Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DLP-инвентаризация в МСБ: 3 канала утечки, которые мы закрыли

Как мы описываем данные, ставим агента по GPO и закрываем почту, USB и личные облака

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Клиентская база, прайсы с персональными скидками и договоры в компании на 30-50 мест живут в почте, на флешках и в личных облаках сотрудников — и уходят вместе с человеком. Мы решаем задачу инвентаризации: описать, какие данные ценны, где они перемещаются и какие каналы открыты. Без этого утечку замечают постфактум — когда тендер уже выигран конкурентом, а доказательств нет.

Почему это важно бизнесу

- Уход менеджера с выгрузкой CRM — потеря годовой воронки: контакты ЛПР и история сделок начинают работать на конкурента.
- Утечка прайса с индивидуальными скидками ломает переговоры: конкурент заранее знает вашу нижнюю границу цены.
- Без доказательной базы расставание с нелояльным сотрудником превращается в трудовой спор, который компания проигрывает.
- 152-ФЗ и договоры с заказчиками требуют защиты данных: утечка — это ещё и проверка со штрафом, а не только упущенная прибыль.
- Первый же перехваченный инцидент окупает внедрение: цена одной сорванной сделки выше годовой стоимости системы.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

5.8

актуальная ветка Staffcop Enterprise: сервер на Ubuntu 18.04/20.04/22.04 или Astra SE 1.7/1.8,…

Staffcop 5.8, «Требования: сервер и БД»

32 ГБ RAM

и 8 ядер на 100 пользователей по таблице требований; на 10 рабочих мест хватает 4 ГБ и 2 ядер

Staffcop 5.8, «Требования: сервер и БД»

5000 IOPS

минимум для NVMe под основную БД плюс скорость от 1500 МБ/с — на медленном диске отчёты строят…

Staffcop 5.8, «Требования: сервер и БД»

443/TCP

порт сервера в примере тихой установки (GATE_PORT); резервный — через GATE_URL2 и GATE_PORT2,…

Staffcop 5.8, «Тихая установка агента»

6416

событие Audit PNP Activity (Detailed Tracking, только Success): учёт носителей до внедрения DL…

Microsoft Learn, Audit PNP Activity

150 %

свободного места от размера текущей базы под создание архивной БД; на одном диске с основной —…

Staffcop 5.8, «Создание архивной БД»

РЕАЛИЗАЦИЯ 1 ИЗ 3

Канал 1: личная почта и веб-почта — перехват на конечной точке

Что настраиваем

Группы «Продажи» и «Бухгалтерия», Windows-агент на всех доменных PM, разбор HTTP/HTTPS на самой станции

Как мы это делаем

1. Раскатываем агента по GPO Computer Startup: msiexec /qn /norestart /l*vx install.log /i "C:\Windows\agent.msi" GATE_URL=<сервер> GATE_PORT=443 GATE_URL2=<резерв> AL...
2. Включаем модули «Веб трафик» (перехват HTTP/HTTPS, в том числе через SSL/TLS) и «Перехват веб-форм» (POST-запросы): веб-почта видна вместе с именами вложений.
3. Теневое копирование включаем в связке с модулем «Файловая активность» — в базу ложится сам файл, а не только имя и размер.
4. Детекторы строим на точных паттернах: регулярки ИНН/КПП, номера договоров, маски имён выгрузок; на .xlsx/.csv/.mdb во внешние домены — правило блокировки.
5. В антивирусе отключаем HTTPS/SSL-инспекцию и вносим в исключения пути агента: C:\Windows\agent.msi, auxiliaryservice.exe, C:\Windows\SysWOW64\TimeControlSvc*.

РЕЗУЛЬТАТ

Выгрузка CRM на личный ящик фиксируется и блокируется на рабочей станции — до того, как письмо ушло в чужой почтовый сервис. У руководителя остаётся доказуемая копия вложения и цепочка событий по конкретному пользователю, а не догадки.

КЛЮЧЕВОЙ НЮАНС

Ключевой раздел документации — «Исключения антивируса»: одновременный разбор SSL двумя системами невозможен. Не сняли HTTPS-инспекцию у антивируса — модуль веб-трафика формально жив, а вложения по HTTPS не раз...

