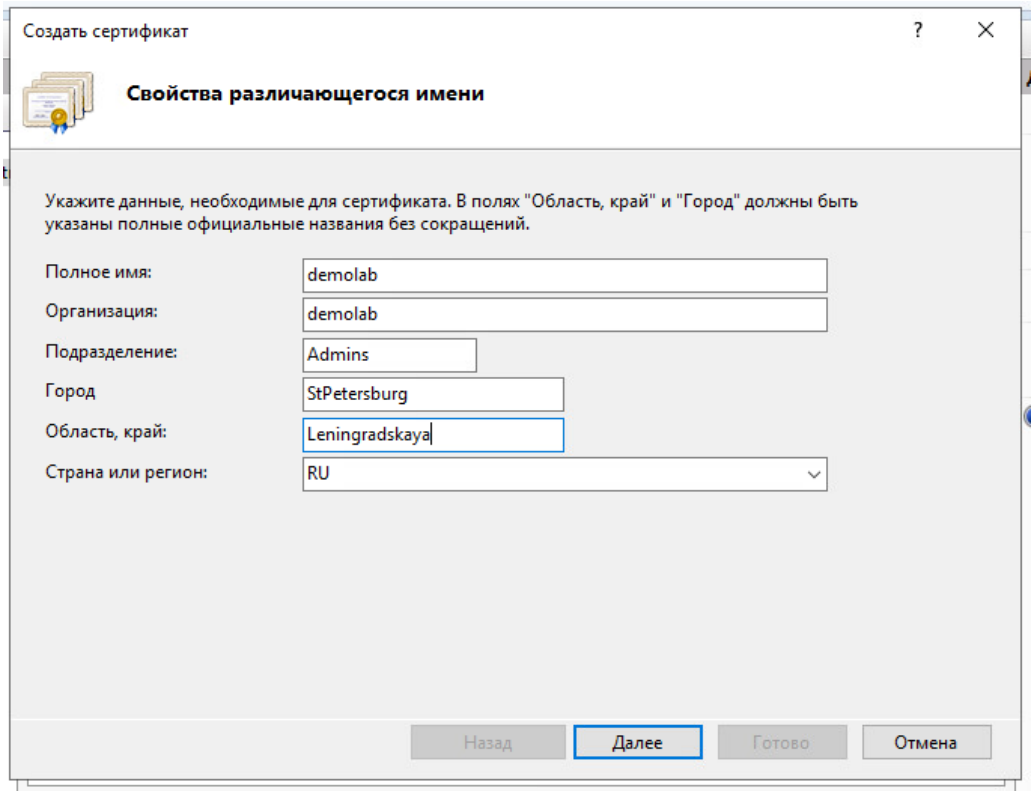

Рисунок 41 – Создание доменного сертификата

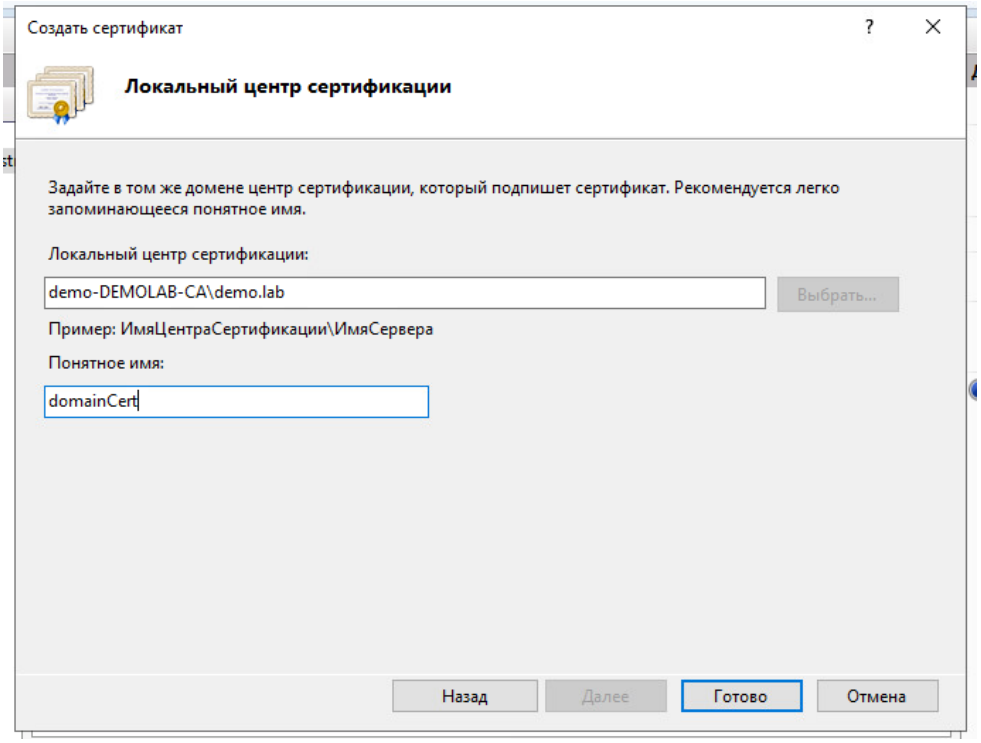

Рисунок 42 – Локальный сертификат при создании доменного сертификата

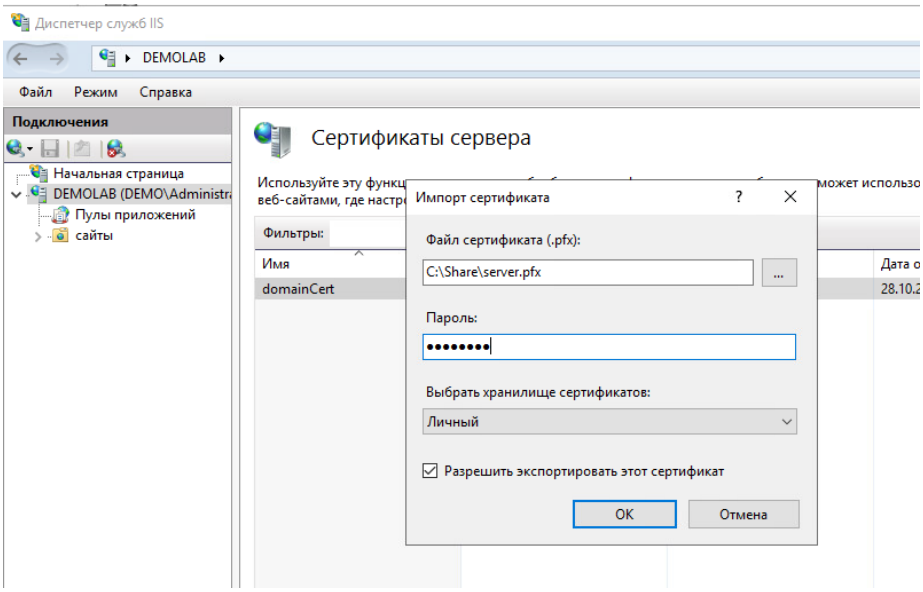

Рисунок 43 – Импорт сертификата на сертификат формата pksc

```
[root@iwtm cert]# openssl req -newkey rsa:2048 -nodes -keyout domain.key -out domain.csr
Generating a 2048 bit RSA private key
.....................................................................................+++
............+++
writing new private key to 'domain.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Leningradskaya
Locality Name (eg, city) [Default City]:StPetersburg
Organization Name (eg, company) [Default Company Ltd]:demolab
Organizational Unit Name (eg, section) []:Admins
Common Name (eg, your name or your server's hostname) []:demolab
Email Address []:demolab@mail.ru

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:xxXX2233
An optional company name []:demolab
[root@iwtm cert]# _
```

Рисунок 44 – Создание закрытого ключа и запроса на подпись

```
An optional company name []:demolab
[root@iwtm cert]# openssl x509 -signkey domain.key -in domain.csr -req -days 365 -out domain.crt
Signature ok
subject=/C=RU/ST=Leningradskaya/L=StPetersburg/O=demolab/OU=Admins/CN=demolab/emailAddress=demolab@m
ail.ru
Getting Private key
[root@iwtm cert]#
```

Рисунок 45 – Подпись сертификата своим созданным ключом