ДЕПАРТАМЕНТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ТОМСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«ТОМСКИЙ ТЕХНИКУМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Примерное задание на комплексный квалификационный экзамен по профессиональным модулям специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

(Квалификация – Техник по защите информации)

Томск 2022

# **ОБЩИЕ ПОЛОЖЕНИЯ**

В качестве итоговой аттестации по каждому профессиональному модулю после завершения обучения проводится экзамен (квалификационный), на котором представители учебного заведения и работодателей проверяют готовность обучающегося к выполнению соответствующего вида профессиональной деятельности и сформированность у него профессиональных (ПК) и общих компетенций (ОК).

Экзамен (квалификационный) проводится после изучения всех МДК модуля, прохождения учебной и производственной практики.

Для проведения процедуры квалификационного экзамена создается экзаменационная комиссия, в которую входят представители образовательного учреждения (преподаватели, представители администрации) и представители работодателей.

Экзамен (квалификационный) проводится в соответствии с графиком экзаменов и на основании приказа директора образовательного учреждения.

# **ПРИМЕРНОЕ ЗАДАНИЕ**

## Содержание практического задания по модулям:

Модуль 1: Установка и конфигурирование компонентов DLP системы.

Модуль 2: Технологии агентского мониторинга.

Продолжительность экзамена 180 минут.

## Описание задания:

В компании «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации. Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием. Основными каналами потенциальной утечки данных являются электронная почта и различные интернет-ресурсы, если не указано иное.

Политики трафика могут быть проверены вручную или с помощью генератора событий, предоставляемым по запросу.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены (кроме адреса DNS сервера на машинах).

Подготовлены следующие виртуальные машины для работы (рекомендуется сделать нулевой Snapshot), сеть настроена в режиме NAT, с доступом в интернет, но без доступа к машинам других участников экзамена:

* Demo.lab. AD и DNS сервер (контроллер домена), 1,5ГБ ОЗУ, 2 ядра, статическая адресация с доступом в интернет,
* IWTM. DLP сервер установлен (но не настроен), активирована лицензия, 8ГБ ОЗУ, 2 ядра,
* IWDM. Виртуальная машина для установки сервера агентского мониторинга, 2ГБ ОЗУ, 2 ядра,
* W10-Agent. Виртуальные машина «нарушителя», 1,5ГБ ОЗУ, 1 ядро.

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов (demo.lab).

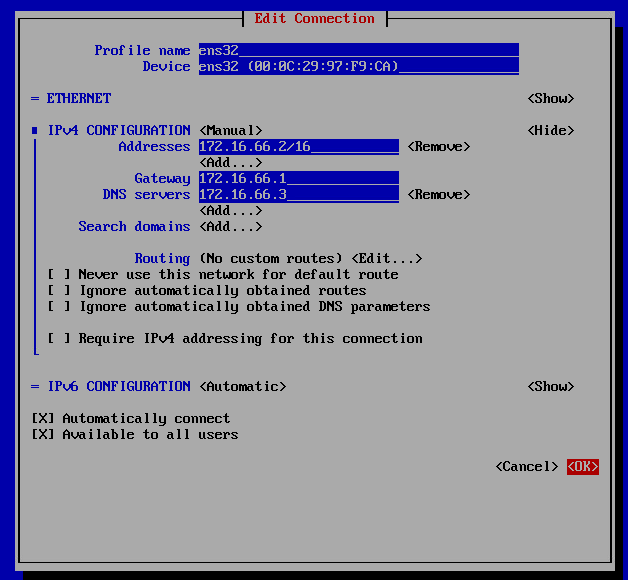
Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными. При выполнении заданий можно пользоваться разрешенными справочными ресурсами в сети Интернет и документацией на компьютерах.

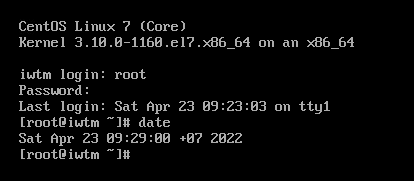
Все дистрибутивы находятся в каталоге, указанном в карточке задания. Все логины, пароли, сетевые настройки и прочее, относящееся к инфраструктуре площадки, указаны в карточке задания.

При создании снимков экрана необходимо делать либо полный снимок экрана, либо целого окна.

