

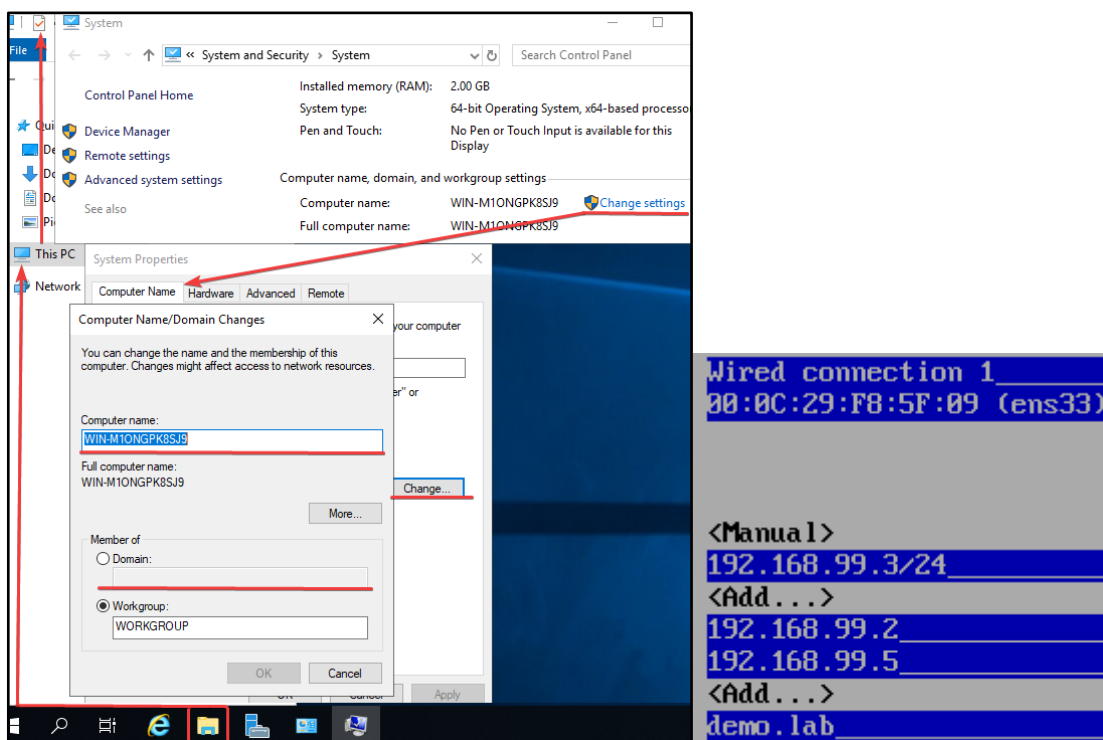
## ЗАДАЧА 1: ОБЩАЯ ПОДГОТОВКА СИСТЕМЫ.

Настроить сетевые адаптеры (свериться с demo.lab), возможно выкл\вкл адаптер. Проверить ping.

- Sconfig – для настройки системы\адаптера из командной строки.
- IWTM → nmtui – настраиваем сетевой адаптер IWTM (свериться с адресом demo.lab).
- /etc/hosts – настраиваем IP-адрес всех машин.
- /opt/iw/tm5/etc/consul/consul.json – «bind\_addr = (IP-адрес)» → iwtm restart.