РЕАЛИЗАЦИЯ 2 ИЗ 3

Канал 2: съёмные носители — от учёта к белому списку

Что настраиваем

Все доменные PM: модуль «USB-устройства» на агенте плюс второй контур на GPO; отдельный профиль для руководителей

Как мы это делаем

1. Первая неделя — учёт без блокировок: Advanced Audit Policy Configuration → Detailed Tracking → Audit PNP Activity (Success), событие 6416 — собираем реальный парк н…
2. Формируем белый список: правило «Разрешить» по Device ID корпоративных флешек (в Windows идентификаторы начинаются с USB\), всё неперечисленное блокируется.
3. В белый список обязательно добавляем классы устройств usb:*ic09isc00* (хабы) и usb:*ic03isc* (клавиатуры и мыши) — иначе вместе с флешками отвалится ввод.
4. Остальным включаем «Блокировать USB-накопители» или «USB-накопители только для чтения»; второй контур на GPO: System → Removable Storage Access → «Removable Disks:…
5. Для разрешённых носителей включаем теневое копирование: модуль «USB-устройства» плюс «Файловая активность» и настройка «Теневое копирование».

РЕЗУЛЬТАТ

Съёмные носители перестают быть слепой зоной: есть перечень разрешённых устройств, копия ушедшего файла и алерт на подключение неизвестного носителя. Массовая выгрузка перед увольнением видна как аномалия объёма, а не как «что-то копировал».

КЛЮЧЕВОЙ НЮАНС

Блокировать сразу нельзя: в МСБ на флешках живут ключи ЭП, дистрибутивы обновлений 1С и сканы. Неделя учёта по 6416, Device ID и классы USB в белом списке экономят две недели разбирательств с бухгалтерией.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Канал 3: личные облака — это домен в браузере, а не exe

Что настраиваем

Группы «Продажи», «Маркетинг», «Бухгалтерия»: запрет клиентов синхронизации плюс блокировка доменов и веб-форм

Как мы это делаем

1. Клиенты синхронизации закрываем правилами AppLocker или WDAC по издателю, а не по имени файла: переименованный exe политику по пути обходит.
2. В конфигурации «Интернет» → «Блокировка сайтов» закрываем веб-интерфейсы личных облаков и файлообменников; правило пишем без протокола, чтобы закрыть и http, и http…
3. «Перехват веб-форм» даёт список файлов, ушедших POST-запросом в облако, даже когда клиент синхронизации на машине не установлен.
4. Где у клиента есть M365, добавляем Purview Endpoint DLP: Sensitive service domains (до 100 сайтов в группе, до 150 групп) и Restricted app groups.
5. Взамен закрытого канала сразу даём легальный: корпоративное хранилище и бэкап рабочих папок, иначе обход находят за неделю.

РЕЗУЛЬТАТ

Веб-загрузка в личное облако перестаёт быть дырой, через которую обходится запрет exe-клиента. Событие пишется с именем файла и доменом, политика одинаково работает на доменных станциях и на личных ноутбуках подрядчиков.

КЛЮЧЕВОЙ НЮАНС

Самая частая ошибка внедрения — блокировка только по процессу клиента синхронизации. Веб-интерфейс того же сервиса остаётся полностью открытым: закрывать нужно домен и веб-форму.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Агент раньше подписанных документов**
  Мониторинг без уведомления обесценивает доказательства по ТК РФ и 152-ФЗ. Агента не ставим, пока не подписаны положение, уведомление и допсоглашение.

- ✕ **Блокировка по имени процесса**
  Правило на Yandex.Disk.exe или Dropbox.exe обходится переименованием файла и веб-интерфейсом. Закрываем по издателю в WDAC/AppLocker и по домену.

- ✕ **База DLP на медленном диске**
  Документация требует NVMe от 1500 МБ/с и 5000 IOPS. ClickHouse подключаем при 100+ пользователях и хранении дольше 3 месяцев: это ещё 40-50 % объёма…

- ✕ **Антивирус разбирает SSL параллельно**
  Две системы не инспектируют HTTPS одновременно. Снимаем SSL-инспекцию у антивируса и вносим пути агента (agent.msi, auxiliaryservice.exe, TimeControl…

- ✕ **Словари из общих слов**
  Детекторы на «клиент» и «прайс» дают шквал ложных срабатываний, и алерты перестают читать. Держим точные паттерны: ИНН/КПП, номера договоров.

- ✕ **Белый список USB без классов устройств**
  Правило «Разрешить» блокирует всё неперечисленное — включая хабы, клавиатуру и мышь. Классы usb:*ic09isc00* и usb:*ic03isc* добавляем в список сразу.