## Описание модуля 1:

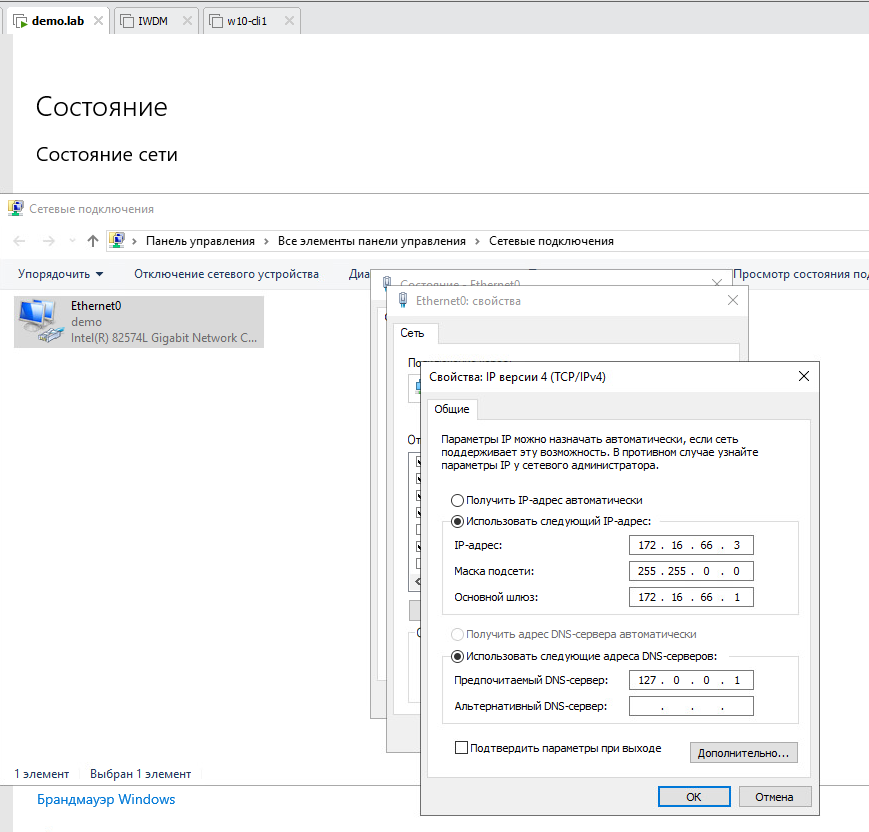
nmtui

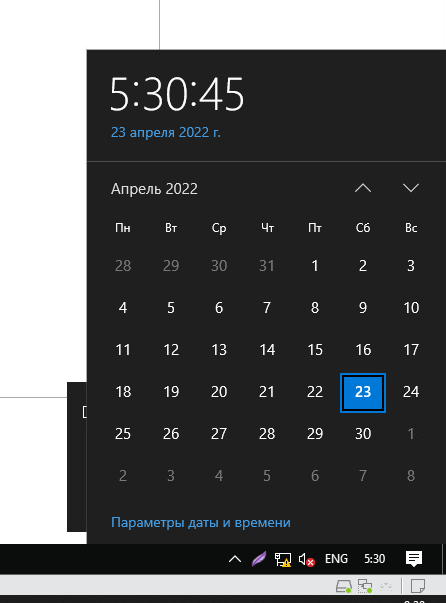


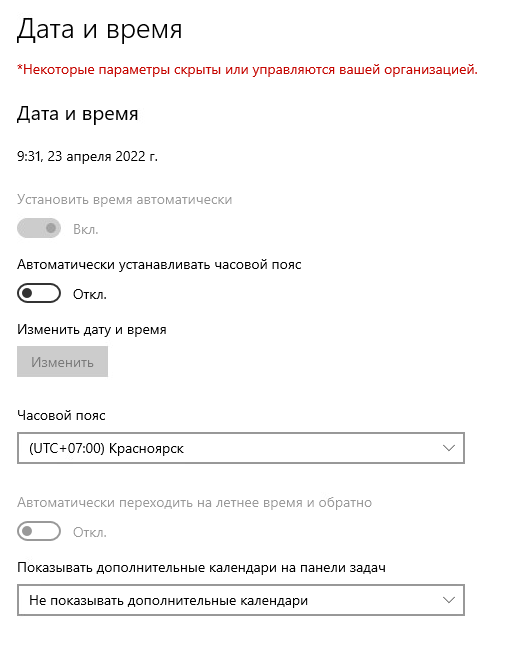


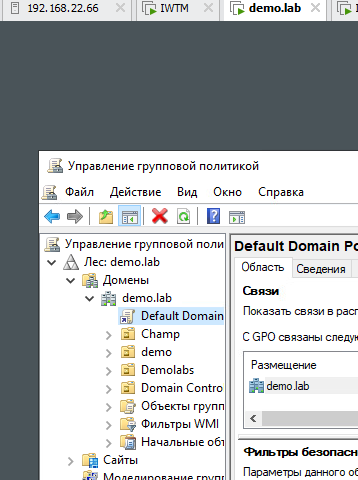
+7 часовой пояс

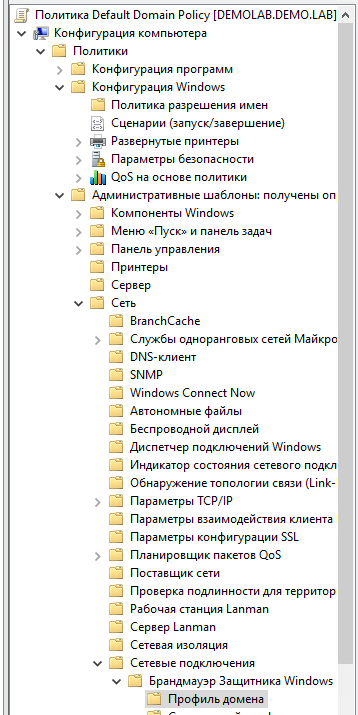
Demo.lab

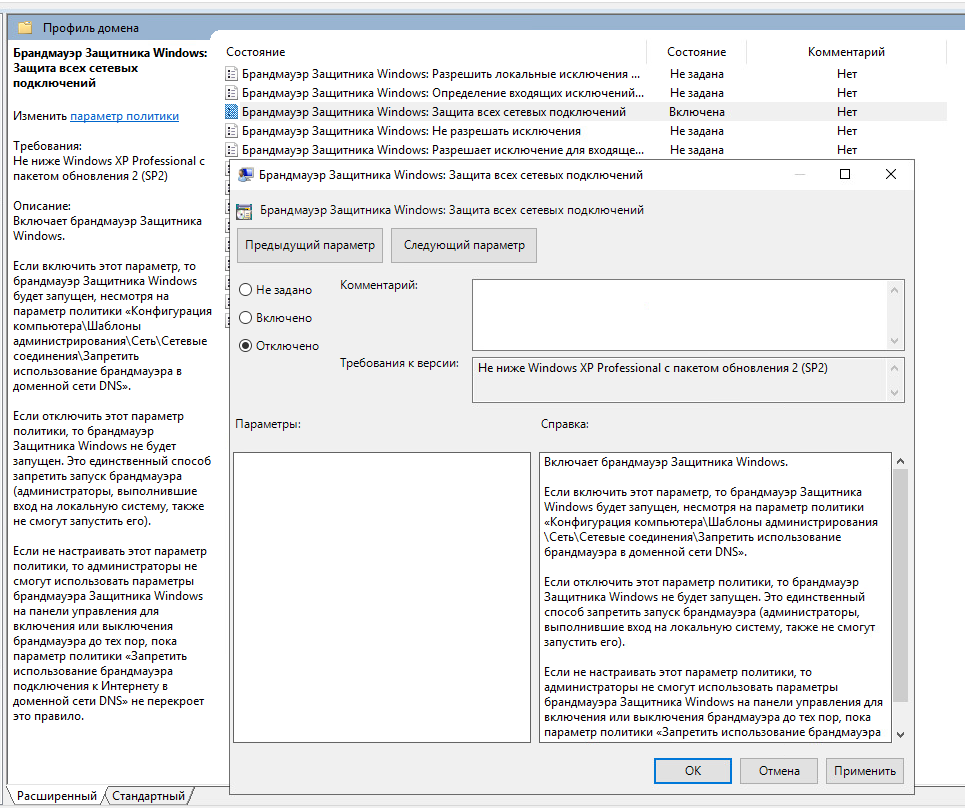


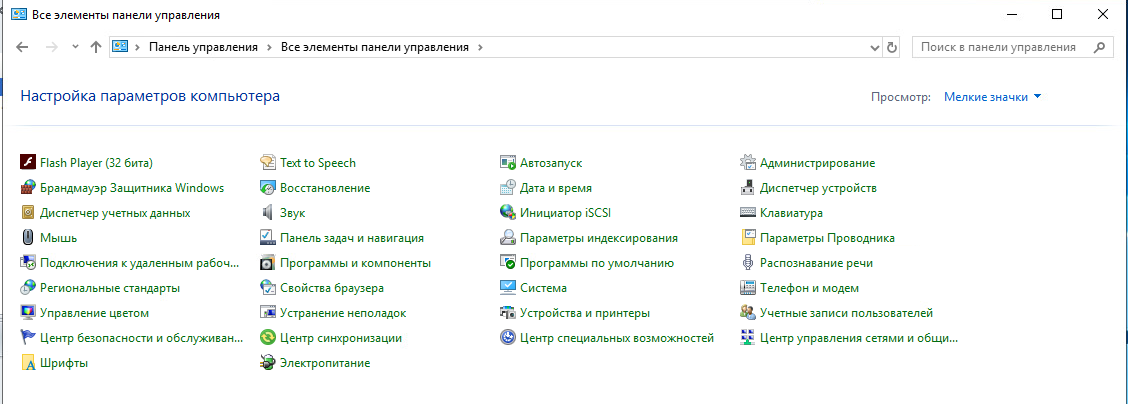


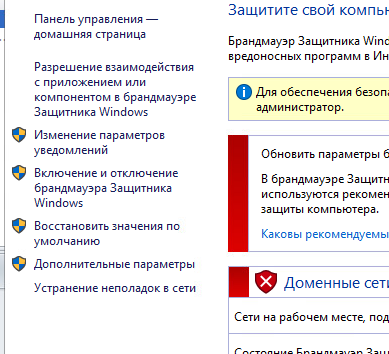


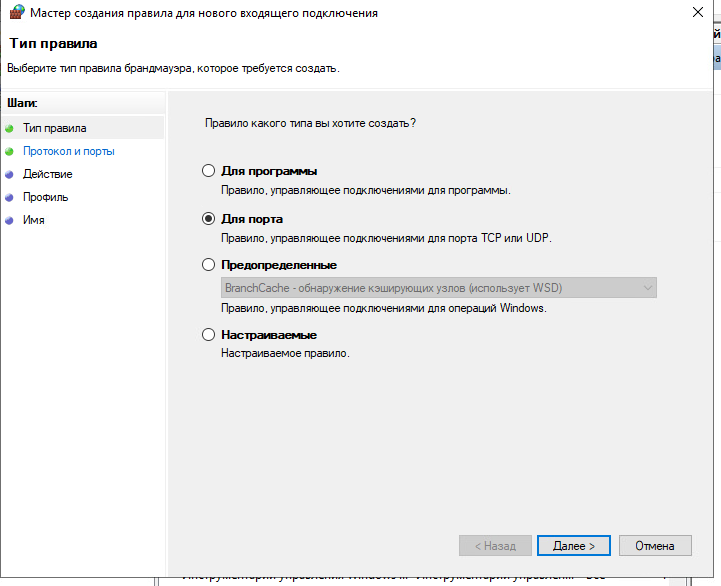


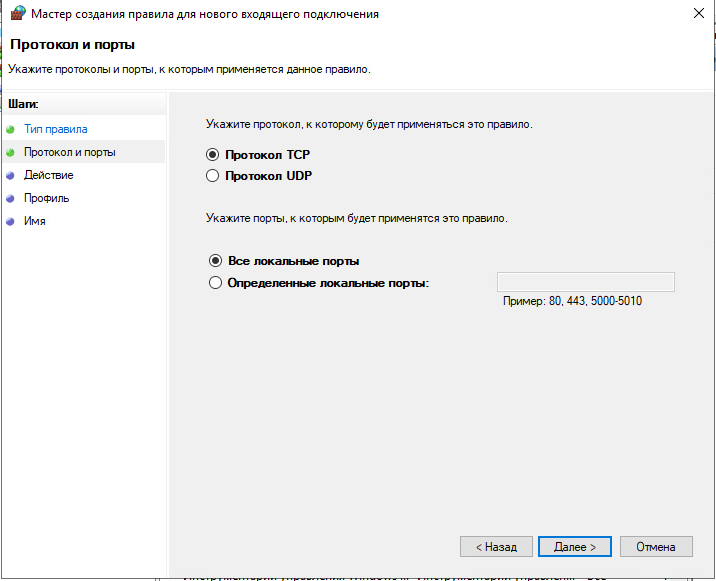


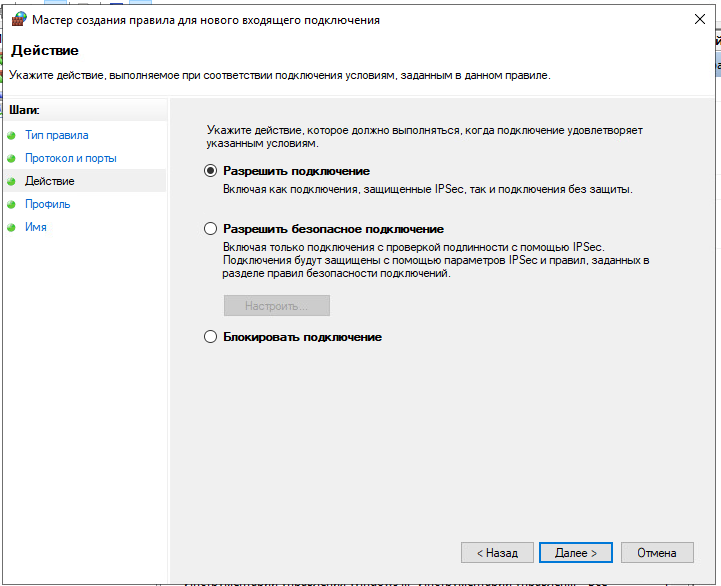


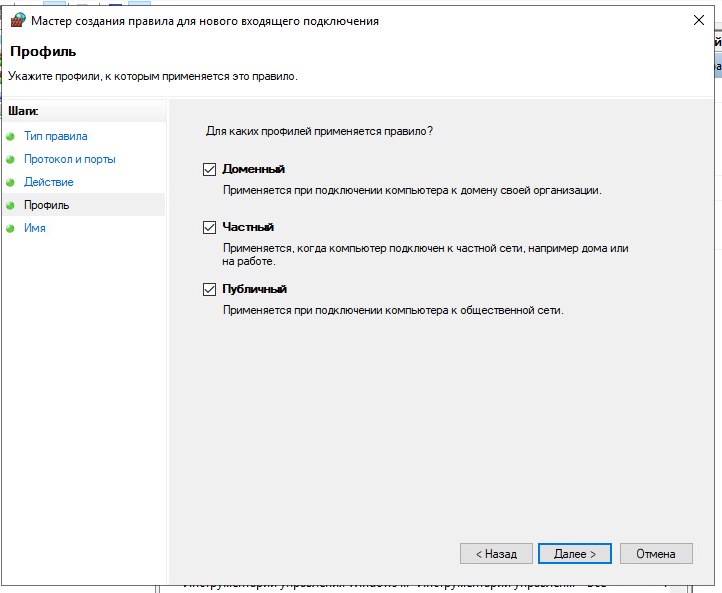


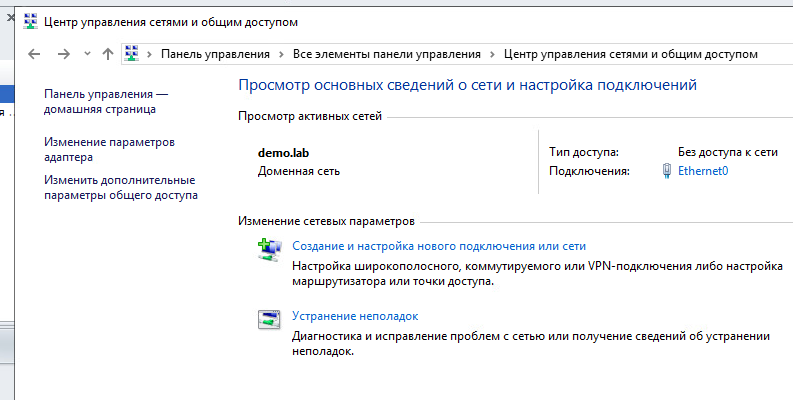


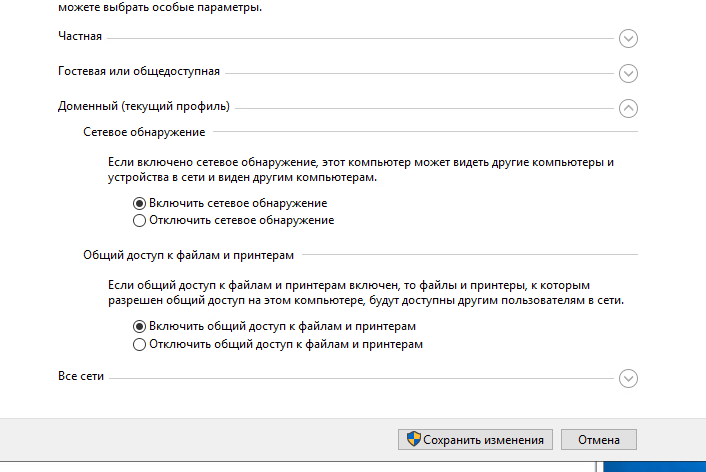


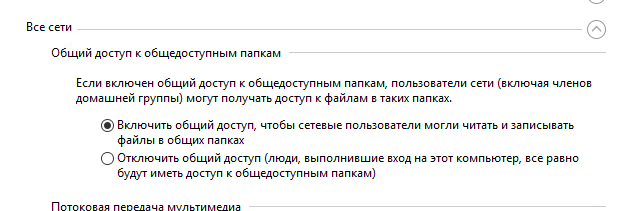






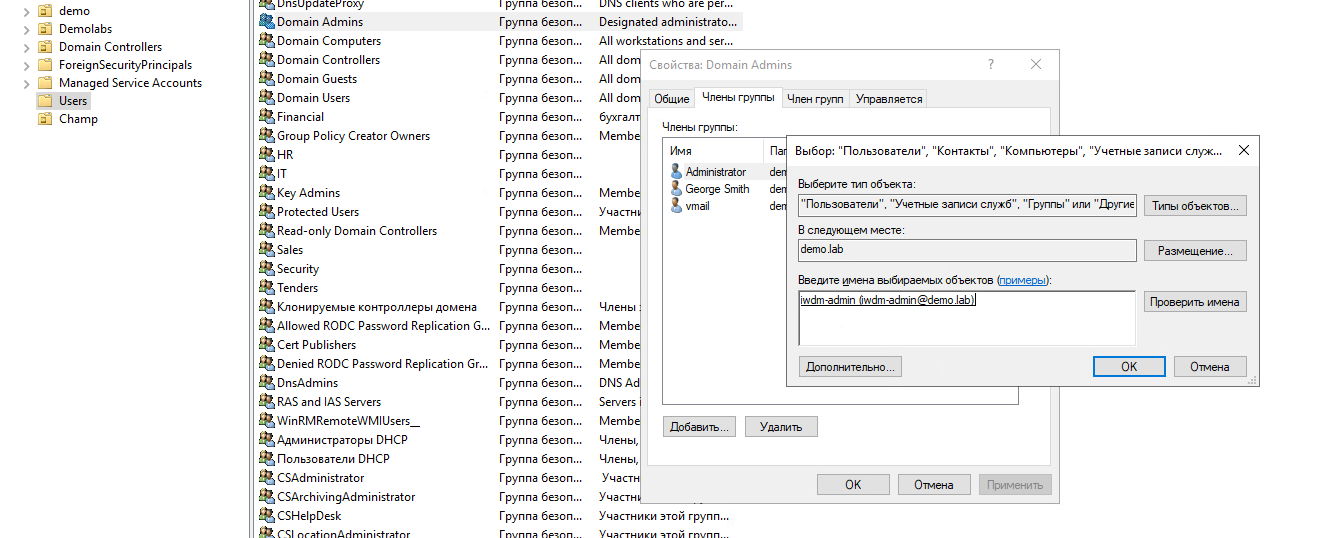
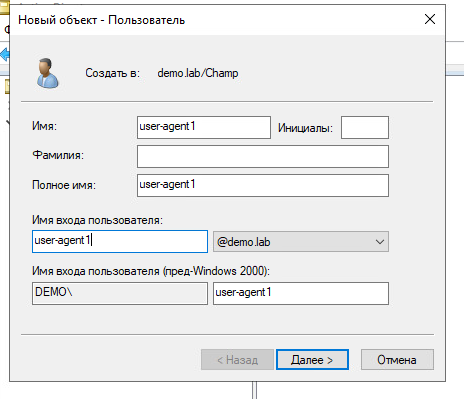