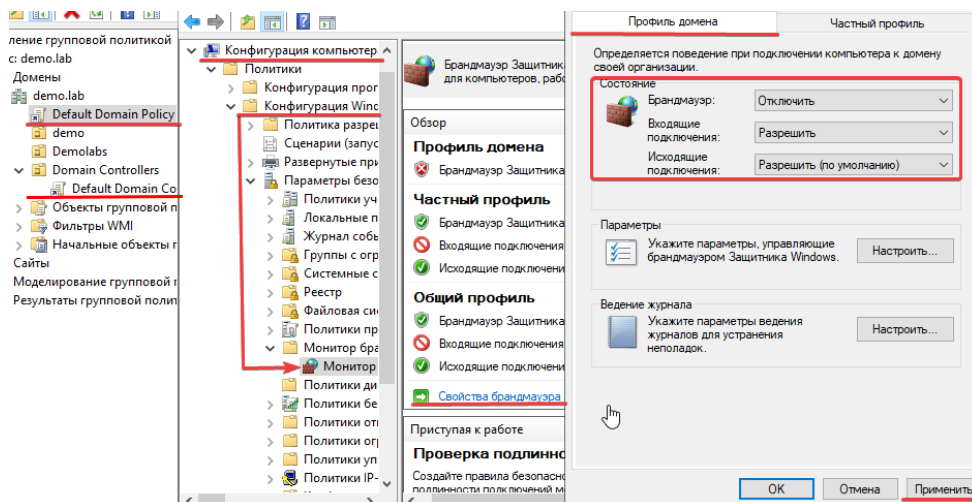
Ввести компьютеры в домен:

- Проводник → Этот компьютер → Значок в верхнем левом углу → Имя ПК, имя домена, параметры рабочей группы → Изменить параметры → Свойства системы →



Настроить фаерволл и включить общий доступ:

- AD → Средства → ГПО → Default Domain и Default Domain Controller → Конф.компьютер → Конф.Win → Монитор брандмауэра → Монитор брандмауэра → Свойства → Отключить защиту в Профиле домена



Оформить файл «отчет.txt» с данными машин и пользователей.

## ЗАДАЧА 2: УПРАВЛЕНИЕ РЕДАКТОРОМ VI.

ESC	Перейти в командный режим
i	Войти в режим набора текста
:wq ENTER	Сохранить и выйти

## ЗАДАЧА 3: ПОДГОТАВЛИВАЕМ СИСТЕМУ ДЛЯ CRAWLER.

- IWTM → `vi /opt/iw/tm5/etc/web.conf` → в параметре «crawler» меняем 0 → 1.

Открываем порты для Crawler в командной строке:

- `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.`

Так же можно открыть все порты:

- Настройки инета → Настройки брандмауэра → Дополнительные настройки брандмауэра → Для входящих и Исходящих → Создать правило → Порт → Для TCP и UDP (по отдельности) → Все порты → Разрешить (самый верхний пункт)

## ЗАДАЧА 4: ФИКС ДВОЯЩЕГОСЯ IP-АДРЕСА В IPCONFIG.

Выполняется в командной строке:

- `netsh interface ipv4 show inter (idx элемента ethernet).`
- `netsh interface ipv4 set interface (номер idx) dadtransmits=0 store=persistent.`
- В службах (services) выключаем пункт DHCP Client.

## ЗАДАЧА 5: ФИКС БАЗЫ ДАННЫХ.

Отредактировать `C:\Program Files\PostgreSQL\10\data\pg_hba.conf`. Добавить строчку: «host all all 0.0.0.0/0», в секцию «IPv4 local connections»

## МОДУЛЬ 1

### ЗАДАЧА 1: НАСТРОЙКА КОНТРОЛЛЕРА ДОМЕНА

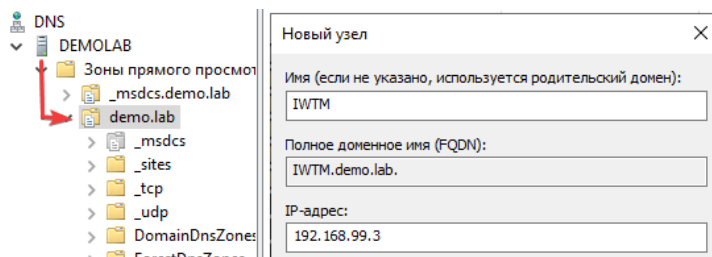
Настройка AD → Средства → «Пользователи и компьютеры»:

- demo.lab (правая кнопка мыши) → Создать → Подразделение “название по заданию” → Создать\настроить пользователей\ПК и права (Domain admin) (уточнить по заданию).