- ✕ **База растёт без регламента**
  Без автоочистки и архивной БД диск заканчивается на 6-9 месяце. Под создание архива нужно 150 % свободного места от размера базы, на общем диске — 20…

- ✕ **DLP без владельца алертов**
  Система, дайджест которой никто не разбирает, — дорогое хранилище логов. Минимум 2-4 часа в неделю у ответственного закладываем в проект.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Положение о конфиденциальной информации, уведомление и допсоглашение — подписаны
- Включён Audit PNP Activity (Success), события 6416 собираются и хранятся не меньше м…
- GPO «Removable Disks: Deny write access» на группы без потребности в флешках
- Клиенты личных облаков закрыты AppLocker или WDAC по издателю

НОРМАЛЬНО

- Сервер Staffcop 5.8 на Ubuntu 22.04 LTS или Astra SE 1.7/1.8, PostgreSQL 15, БД на N…
- Агенты раскатаны по GPO с GATE_URL/GATE_URL2, ALLUSERS=1 и включённой «Защитой агент…
- Белый список USB по Device ID и классам устройств плюс теневое копирование
- Закрыты домены личных облаков и веб-почты, снята SSL-инспекция антивируса

ХОРОШО

- ClickHouse при 100+ пользователях и хранении дольше 3 месяцев, архивная БД и автоочи…
- Разные профили: блокировки для линейных ролей, только мониторинг для руководителей
- Детекторы на регулярках ИНН/КПП и OCR скриншотов вместо словарей общих слов
- Три уровня реакции: авто-блок, недельный дайджест руководителю, критика в Telegram

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Подписаны ли уведомление о мониторинге и допсоглашение к трудовому договору у всех сотрудников?
- [ ] Есть ли утверждённый перечень защищаемых данных с ответственным владельцем по каждой категории?
- [ ] Известен ли перечень разрешённых USB-носителей по Device ID (строка вида USB\VID_...&PID_...)?
- [ ] Добавлены ли в белый список классы usb:*ic09isc00* и usb:*ic03isc*, чтобы не отвалились хабы и мышь?
- [ ] Включён ли Audit PNP Activity и собираются ли события 6416 хотя бы месяц до блокировок?
- [ ] Закрыты ли веб-интерфейсы личных облаков доменным правилом, а не только exe-клиенты?
- [ ] Лежит ли база DLP на NVMe от 1500 МБ/с и 5000 IOPS и хватает ли RAM по таблице требований?
- [ ] Снята ли HTTPS-инспекция в антивирусе и внесены ли пути агента в исключения на всех РМ?
- [ ] Включена ли «Защита агента» паролем — и знает ли админ, что перед обновлением её нужно снять?
- [ ] Есть ли автоочистка и запас 150 % места под архивную БД, и кто разбирает дайджест алертов?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Инвентаризируем ценные данные и строим карту каналов: почта, носители, облака, печать, мессенджеры
- Готовим пакет документов: положение о конфиденциальной информации, уведомление, допсоглашение к ТД
- Разворачиваем сервер и агентов по GPO, настраиваем детекторы, белые списки устройств и блокировки
- Ставим регламент алертов: авто-блок, недельный дайджест руководителю, критические — в Telegram
- Ведём систему на поддержке: разбор инцидентов, чистка ложных срабатываний, обслуживание базы

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Staffcop Enterprise, «Требования: сервер и базы данных» (RAM, NVMe 1500 МБ... (docs.staffcop.ru — 5.8)

02 Staffcop Enterprise, «Тихая установка Windows-агента»: параметры msiexec,... (docs.staffcop.ru — 5.8)

03 Staffcop Enterprise, «Конфигурация: Устройства» и кейс «Контроль USB-накоп... (docs.staffcop.ru — 5.8)

04 Staffcop Enterprise, «Конфигурация: Интернет» — веб-трафик, веб-формы, бло... (docs.staffcop.ru — 5.8)

05 Staffcop Enterprise, «Исключения антивируса» и «Конфигурация: Защита агент... (docs.staffcop.ru — 5.8)

06 Staffcop Enterprise, «Создание архивной базы данных» и «Автоочистка» (docs.staffcop.ru — 5.8)

07 Configure endpoint DLP settings, Microsoft Purview: sensitive service doma... (learn.microsoft.com — 2026)

08 Advanced Audit Policy: Audit PNP Activity (6416) и ADMX_RemovableStorage P... (learn.microsoft.com — 2026)

09 Шаблон ITfresh: карта каналов утечки и регламент трёх уровней алертов (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.