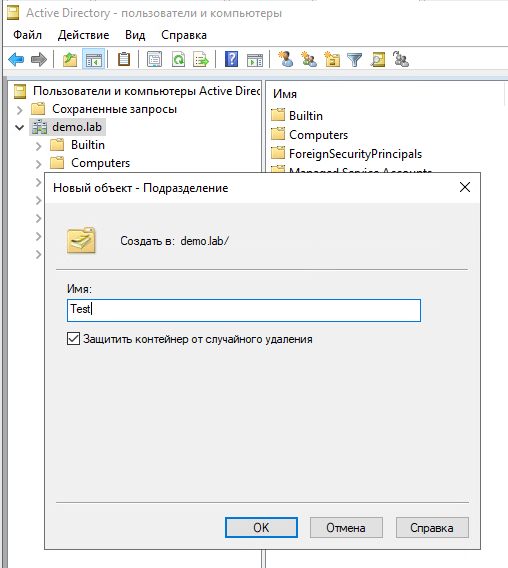






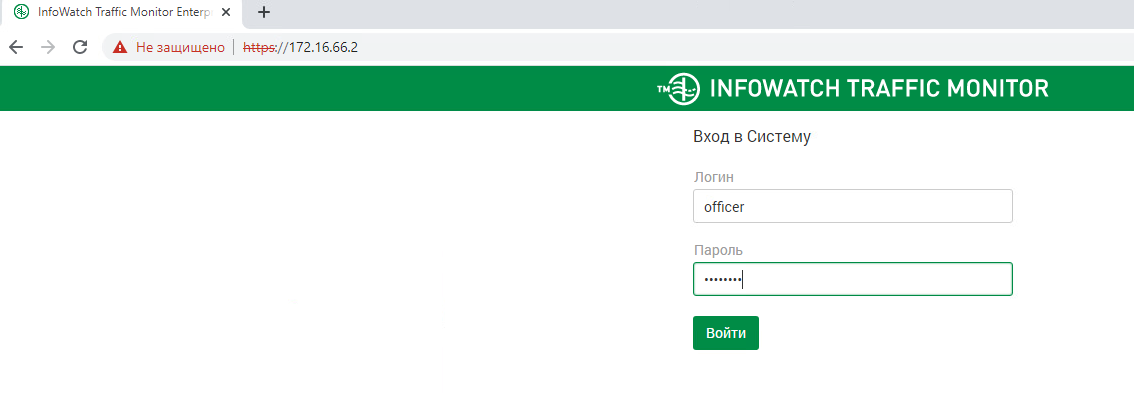
## Задание 1: Настройка контроллера домена

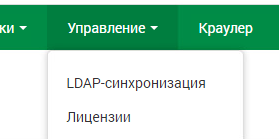
В корневом каталоге оснастки «Пользователи и компьютеры» AD сервера необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

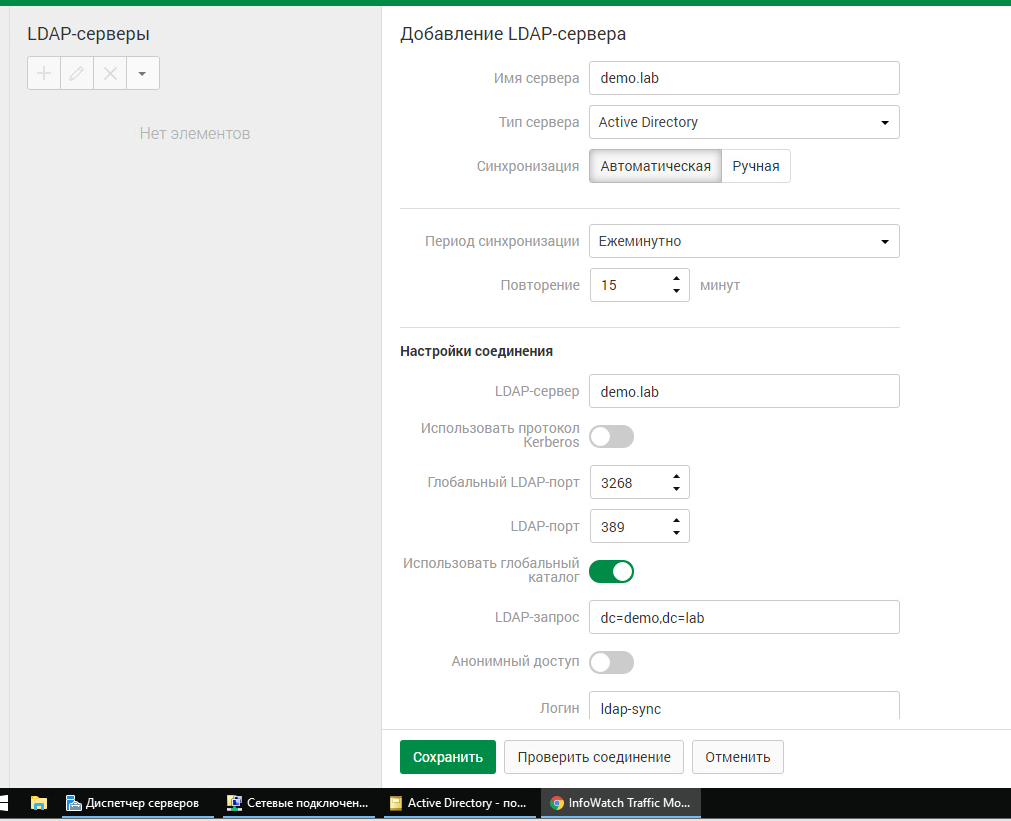


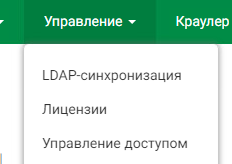
* Логин: user-one, пароль: xxXX1234, права пользователя домена
* Логин: iwdm-admin, пароль: xxXX1234, права администратора домена
* Логин: iwtm-officer, пароль: xxXX1234, права пользователя домена
* Логин: ldap-sync, пароль: xxXX1234, права пользователя домена

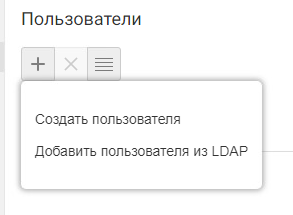
## Задание 2: Настройка DLP сервера

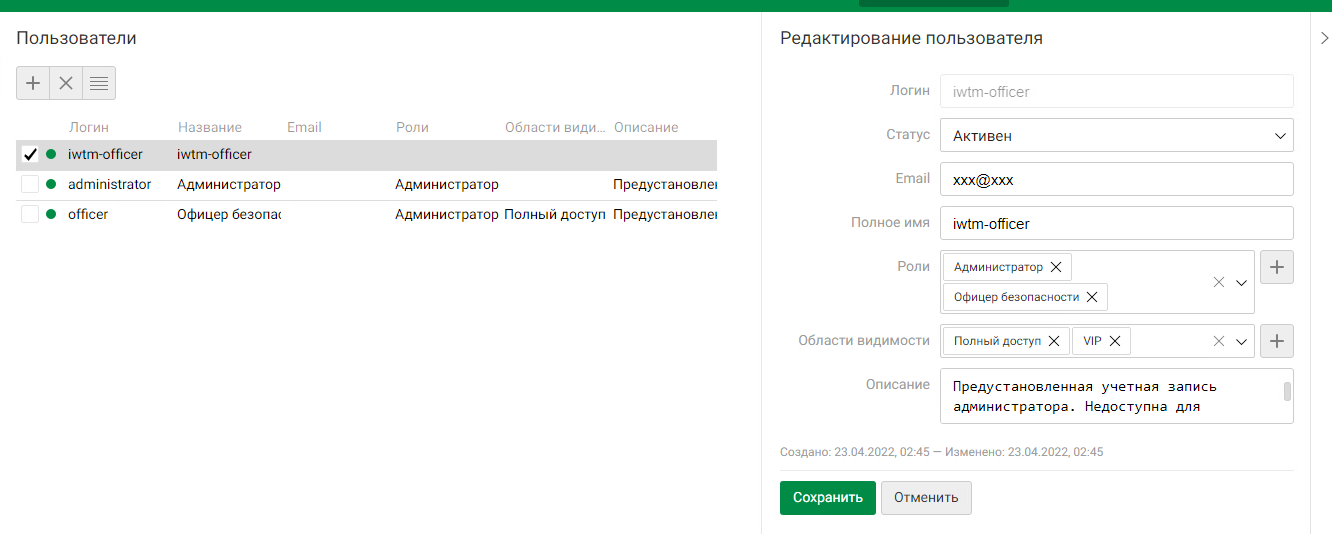
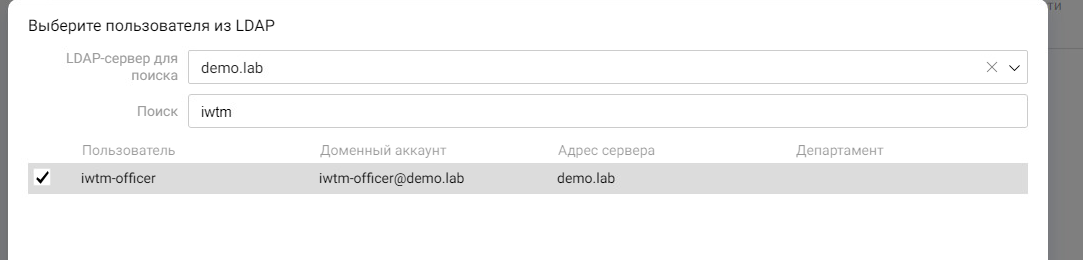












DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

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

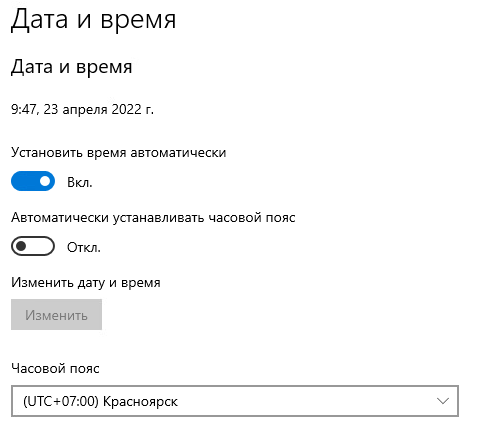
Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-officer с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

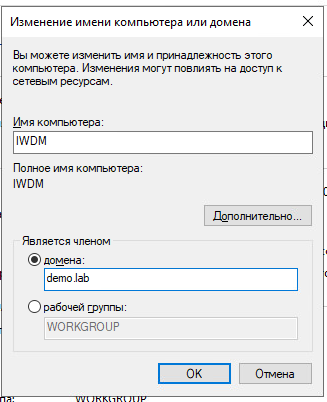
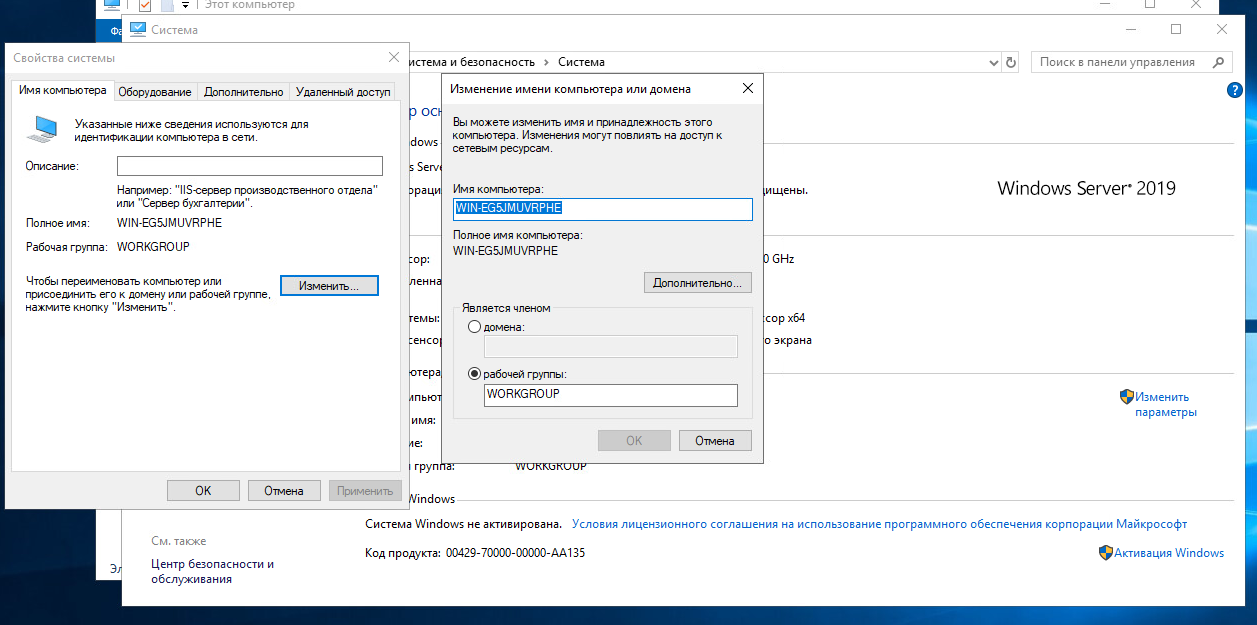
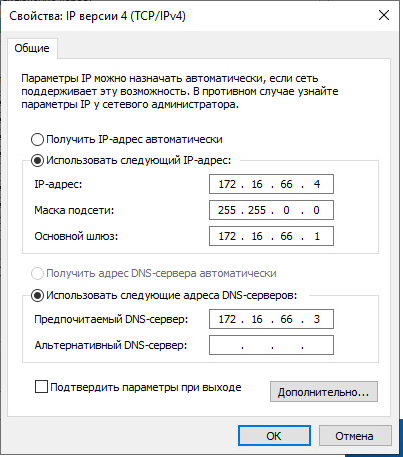
Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» на рабочем столе компьютера.

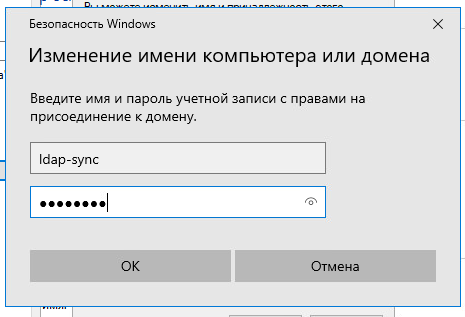
## Задание 3: Установка и настройка сервера агентского мониторинга

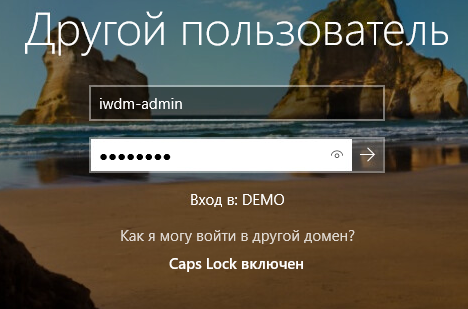
IWDM

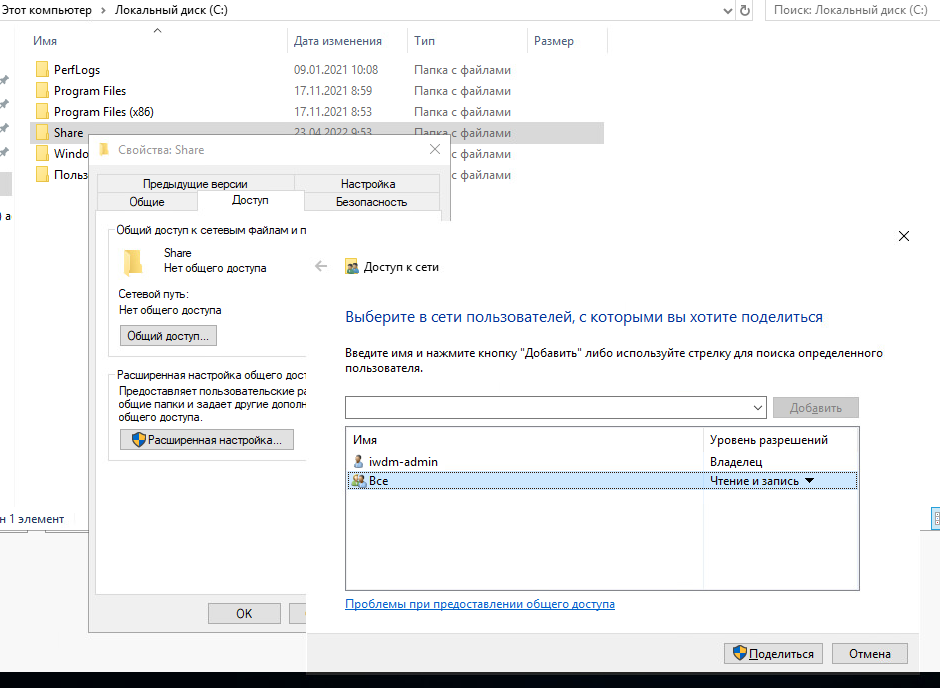
СРАЗУ ЖЕ ЧАСОВОЙ ПОЯС МЕНЯЙ!!!