### ЗАДАЧА 2: НАСТРОЙКА DLP-СЕРВЕРА

Настройка Active Directory:

- Средства (DNS) → DEMOLAB → Зоны прямого просмотра → demo.lab.
- Создать узлы (A и AAAA) для каждой машины.
- Проверить настройки адаптера и соответствие DNS адреса.



Войти в веб-консоль (IP-адрес iwtm) под пользователем officer. Синхронизировать каталог с домена и добавить пользователя из AD: Управление → LDAP-синхронизация → Создать (+) →

Имя сервера: произвольное

LDAP-сервер: IP-адрес demo.lab | LDAP-запрос: DC=DEMO,DC=LAB

Логин: (по заданию) | Пароль: xxXX1234

- Управление → Управление доступом → Пользователи (+): Добавить пользователя из LDAP →

Почта: (админ.консоли)@demo.lab | Роли: Администратор, Офицер безопасности

Области видимости: Полный доступ, VIP

### ЗАДАЧА 3: УСТАНОВКА\НАСТРОЙКА СЕРВЕРА МОНИТОРИНГА

Установить PostgreSQL базу данных.

Установка DM:

Сервер: 127.0.0.1 | Имя: iwdm | Польз.: postgres | Пароль: xxXX1234

Локальный пользователь: officer\ xxXX1234

Соединение с ТМ: ip-iwtm, токен-веб | Адрес Платформы: ip-iwdm, токен-веб

Войти в консоль управления: 127.0.0.1 → admin\ xxXX1234. Настраиваем Device Monitor:

- Инструменты → Настройки → Интеграция с службами каталогов.
- Инструменты → Пользователи консоли и роли → Добавить из AD → Выберите добавляемого пользователя для администрирования DM.

Установка Crawler:

- `ssh root@ip-адре` → `cat /opt/iw/tm5/etc/consul/consul.json` → скопировать «datacenter» и «encrypt»

IP-адрес: IP-IWTM | Имя: iwtm | Имя пользователя: iwtm\_linux | Пароль: xxXX1234  
TM-IP-адрес: IP-IWTM» | Имя: поле iwtm | Ключ: поле «encrypt» (4RTZ5ttYY6RwIYX28XWNPw==).  
Токен: веб-консоль. | Учетная запись: Локальная система

Оформить файл «отчет.txt».

Группа сотрудников	Роль пользователя
demo	Офицер безопасности группы
Группа сотрудников по умолчанию	Офицер безопасности группы

Группа компьютеров	Роль пользователя
Все группы	Офицер безопасности группы

Общие роли
Офицер безопасности
Администратор

## ЗАДАЧА 4: УСТАНОВКА АГЕНТА НА МАШИНЕ НАРУШИТЕЛЯ

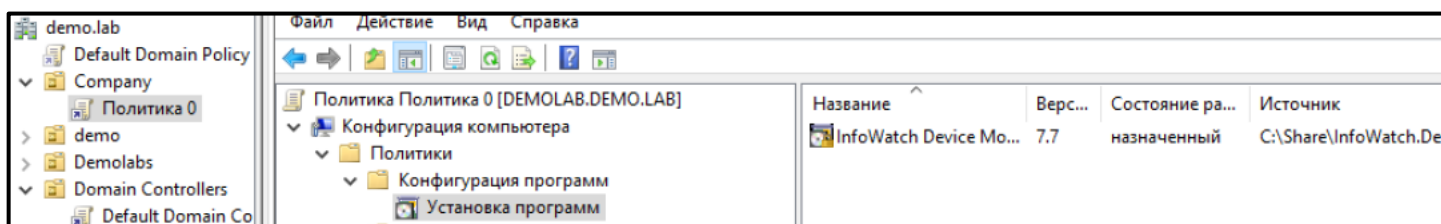
Установка агента мониторинга с помощью средств распространения (скриншот):

- Задачи → Создать задачу → Задача первичного распространения → Добавить «название клиентской машины»

Логин: DEMO\ «администратор домена» | Пароль: xxXX1234  
Установить пароль на удаление агента мониторинга: xxXX123

Установка агента мониторинга с помощью ГПО (скриншот):

- Создать папку Share на IWDМ → Свойства → Общий доступ → Для всех.
- Инструменты → Создать пакет установки → Установить пакеты в папку Share → Установить пароль
- demo.lab → GPM → Создать новую политику → Конф.компьютера → Политики → Конф.программ → Установка программ → Создать → Пакет → Удалить всех пользователей в безопасности → Добавить КОМПЬЮТЕР клиента → обновить ГПО на ПК demo.lab\клиента: gpupdate /force.



