Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Контроль ПК сотрудников: законно по ТК РФ и 152-ФЗ

Наша методология: ЛНА и подписи — до установки агента, аудит Windows — после

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Заказчик хочет видеть, что происходит на рабочих машинах: утечки клиентских баз, работа «налево» с корпоративной лицензии, слив файлов на флешку. Мы делаем так, чтобы данные годились как доказательство в трудовом споре и не создавали состава по ст. 137-138 УК РФ. Контроль для нас — связка: ЛНА и подпись работника, сбор в объявленном объёме, срок хранения и доступ к записям.

Почему это важно бизнесу

- Без ЛНА и подписи работника данные мониторинга суд не примет как доказательство
- Увольнение за разглашение тайны — пп. «в» п. 6 ч. 1 ст. 81 ТК РФ: нужна чистая процедура
- Логи активности — персональные данные: их нельзя хранить бессрочно и «всем админам»
- Чтение личной почты и мессенджеров работника — риск уголовной статьи, а не штрафа
- Режим коммерческой тайны без описи сведений и расписок юридически не существует

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

ст. 22 ТК

Право работодателя требовать соблюдения ПВТР — основание для контроля служебной техники

ТК РФ, ст. 22

ст. 68 ТК

Ознакомление с ПВТР и локальными актами под роспись ДО подписания трудового договора

ТК РФ, ст. 68 ч. 3

гл. 14 ТК

Обработка персданных работника: ст. 86-90 — объём, передача, права работника

ТК РФ, ст. 86-90

30 дней

Срок уничтожения ПДн после достижения цели или отзыва согласия, если иное не в договоре

152-ФЗ, ст. 21 ч. 3 и ч. 5

90 дней

Наш штатный срок хранения рядовых логов активности; год — по инцидентам ИБ

Политика ИБ заказчика

4688

Event ID создания процесса в журнале Security — база доказательной хронологии

learn.microsoft.com: Audit Process Creation

РЕАЛИЗАЦИЯ 1 ИЗ 3

Бухгалтерский аутсорсинг, 8 рабочих мест: контроль без DLP

Что настраиваем

Аутсорсинговая бухгалтерия, домен AD, один терминальный сервер с 1С, работа с реквизитами и первичкой десятков клиентов

Как мы это делаем

1. Неделя 1: опись сведений, составляющих коммерческую тайну, положение о КТ, расписки по ст. 11 98-ФЗ
2. Неделя 1: правим ПВТР и политику ИБ — перечисляем поимённо: URL, входы-выходы, запуск процессов, USB, печать
3. Неделя 2: ознакомление под подпись, лист ознакомления в личное дело, отдельный инструктаж на 20 минут
4. Неделя 2: включаем расширенный аудит через GPO — Audit Logon/Logoff, Audit Process Creation (с командной строкой), Audit File System по SACL
5. Неделя 3: пересылка событий на сборщик, ретенция 90 дней, доступ к архиву — только у двух названных в приказе лиц

РЕЗУЛЬТАТ

Заказчик получил хронологию по каждому рабочему месту без единого скриншота и без покупки DLP. Первый разбор показал ведение сторонних клиентов с корпоративной лицензии 1С в рабочее время — вопрос закрыли соглашением сторон: доказательства собраны в объёме, объявленном работникам заранее.

КЛЮЧЕВОЙ НЮАНС

Для компании до 10 рабочих мест штатного аудита Windows и логов прокси достаточно. Дорогая система не компенсирует отсутствие ЛНА, а бесплатный аудит при наличии ЛНА — работает.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Медклиника: DLP там, где утечка стоит дороже лицензии

Что настраиваем

Клиника на 22 сотрудника, персданные пациентов специальной категории, регистратура с общим доступом к картотеке

Как мы это делаем

1. Определяем цель обработки: защита персданных пациентов; фиксируем её в политике и в уведомлении в Роскомнадзор
2. Готовим согласия и уведомления работникам с точным перечнем контролируемых каналов: съёмные носители, печать, корпоративная почта
3. Внедряем агент DLP только на корпоративные машины; личные устройства исключаем из периметра, доступ к контуру — с терминала
4. Разграничиваем роли: оператор видит события, содержимое перехвата открывает только комиссия по инцидентам
5. Регламент реагирования: акт, письменное объяснение в 2 рабочих дня по ст. 193 ТК РФ, взыскание в месячный срок со дня обнаружения

РЕЗУЛЬТАТ

Через квартал система зафиксировала копирование картотеки на съёмный носитель. Материалы легли в дисциплинарную процедуру без оспаривания: работник заранее расписался за перечень контролируемых каналов, а срок и порядок затребования объяснения были соблюдены.

КЛЮЧЕВОЙ НЮАНС

DLP оправдана, когда цена утечки выше стоимости лицензии и сопровождения. Но её выводы становятся доказательством только вместе с корректной процедурой по ст. 192-193 ТК РФ.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Юрфирма: снимаем запрос на кейлоггер, ставим периметр

Что настраиваем

Юридическая практика, 12 человек, адвокатская тайна клиентов, изначальный запрос — перехват всей переписки и нажатий клавиш

Как мы это делаем

1. Отказываемся от перехвата личных каналов: тайна связи защищена ст. 23 Конституции РФ и ст. 138 УК РФ
2. Переносим контроль на периметр: журнал прокси и межсетевого экрана — адреса, объём трафика, время, без содержимого
3. Закрываем каналы GPO: запрет записи на съёмные носители, белый список ПО, блокировка личных облачных хранилищ
4. Корпоративную почту читаем только на своём сервере и только по прописанной в политике процедуре с актом
5. Проводим встречу с коллективом: объясняем через обязанность защищать данные клиентов, а не через недоверие

РЕЗУЛЬТАТ

Компания получила контроль каналов утечки без сбора содержимого личной переписки. Юридические риски снялись полностью: собираются только метаданные служебной активности, объявленные работникам, а сам инструмент не создаёт состава по ст. 137 и 138 УК РФ.