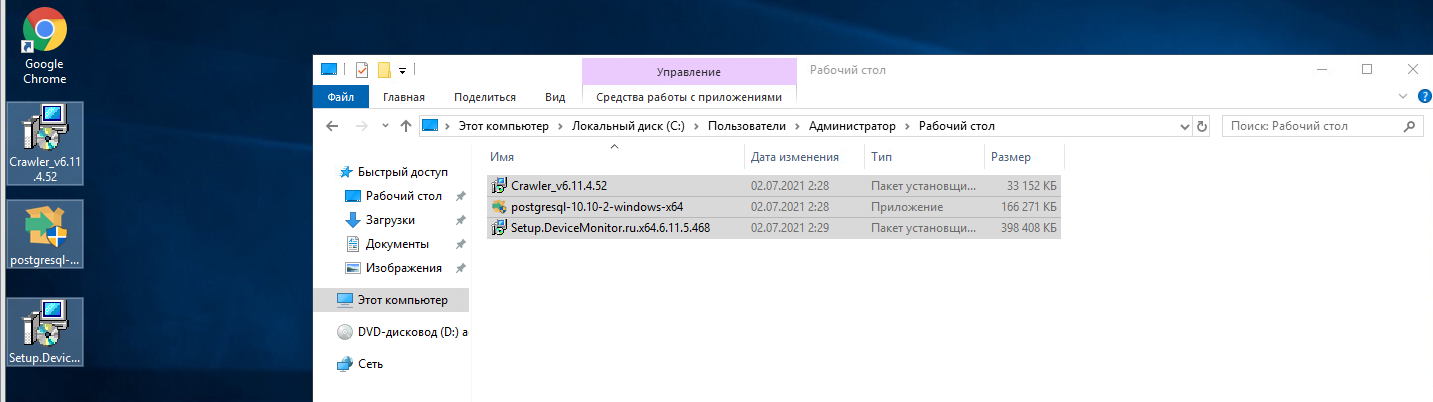




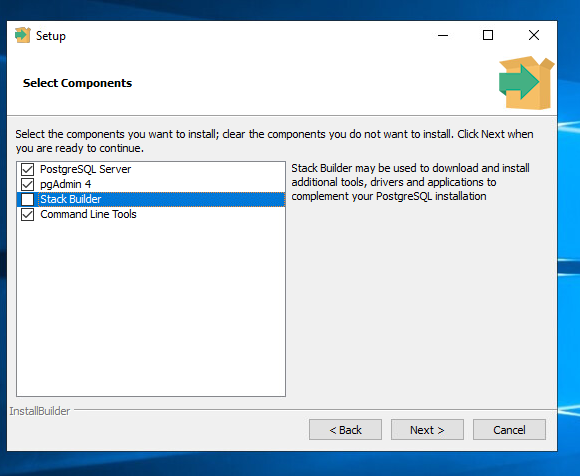


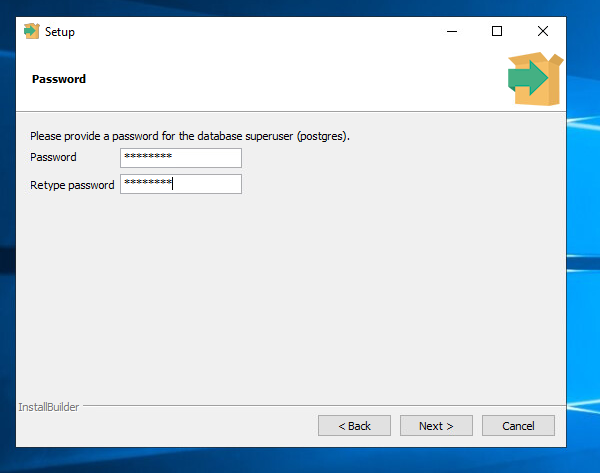


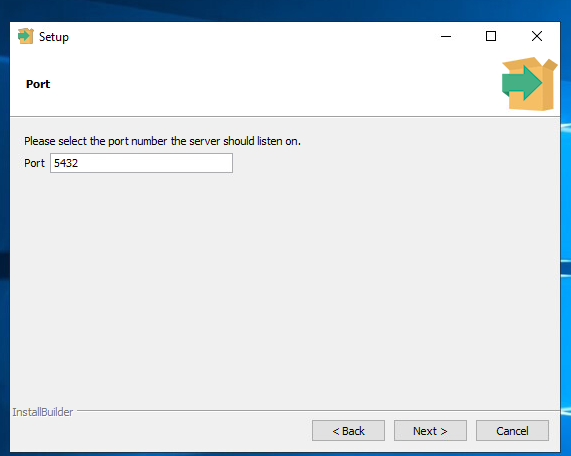


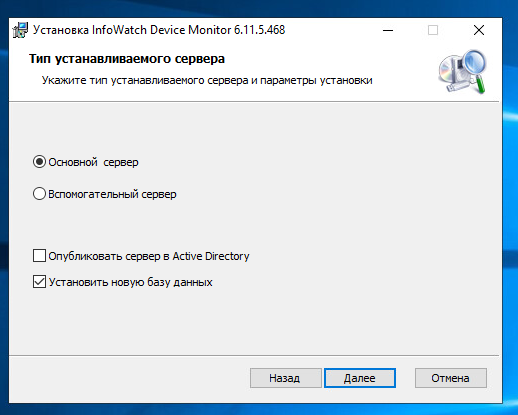


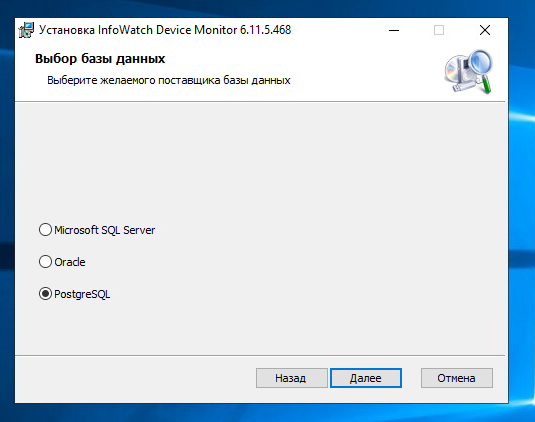
Установка Postgres

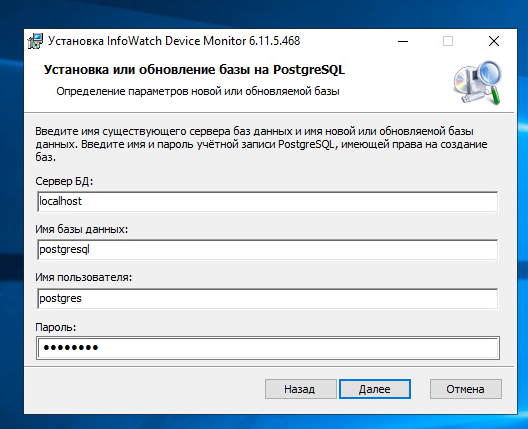


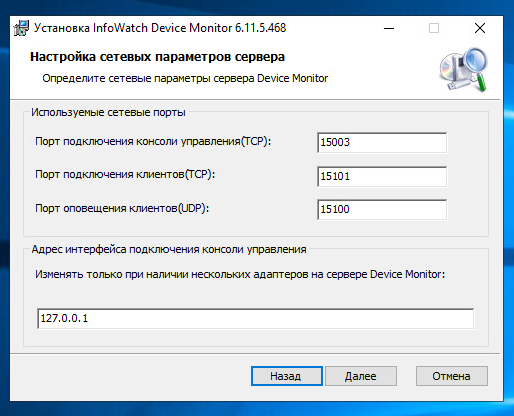


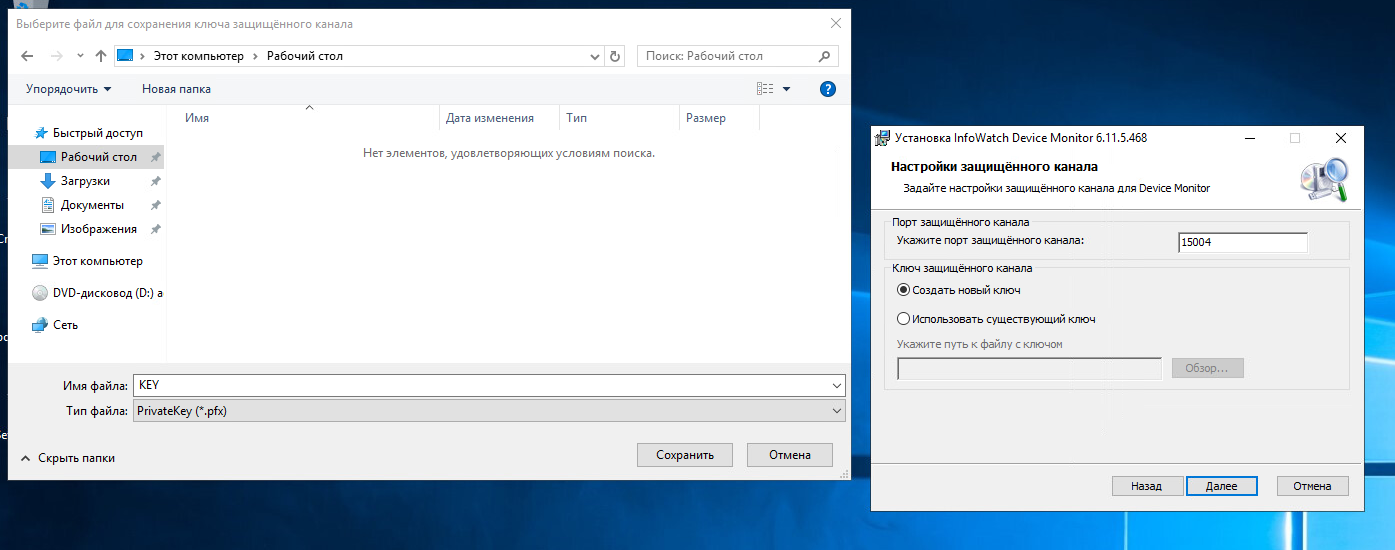


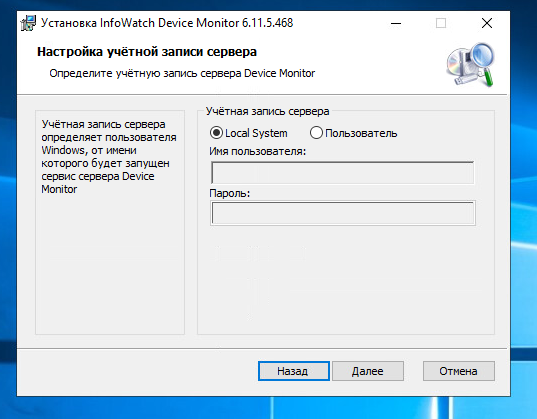


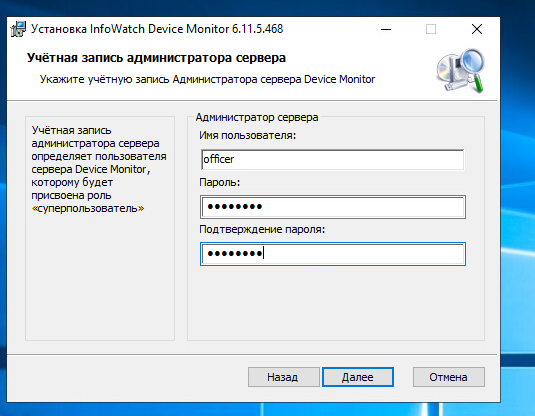


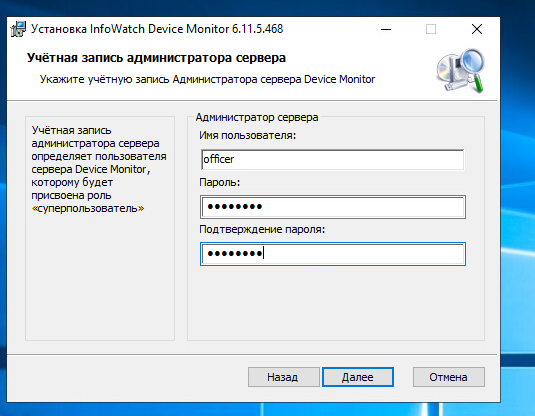


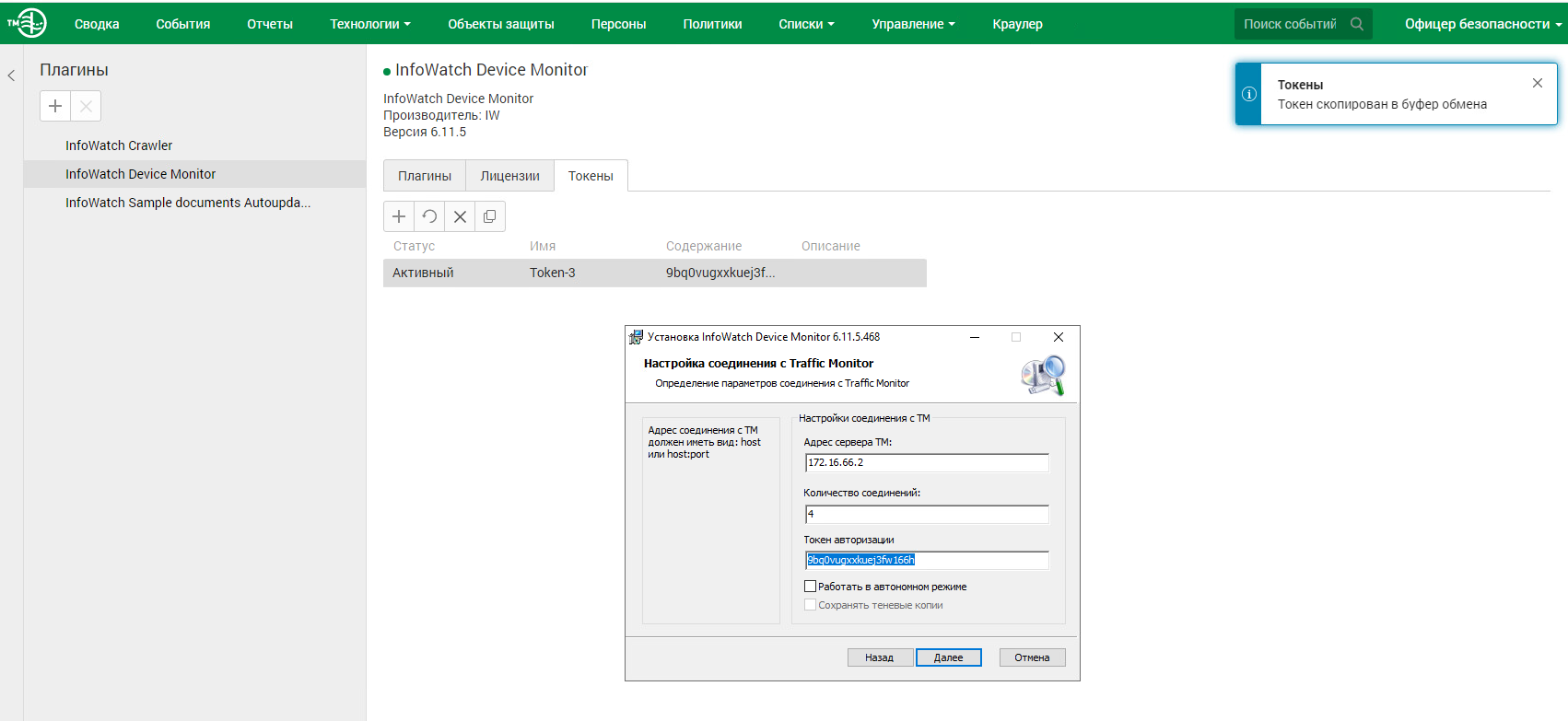


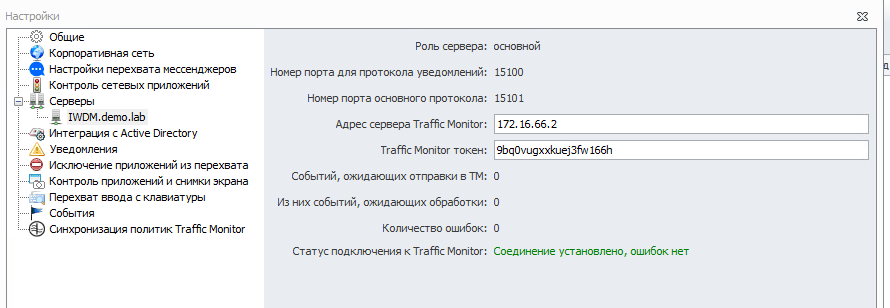




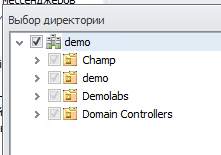


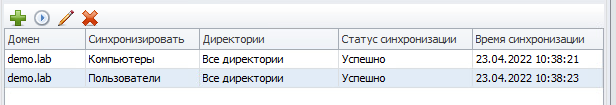


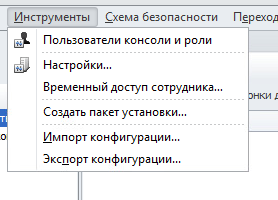


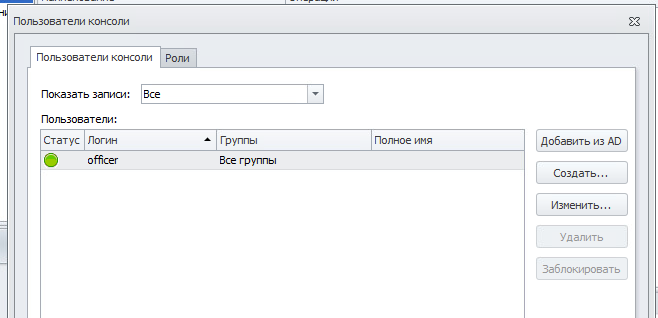


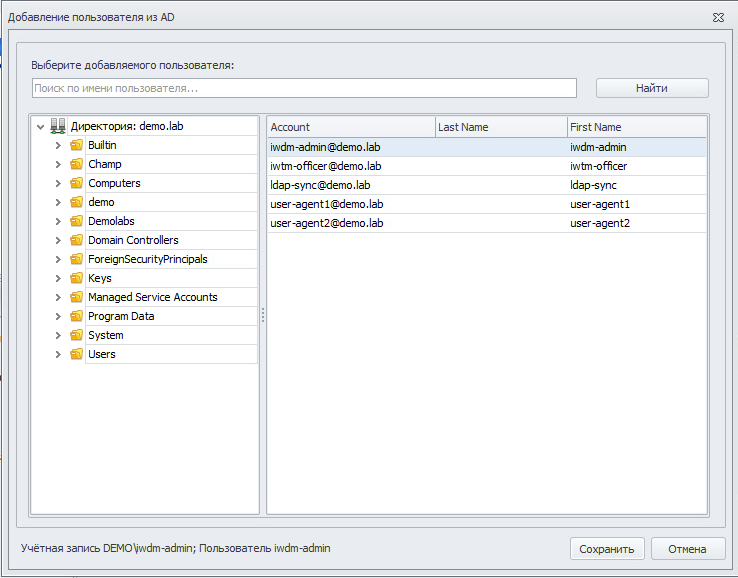


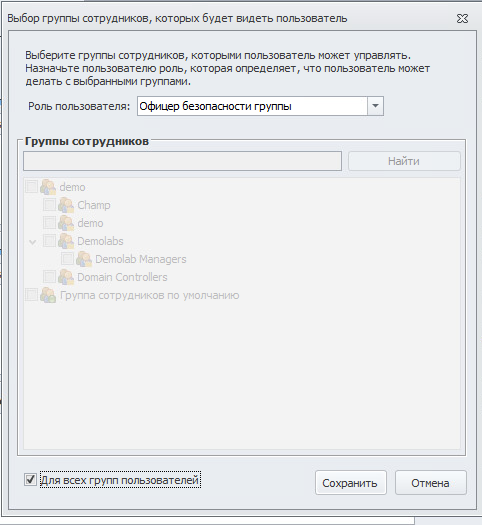


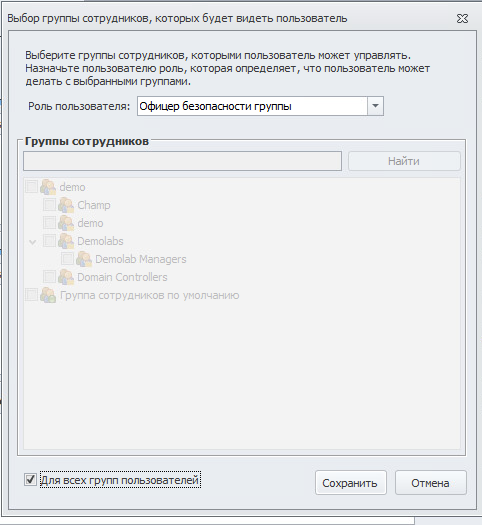