Оформить файл «отчет.txt»

## МОДУЛЬ 2

### ЗАДАЧА 0: ОФОРМЛЕНИЕ ЗАДАНИЙ И СКРИНШОТОВ

Разделы/политики/группы и т. п. называются: «Политика 1» | «Правило 1.2» и т. д.

Все скриншоты необходимо сохранить в папке «Модуль 2»:

- Для созданной политики: CR-1.jpg. | Для работающей политики: RW-1.jpg.
- Для нескольких скринов одной политики: RW-«Н.задания»-«Н.скриншота».jpg. Н-р: RW-1-2.jpg

### ЗАДАЧА 1: ПОДГОТОВКА СЕРВЕРА АГЕНТСКОГО МОНИТОРИНГА

Настраиваем Device Monitor (скриншот):

- Политики → Создать политику → «название по заданию»
- Группы компьютеров → Создать группу устройств → «название по заданию» → Добавить клиентскую машину.

### ЗАДАЧА 2: ПОЛИТИКИ DM. (СКРИНШОТЫ)

Правило 1. Запретить запуск приложения `scalc.exe\mspaint.exe`. (скриншот)

- Приложения → + → Название → Открываем → Только по имени приложения → Название файла (свойства приложения → расположение файла → свойства → копируем название).
- Политика → Название → Application Monitor → Запретить запуск → Черный список → Название.

Правило 2. Запретить создание снимков в текстовых редакторах `wordpad.exe\ scalc.exe`. (скриншот)

- Приложения → + → Название → Открываем → Только по имени приложения → Название файла (свойства приложения → расположение файла → свойства → копируем название).
- Название → ScreenShot Control Monitor → Если запущены приложение

Правило 3. Запретить DropBox, разрешить GoogleDisk, остальные в режиме чтения. (скриншот)

- Название → Could Storage Monitor → DropBox (запретить), Google Drive (разрешить), все остальное (только скачивание).

Правило 4. Запретить печать на сетевых принтерах\Разрешить печать на локальных. (скриншот)

- Политики → Название → Device Monitor → Сетевой принтер → Запретить.
- Политики → Название Н.1 → Device Monitor → Локальный принтер → Разрешить

Правило 5. Запретить запись файлов на съёмные носители информации, оставить считывания информации (скриншот)

- Политика → Device Monitor → Съёмное устройство хранения → Только чтение

Правило 6. Разрешить использование доверенного носителя информации. (скриншот)

- Политика → Device Monitor → Съёмное устройство хранения → Полный доступ на зашифрованные носители.
- Белый список → + → Найти → Клиентская машина → Выбираем все съёмные носители

Правило 7. Заблокировать CD/DVD. В случае отсутствия CD/DVD - его создать. (скриншот)

- Название → Device Monitor → CD/DVD – Нет доступа

Правило 8. Выдача временного доступа клиенту до заблокированного CD/DVD. (скриншот)

- Политика → Название → Инструменты → Временный доступ сотрудника → По телефону → Выбираем CD/DVD, сотрудника, код (с cli0машины), Н минут
- Список устройств → Выбираем дисковод → Запросить доступ → Вводим код запроса в DM → Получаем код подтверждения.

Правило 9. Запретить использовать терминальные сессии. (скриншот)

- Политики → Device Monitor → Терминальный порт → Использования запрещено.