КЛЮЧЕВОЙ НЮАНС

Часто запрос «поставьте кейлоггер» закрывается ограничением каналов, а не тотальным перехватом. Запрет записи на USB предотвращает утечку, а перехват — только фиксирует её постфактум.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Софт поставили, документов нет**
  Сбор данных без ЛНА и подписи работника — обработка без основания; материалы в споре обесцениваются, а сам сбор оспорим.

- **Размытая формулировка в политике**
  «Контроль компьютерной активности» не годится: нужен закрытый перечень — URL, входы, процессы, USB, печать, корпоративная почта.

- **Чтение личной почты и мессенджеров**
  Тайна переписки защищена ст. 23 Конституции РФ и ст. 138 УК РФ независимо от того, чьё оборудование использовал работник.

- **Агент на личном ноутбуке**
  Установка контроля на устройство работника без отдельного письменного соглашения — выход за пределы служебного отношения.

- **Логи хранятся вечно**
  152-ФЗ требует хранить ПДн не дольше целей (ст. 5) и уничтожить их по достижении цели (ст. 21); бессрочный архив скриншотов — нарушение.

- **Доступ к записям у всех админов**
  Без приказа о допущенных лицах и разграничения ролей утечка из самой системы контроля становится вопросом времени.

- **Нет режима коммерческой тайны**
  Без перечня сведений, грифа и расписок по ст. 10-11 98-ФЗ увольнение за разглашение разваливается в суде.

- **Нарушен порядок взыскания**
  Ст. 193 ТК РФ: два рабочих дня на объяснение, акт при отказе, месяц со дня обнаружения проступка — пропуск обнуляет процедуру.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Пункт о контроле служебной техники в ПВТР и трудовом договоре
- Лист ознакомления под подпись у каждого работника, копия в личное дело
- Журнал прокси или межсетевого экрана: адреса, время, объём — без содержимого
- Приказ о лицах, допущенных к просмотру записей мониторинга

НОРМАЛЬНО

- Политика ИБ с закрытым перечнем контролируемых каналов и сроками хранения
- Расширенный аудит Windows через GPO: входы, запуск процессов, доступ к файлам
- Централизованный сбор событий с ретенцией 90 дней и год по инцидентам
- Режим коммерческой тайны: перечень сведений, гриф, расписки работников

ХОРОШО

- DLP на корпоративных машинах с ролевым доступом к содержимому перехвата
- Комиссия по инцидентам и регламент по ст. 192-193 ТК РФ с формами актов
- Ежегодный пересмотр ЛНА и повторное ознакомление при изменении объёма
- Плановое уничтожение записей по акту и контроль срока ответственным лицом

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- ☐ Определена и записана цель обработки: защита данных клиентов, а не «наблюдение за людьми»
- ☐ ПВТР, политика ИБ и трудовой договор содержат одинаковый перечень контролируемых каналов
- ☐ Каждый работник расписался за ознакомление до включения сбора данных, а не после
- ☐ Оформлен режим коммерческой тайны: перечень сведений, гриф, расписки по 98-ФЗ
- ☐ Подано уведомление об обработке персданных в Роскомнадзор и оно актуально
- ☐ Личные почта, мессенджеры и облака работника из объёма контроля исключены явно
- ☐ Личные устройства не контролируются либо покрыты отдельным письменным соглашением
- ☐ Прописаны сроки хранения записей и назначен ответственный за их уничтожение
- ☐ Доступ к архиву мониторинга разграничен приказом, действия операторов журналируются
- ☐ Есть регламент реагирования: акт, объяснение в 2 рабочих дня, решение в месячный срок

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).

- Собираем комплект ЛНА под ваш бизнес: ПВТР, политика ИБ, положение о коммерческой тайне
- Проводим ознакомление персонала и оформляем листы подписей до технического внедрения
- Настраиваем аудит Windows через GPO, сбор событий, ретенцию и разграничение доступа
- Подбираем уровень средств: от журналов периметра до DLP — по реальной цене утечки
- Сопровождаем инцидент: выгрузка доказательств, акты, процедура по ст. 193 ТК РФ

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 Трудовой кодекс РФ, ст. 22, 68, 81, 86-90, 192-193 (pravo.gov.ru — 2026)

02 Конституция РФ, ст. 23 и 24 — тайна связи и частная жизнь (pravo.gov.ru — 2020)

03 152-ФЗ «О персональных данных», ст. 5, 6, 9, 18.1, 21 (pravo.gov.ru — 2026)

04 98-ФЗ «О коммерческой тайне», ст. 10 и 11 — меры охраны (pravo.gov.ru — 2026)

05 149-ФЗ «Об информации», ст. 6 — права обладателя информации (pravo.gov.ru — 2026)

06 УК РФ, ст. 137 и 138 — частная жизнь и тайна переписки (pravo.gov.ru — 2026)

07 Advanced security audit policy settings: Audit Process Creation (learn.microsoft.com — 2026)

08 Приказ Роскомнадзора от 28.10.2022 № 179 о подтверждении уничтожения ПДн (pravo.gov.ru — 2022)

09 Событие 4688: A new process has been created — Windows Security (learn.microsoft.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.