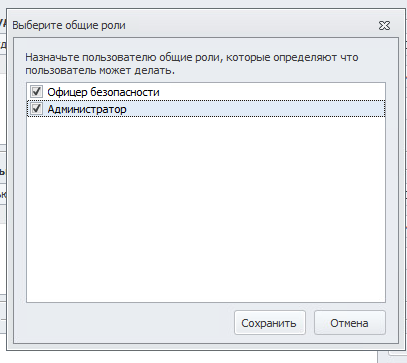


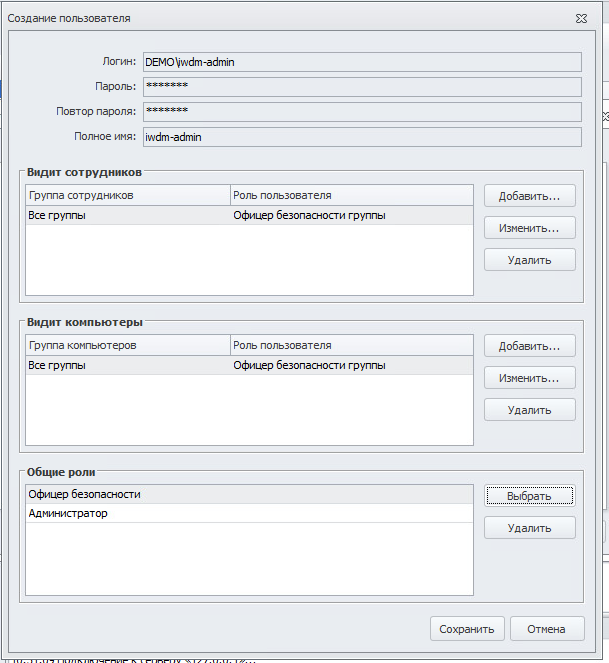


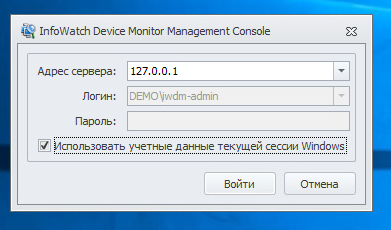












Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя iwdm-admin (важно). После входа в систему необходимо переместить введенный в домен компьютер.

Установить базу данных PostgreSQL с паролем суперпользователя xxXX1234.

Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

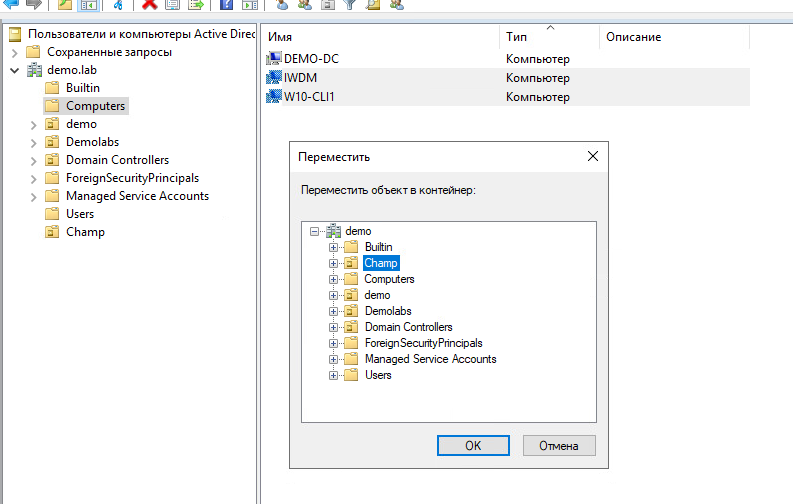
При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: officer с паролем xxXX1234

Синхронизировать каталог пользователей и компьютеров с Active Directory.

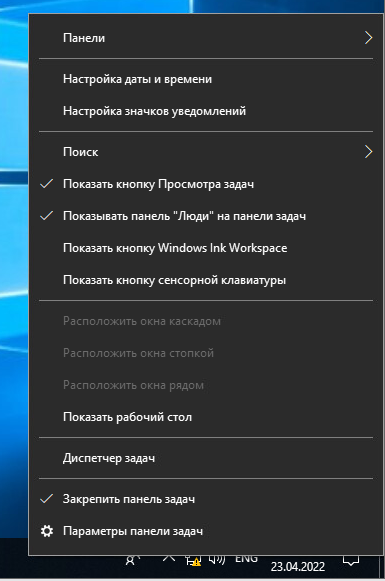
После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя iwdm-admin, установить полный доступ к системе, установить все области видимости.

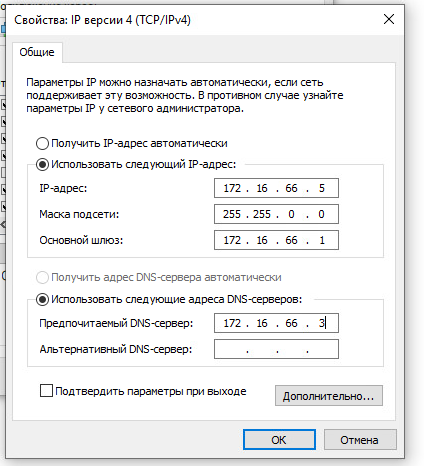
Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.