Правило 11. Контроль за ПК при использовании браузера с снимками каждые 60 секунд\при переходе в другое окно. (скриншот)

- Приложения → + → Название → Название приложения браузера (свойства → расположение файла → свойства → копируем название) (???)
- Политика → ScreenShot Monitor → Всегда\если активно приложение\при смене окна → Название → 60 сек

Правило 12. Запретить передачу файлов с расширением .jpg (.jpeg) на съемные носители информации\сетевое расположение. (скриншот)

- Политики → File Monitor → Приемник копирования → Сетевые ресурсы → Маска файла: \*.jpg, \*.jpeg → Категория файла: Графические данные → Разрешить копирование и создавать события с теньвыми копиями (запретить если доступно).

**БРАУЗЕР**

- Списки → Теги → + → Название
- Технологии → Категории и термины → +: Название → +: jpeg → +: jpg
- Объекты защиты → + → Название → Добавляем наши термины
- Политики → Добавить политику: → Защищаемые данные → Объекты: объект защиты и Файловый форматы: JPEG. → Правило передачи → Направление: оба → Тип события: все → Компьютеры: все → Вердикт: Заблокировать → Уровень: Высокий → Тег: Название.

Правило. Необходимо поставить на контроль буфер обмена в notepad.exe\ notepad++.exe. (скриншот)

- Приложения → + → Только по имени приложения → Название файла (свойства приложения → расположение файла → свойства → копируем название).
- Политика → Clipboard Monitor → В приложения кроме терминальной сессии: Название
- Device Monitor – Журнал → + → Новый фильтр.

## ЗАДАЧА 3: ГРУППОВЫЕ ПОЛИТИКИ. (СКРИНШОТЫ)

Скрин при выполнении\после выполнения вкладка параметры

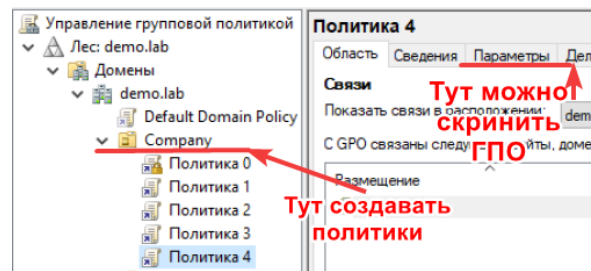
У групповых политик очистить фильтр безопасности и добавлять пользователя\компьютер по заданию. Чтобы обновить ГПО на ПК клиента: `gpupdate /force`.

`C:\Windows\SYSTEM32\sysvol\winitpro.loc\scripts\Screen.`

UNC-путь будет выглядеть так: `\\server-name\SYSTEM32\winitpro.loc\scripts\Screen\corp_wallpaper.jpg`.

Проверьте, что у пользователей домена есть права на чтение этого файла (проверьте NTFS разрешения, предоставив право Read группе Domain Users или Authenticated Users).

В безопасность политики добавляется юзер и его компьютер!!!



Политика 1. Настроить политику паролей и блокировки. (скриншот)

- Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики учетных записей → Политика паролей
- Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Политики учетных записей → Политика блокировки учетных записей.

Политика 2. Запретить запуск приложений: PowerShell, ножницы, сведения о системе. (скриншот)

- Конфигурация пользователя → Политики → Административные шаблоны → Система → Не запускать указанные приложения (powershell.exe, SnippingTool.exe, wordpad.exe, notepad.exe.)

Политика 3. Запретить использование: панели управления, реестра, командной строки. (скриншот)

- Конфигурация пользователя → Политики → Административные шаблоны → Система → Запретить доступ к средствам редактирования реестра.
- Конфигурация пользователя → Политики → Административные шаблоны → Система → Запретить использование командной строки.
- Конфигурация пользователя → Политики → Административные шаблоны → Панель управления → Запретить доступ к панели управления.

Политика 5. Запретить пользователю самостоятельно менять обои рабочего стола. (скриншот)

- Конфигурация пользователя → Политики → Административные шаблоны → Панель управления → Персонализация → Запрет изменения фона рабочего стола.

Политика. При входе на компьютер 2 отображается сообщение с именем сервера. (скриншот)

- Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Параметры безопасности → Интерактивный вход в системы: текст сообщения для пользователей при входе → demo.lab.

Политика. Отключить возможность локального входа для пользователей. (скриншот)

- Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Локальные политики → Назначение прав пользователя → Запретить локальный вход

Политика. Запретить показ анимации при входе в систему (скриншот)

- Конфигурация компьютера → Политики → Административные шаблоны → Система → Вход в систему → Показать анимацию при первом входе в систему = Отключено.

## ЗАДАЧА 1: ОФОРМЛЕНИЕ ЗАДАНИЙ И СКРИНШОТОВ

Для настройки политик используйте файл AdditionalFiles.iso в datastore1.

Задание 1. Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты (такого задания может не быть).

Задание 2. Создайте локальную группу пользователей и добавьте N пользователей.

– Персоны → Пользовательские группы → Создать группу. Добавить пользователей в группу.

Задание 3. Создать список веб-ресурсов. Добавить сайты: rt.ru, infotecs.ru, vmware.com.: Списки → Веб-ресурсы → Создать список веб-ресурсов → Название → Перейти к списку → Добавить веб-ресурс.

Задание 4. Настроить периметр компании: Почтовый домен компании, список веб-ресурсов, группа персон, исключить из перехвата почту генерального директора.

– Списки → Периметры → Компания → Контакты → Почтовый домен: @demo.lab | Список веб-ресурсов: Сайты партнеров | Группа персон: Название.

– Исключить из перехвата → Контакты: kornilov@demo.lab (или другая почта).

## ЗАДАЧА 1: ПОДГОТОВКА ВЕБ→КОНСОЛИ

Политика 1. Запретить сотрудникам, кроме отдела кадров отправлять документы с паспортными данными.

- Списки → Теги → +:
- Объекты защиты: + → Перейти в каталог → +: Название → Поиск: паспорт (текстовые\графические)  
Создать объект защиты на каждый выбранный элемент → Добавить условие для каждого объекта
- Политики → Добавить политику: Защиты данных → Защищаемые данные → Объекты: объект защиты → Правило передачи → Направление: В одну → Тип события: Все → Компьютеры: Все → Отправители: не HR → Получатели: не demo.lab

Политика 2. Вести наблюдение за передачей документа договора. Документ может изменяться: 50%. (возможно придется заполнить документ, если выскакивает ошибка)

- Списки → Теги → +:
- Технологии → Эталонные документы → +: договор, порог цитируемости: 50%\50% → +: договор.doc
- Объекты защиты: + → Условие: Договор (эталонные док.) → Добавить условие
- Политики → Добавить политику: Защиты данных → Защищаемые данные: объект защиты → Правило передачи → Направление: В одну → Тип события: Все → Компьютеры: Все → Получатели: не Компания



Политика 3. Необходимо запретить обмен фотографией и измененной (до ≈50%) фотографией котика.

- Списки → Теги → +: Название
- Технологии → Эталонные документы → +: котик, 10%\50% → +: котик.jpg
- Объекты защиты → +: Название → +: Название → Условие: котик (эталонные док.) → Добавить условие
- Политики → Добавить политику: Защиты данных → Защищаемые данные: объект защиты → Правило передачи → Направление: В оба → Тип: Все

Политика 4. Отслеживать документы с печатью всем сотрудникам, кроме отдела бухгалтерии и генерального директора (внутри и за пределами компании без контроля).

- Списки → Теги → +: Название
- Технологии → Печати → +: печать → +: печать.png
- Объекты защиты → +: Название → +: Название → Поиск: Печать (печати) → Добавить условие
- Политики → Добавить политику: Защиты данных → Объект защиты: объект защиты → Сохранить
- Передача → Направление: В оба → Тип: Все → Компьютеры: Все → Отправитель: не Kornilov, Accounting

Политика 5. Необходимо отслеживать передачу данных кредитных карт\сканов.

- Списки → Теги → +: Название
- Объекты защиты → +: Название → +: Название → Поиск: Карта, номер, номер (16 цифр) (Графический\текстовой), Добавить условия → Создать объект защиты на каждый выбранный элемент
- Политики → Добавить политику: Политику защиты → Объект защиты: объект защиты → Сохранить
- Передача → Направление: В одну → Тип: Все → Компьютеры: все → Отправители: Accounting

Политика 6. Настроить мониторинг выгрузок БД: телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД, ОКОПФ и в 1 документе → более 5 компаний. При отправке из определенного отдела.