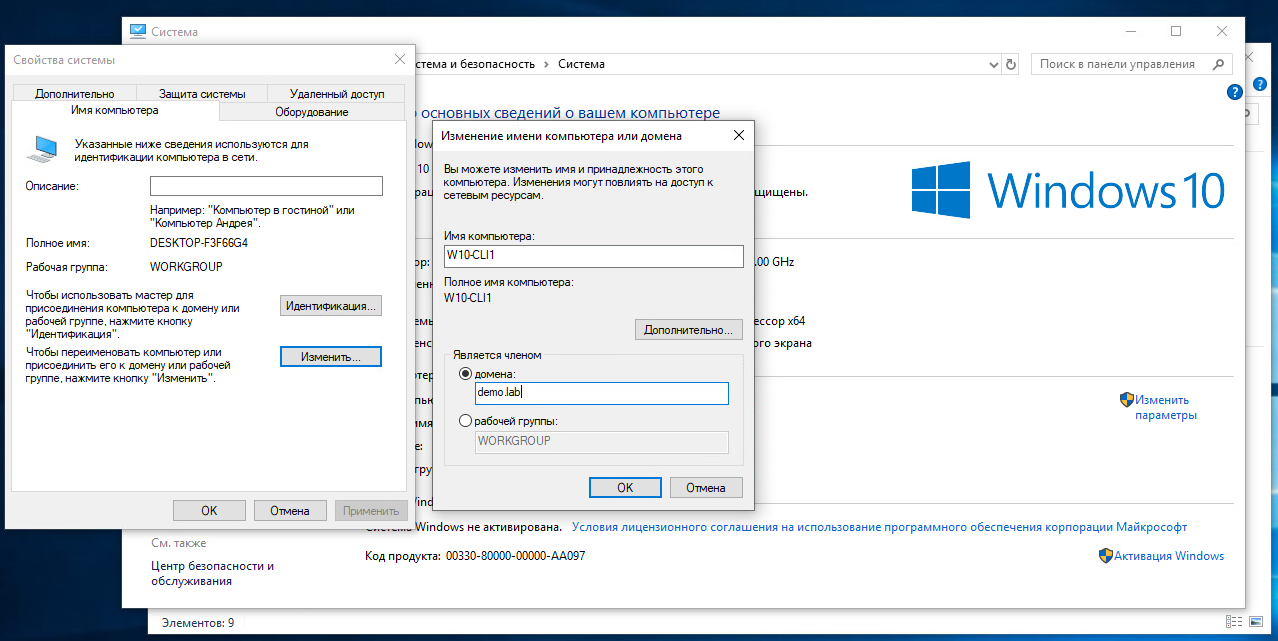
## Задание 4: Установка агента мониторинга на машине нарушителя

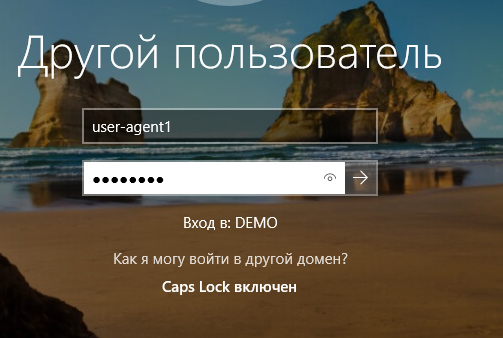


W10-CLI1

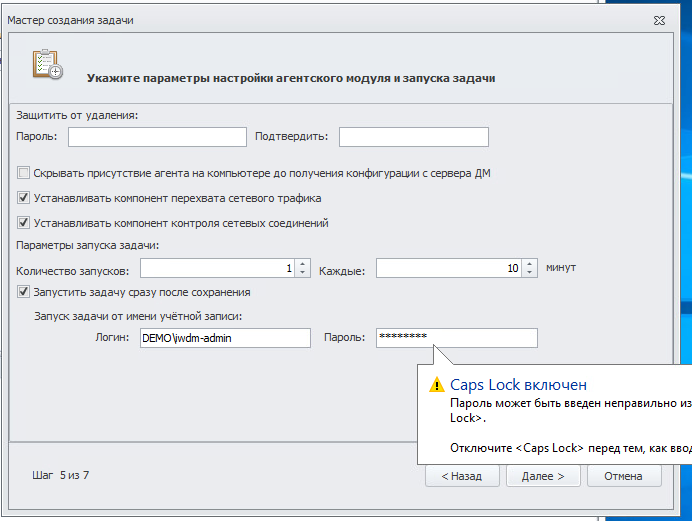


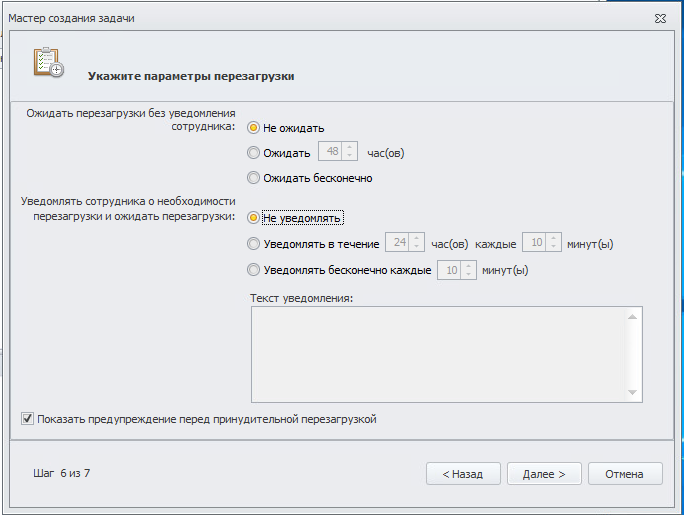












Необходимо ввести клиентскую машину в домен, после перезагрузки войти в систему от ранее созданного пользователя user-one.

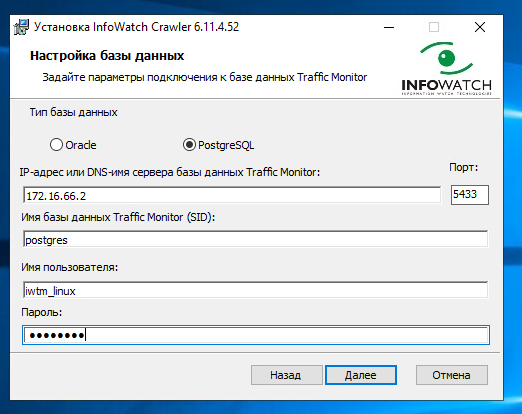
Установить агент мониторинга:

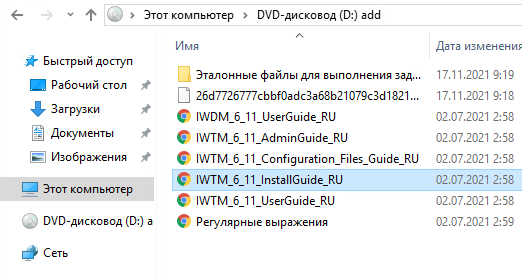
На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

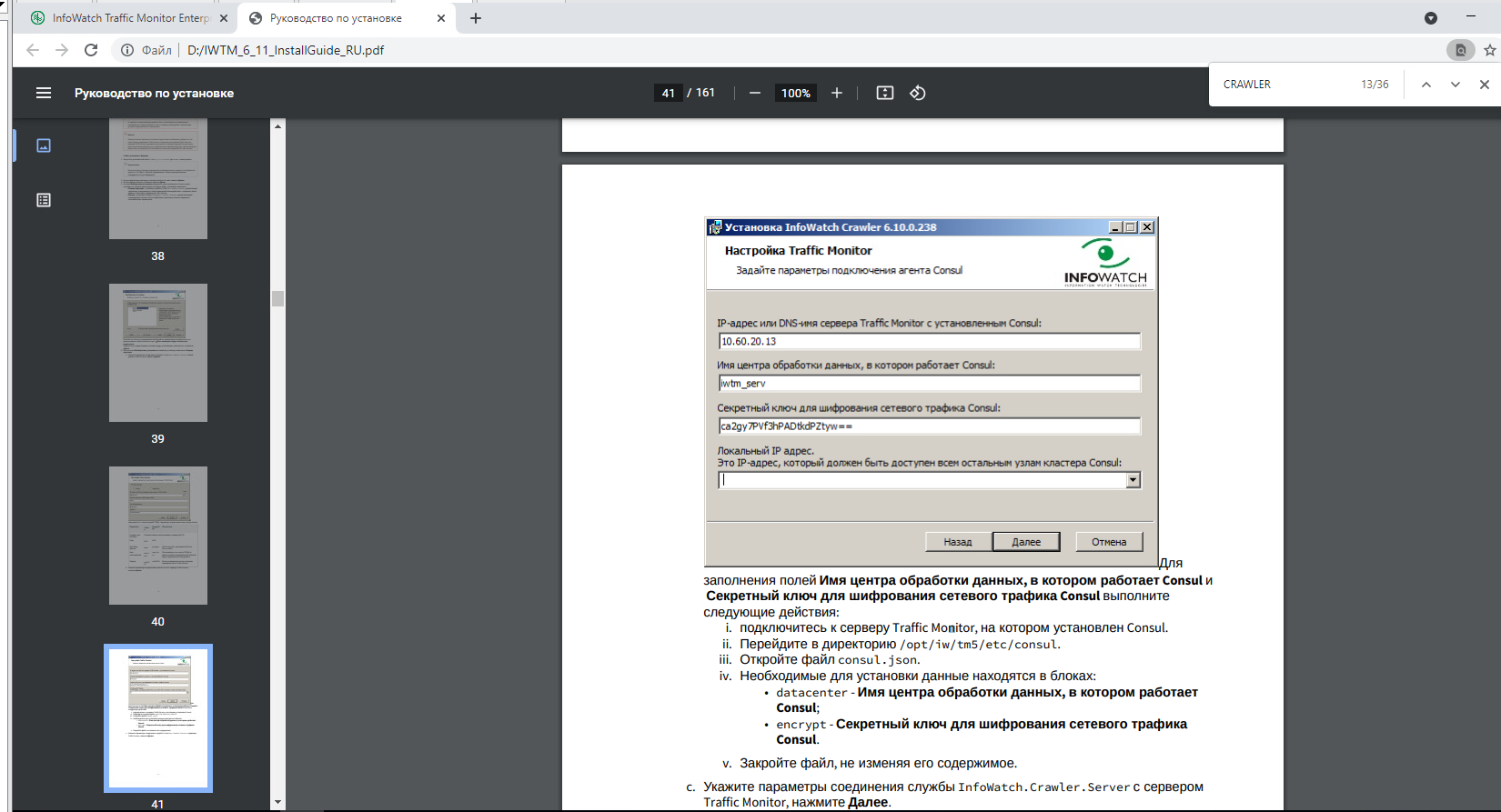
Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