- Списки → Теги → +: Название
- Технологии → Выгрузка из БД → +: Название → +: Выгрузка из БД.csv → Редактировать → Условие обнаружения: 5+7+10+14+16+18 (количество цифр в каждом объекте)
- Объекты защиты → +: Название → Перейти в каталог → +: Название → Добавить условие → Поиск: Выгрузка из БД (выгрузки из БД)
- Политики → Добавить политику → Объект защиты: объект защиты → Правило передачи → Направление: В одну сторону → Тип: Все → Компьютеры: Все (1 клиентская машина) → Отправители: не HR

Политика 7. Контроль передачи содержащие слова: «абонент», «оборудование», «услуга» в 1 сообщении\документе одновременно. Отправляются за пределы компании (кроме отдела IT).

- Списки → Теги → +: Название
- Технологии → Категории и термины: + (вес: 1, учитывать: все) → +: Слово, Характеристический, Учитывать регистр. (повторить для каждого слова)
- Объекты защиты: + → Категории (созданное ранее «Категории и термины»)
- Политики → Добавить политику: Защиты данных → Защищаемые данные: объект защиты → Правило передачи → Направление: В одну сторону → Тип события: Все → Отправители: Компания (имя домена)

Политика 8. Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках. Кроме генерального директора и совета директоров.

- Списки → Теги → +: Политика 8
- Технологии → Эталонные документы: + → Порог цитируемости: 25%\25% → +: Анкета участника
- Технологии → Бланки: + → +: Анкета участника
- Объекты защиты: + → Поиск: Анкета участника (эталонные документы и бланки) ( либо «Создать объект защиты для каждого объекта, либо «Условие: ... или...или»
- Политики → Добавить политику: Защиты данных → Защищаемые данные: объект защиты → Правило передачи → Направление: В одну сторону → Тип события: Все → Отправители: не Karnilov и

Политика 9. Блокировать передачу (контролировать) файлов формата .mp4\ссылок чатов IRC.

- Списки → Теги → +: Политика 9
- Технологии → Текстовые данные → +: Название → +:Название → Добавить шаблон → Регулярные выражения: irc://[^\s/]+(/[^\s/]+)?
- Объекты защиты: + → Поиск: Политика 9 (текстовые данные) → Добавить условие
- Политики → Добавить политику: Защиты данных → Защищаемые данные: объект защиты и файловые (MP4) → Правило передачи → Направление: обе → Тип события: Все → ПК: Все → Отправители: все

Политика 11. Предотвратить передачу паролей в открытом виде. Любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки. Контролировать наличие паролей в сетевых каталогах. Пользователи отдела ИТ могут рассылать совершенно свободно, но только внутри компании. Стандартизированные форматы паролей (кириллица): 6 букв – 1 знак !?#\$%^/\_& – 2→4 цифры – 4 буквы – 2→3 знака !?#\$%^/\_& (например, ПаРоль#67pКнЕ!?) ).

- Списки → Теги → +: Политика 11
- Технологии → Текстовые данные → +: Название → +:Название → Добавить шаблон → Регулярные выражения: [А-Яа-я]{6}[!?\$%^/\_&]{1}[0-9]{2,4}[А-Яа-я]{4}[!?\$%^/\_&]{2,3}
- Политики → Добавить политику: Защиты данных → Защищаемые данные: объект защиты → Правило передачи → Направление: обе → Тип события: Все → ПК: Все → Отправители: не IT

Политика 12. Контролировать передачу архивов, файлы таблиц только за пределы компании.

- Списки → Теги → +: Название
- Политики → Добавить политику: Защиты данных → Защищаемые данные: файловые объекты (расширения архивов и таблиц) → Правило передачи → Направление: одно → Тип события: Все → ПК: Все → Отправители: Компания (имя домена)