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

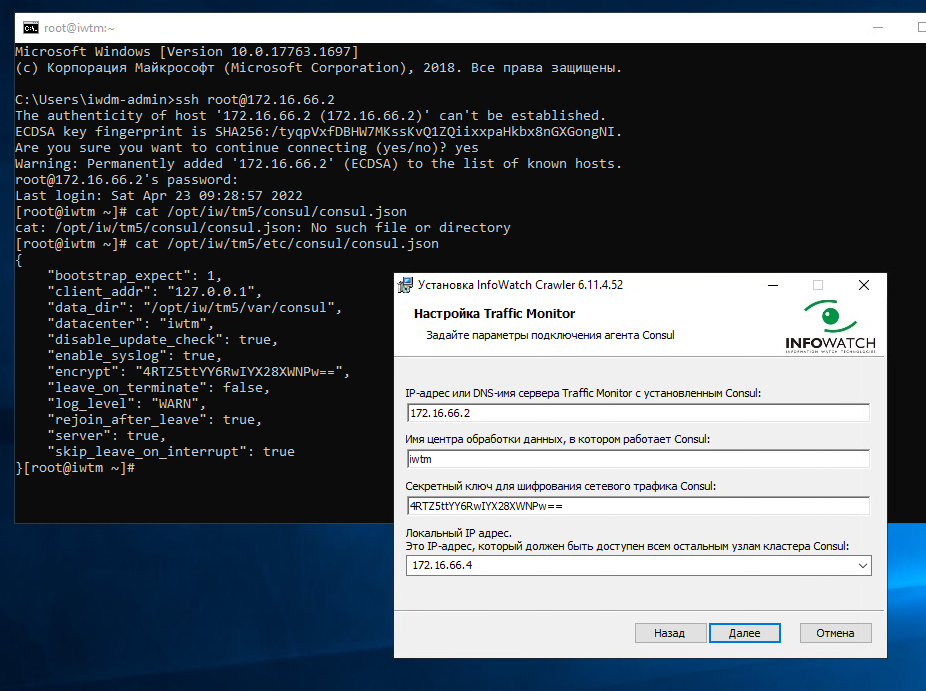
## Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов

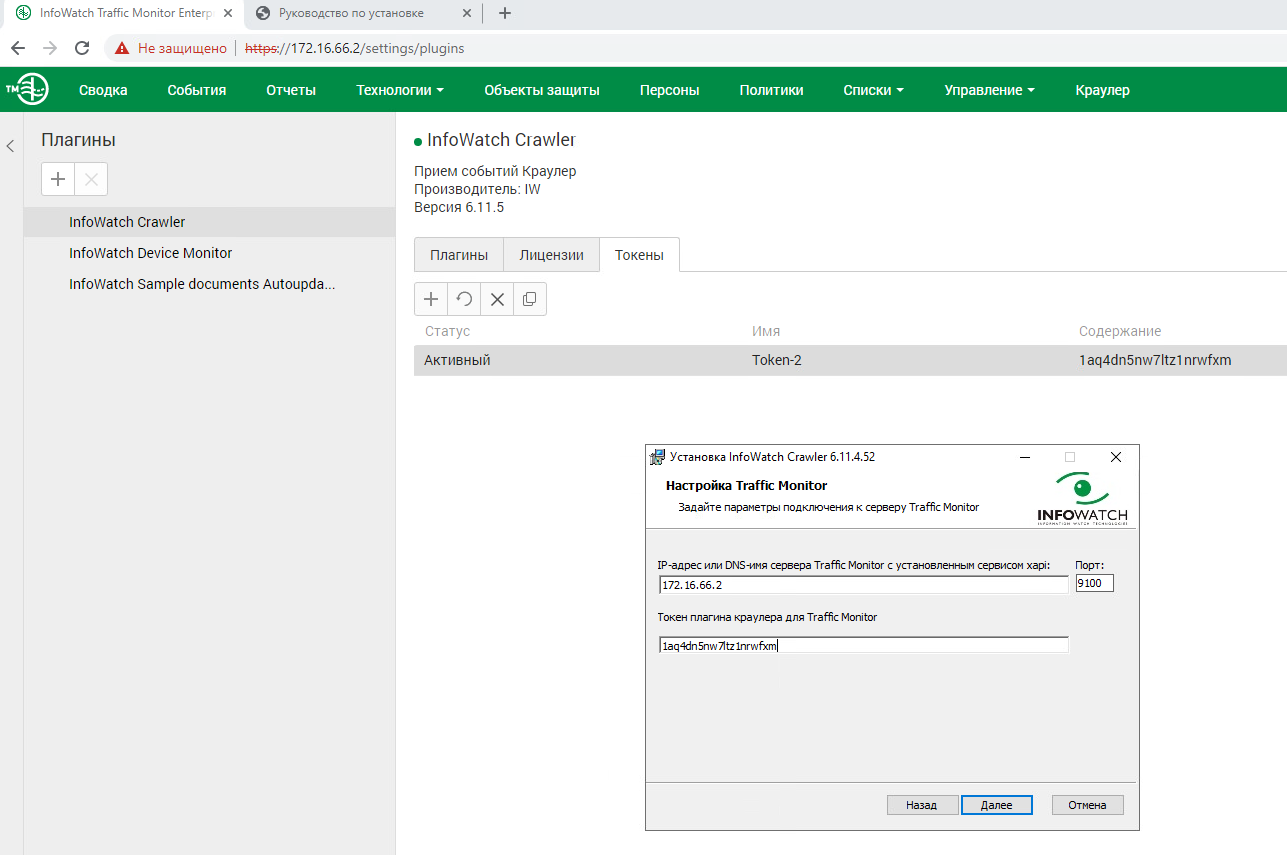


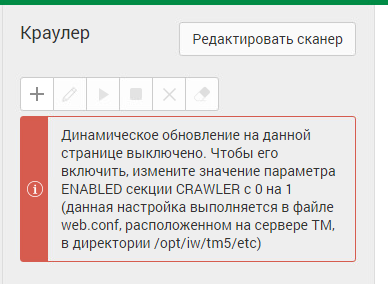








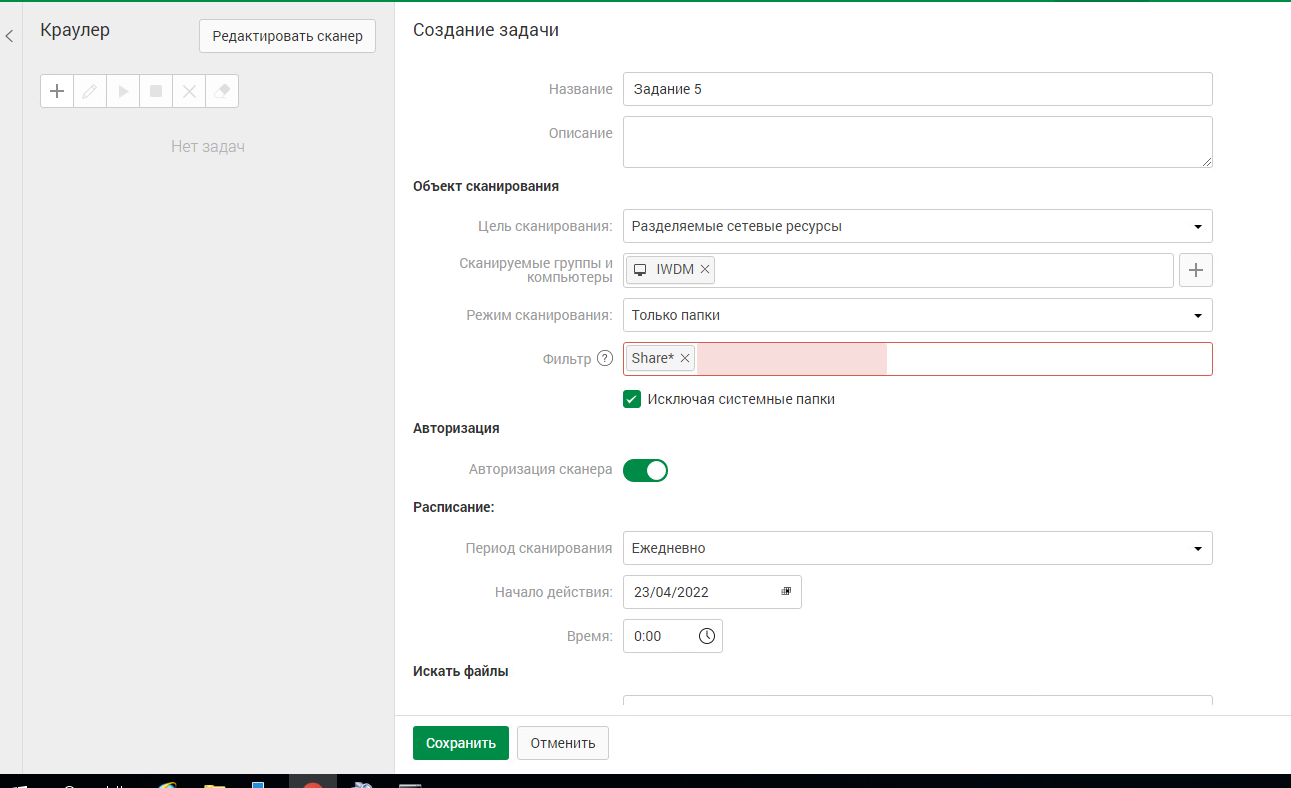


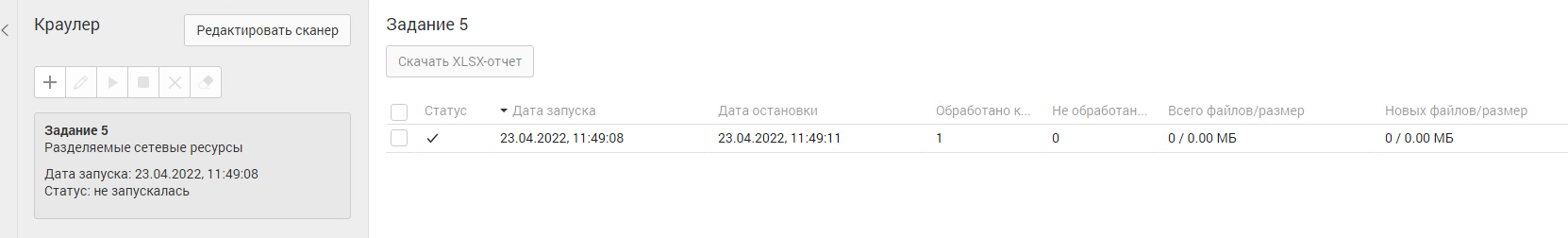


****









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

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

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).

## 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 некий термин, установить уровень угрозы для всех событий, добавить тег.

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.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

## Описание модуля 2:

Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

## Задание 1

Необходимо создать группу компьютеров: «Отдел1», а также создать новую политику: «Отдел1». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Отдел1.

Зафиксировать выполнение скриншотом.

## Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Отдел1».

## Правило 1

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

## Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

## Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

Проверить работоспособность и зафиксировать выполнение.

## Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

## Правило 5

Необходимо запретить запись файлов на все съёмные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

## Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

## Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение

## Правило 8

С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

## Правило 9

Необходимо поставить на контроль буфер обмена в блокноте и notepad++.

Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

## Правило 10

Необходимо запретить использовать копирование данных в терминальных сессиях для пользователя.

Проверить работоспособность и зафиксировать выполнение

## Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение

## Правило 12

Запретить передачу файлов с расширением .jpg (.jpeg) на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

## Групповые политики домена

Групповые политики применяются только на компьютер 1, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

## Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля -30 дней, Минимальная длина пароля - 8, пароль должен отвечать требованиям сложности, Блокировка учетной записи при повторном вводе неверного пароля (3 раза), продолжительность блокировки 15 минут.

Зафиксировать настройки политики скриншотами.

## Групповая политика 2

Запретить запуск приложений по списку: PowerShell, ножницы, сведения о системе.

Зафиксировать настройки политики и выполнение скриншотами.

## Групповая политика 3

Запретить использование панели управления стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

## Групповая политика 4

Запретить пользователю самостоятельно менять обои рабочего стола.

Зафиксировать настройки политики и выполнение скриншотами.

## Групповая политика 5

Настроить дополнительные параметры системы, согласно которым при входе на компьютер 1 отображается сообщение с именем сервера авторизации.

Зафиксировать настройки политики и выполнение скриншотами.