Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

152-ФЗ для офиса до 50 РМ: защита без штрафов РКН

Как мы собираем документы и закрываем технические дыры по 152-ФЗ за одну-две недели

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Малый офис обрабатывает ПДн сотрудников и клиентов, но без пакета документов и базовых техмер беззащитен перед проверкой РКН и перед утечкой. Банки требуют подтверждение соответствия 152-ФЗ для эквайринга, а внеплановая проверка приходит по жалобе бывшего сотрудника. Мы закрываем оба фронта — документальный контур и технические меры под УЗ-4 — чтобы проверка прошла спокойно, а инцидент не разорил компанию.

Почему это важно бизнесу

- Оборотный штраф за повторную утечку — 1-3% годовой выручки, не менее 20 млн ₽: для компании на 20-30 человек это конец бизнеса
- Банки требуют подтверждение соответствия 152-ФЗ перед открытием эквайринга — отказ бьёт по приёму платежей внезапно
- Внеплановая проверка приходит по жалобе бывшего сотрудника или клиента в любой момент, и к ней обычно никто не готовится
- Утечка из-за шифровальщика или сгоревшего диска — такой же инцидент с ПДн, как кража, с теми же сроками и штрафами

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

УЗ-4

базовый уровень защищённости ИСПДн для типового офиса (бухгалтерия, юрфирма)

ПП РФ №1119

24 ч

срок первичного уведомления РКН об инциденте с ПДн после обнаружения

152-ФЗ, ч.3.1 ст.21 (с 01.09.2022)

≥8 / 90 дн

минимальная длина пароля и период смены в доменной парольной политике

GPO Default Domain Policy

5

порог блокировки учётной записи после неудачных попыток входа

наш стандарт (GPO)

3-2-1

схема резервного копирования, которую мы закладываем против шифровальщика

наш стандарт

КС1

класс СКЗИ КриптоПро CSP для обмена с госорганами и банковской отчётности

КриптоПро CSP 5.0 R3

РЕАЛИЗАЦИЯ 1 ИЗ 3

Документальный контур ПДн и уведомление РКН

Что настраиваем

юрлицо или ИП до 50 РМ: политика, приказы, согласия, реестр операторов на pd.rkn.gov.ru

Как мы это делаем

1. Готовим Положение об обработке ПДн и приказ о назначении ответственного, публикуем политику конфиденциальности на сайте со ссылкой из формы сбора данных
2. Подаём уведомление о начале обработки через pd.rkn.gov.ru по форме Приказа РКН №180 от 28.10.2022 — с УКЭП или через Госуслуги
3. Ставим на сайте отдельный, не пред-проставленный чекбокс согласия со ссылкой на политику; собираем письменные согласия сотрудников по ст.9
4. Заводим журнал учёта согласий и сроков хранения, удаляем ПДн по достижении цели обработки (ст.5 и ст.21 152-ФЗ)

РЕЗУЛЬТАТ

Пакет, который проверяющий РКН запрашивает первым, готов заранее: документальную часть проверки проходим без замечаний, а банк получает подтверждение соответствия для эквайринга.

КЛЮЧЕВОЙ НЮАНС

Смотрим в ст.22 152-ФЗ: исключения из обязанности уведомлять о начале обработки сузили с 01.09.2022 — позиция «мы не Сбербанк, нас не касается» больше не работает даже для ИП.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Технические меры для УЗ-4 по Приказу ФСТЭК №21

Что настраиваем

домен Windows Server, 15-50 PM: антивирус, разграничение доступа, парольные GPO, периметр

Как мы это делаем

1. Определяем уровень защищённости по ПП №1119 (типовой офис — УЗ-4) и берём базовый набор мер Приказа №21: ИАФ, УПД, АВЗ, РСБ, ОЦЛ
2. Разворачиваем Kaspersky Endpoint Security 12.x под KSC 15.x (или Dr.Web ESS) с единой консолью и контролем статуса антивирусных баз
3. Через Default Domain Policy задаём длину пароля ≥8, смену раз в 90 дней, блокировку после 5 попыток; снимаем у пользователей права локального админа
4. Закрываем RDP 3389 с периметра, оставляем доступ извне только через VPN; в 1С разграничиваем видимость базы по менеджерам

РЕЗУЛЬТАТ

Минимальный, но проверяемый набор мер: консоль показывает, где не встали обновления, а открытый порт 3389 — первое, что мы закрываем в день аудита.

КЛЮЧЕВОЙ НЮАНС

Для УЗ-4 Приказ №21 не требует закрывать все 15 групп сертифицированными СЗИ — не покупаем DLP за полмиллиона, берём базовый набор и адаптируем под реальную ИСПДн.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Регламент реагирования на утечку: 24 и 72 часа

Что настраиваем

процедура на одну страницу плюс аудит и логи на сервере как доказательная база масштаба

Как мы это делаем

1. Прописываем роли: кто фиксирует инцидент, кто в течение часа эскалирует, кто готовит и подаёт уведомление в РКН
2. Настраиваем аудит на Windows Server — вход в систему и доступ к файловым шарам в Security-журнале, плюс централизованный сбор логов
3. Первичное уведомление подаём через форму pd.rkn.gov.ru/incidents в течение 24 часов, итоговый отчёт с причинами и мерами — в течение 72 часов
4. Инцидент шифровальщика или потерю диска трактуем как инцидент с ПДн: восстанавливаем из бэкапа Veeam или Windows Server Backup по схеме 3-2-1

РЕЗУЛЬТАТ

Компания узнаёт об утечке сразу, а не через месяц, когда сроки уже прошли: логи позволяют показать реальный, часто небольшой масштаб и не получить максимальный штраф.

КЛЮЧЕВОЙ НЮАНС

За нарушение срока уведомления — отдельный штраф для юрлиц 1-3 млн ₽ (ч.11 ст.13.11 КоАП, с 30.05.2025); сами сроки 24 и 72 часа действуют ещё с 01.09.2022 (ч.3.1 ст.21 152-ФЗ).

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Уверенность «нас это не касается»**
  Размер бизнеса не важен: ИП на 3 человека — тоже оператор ПДн. Уведомление о начале обработки обязательно почти всем с 01.09.2022.

- ✕ **Форма на сайте без чекбокса согласия**
  Сбор ПДн через веб-форму без отдельного согласия и ссылки на политику — прямое нарушение ст.9, всплывает при любой проверке за минуту.

- ✕ **Согласия хранятся «в папке»**
  Согласия собираются, но найти по конкретному субъекту нереально. Заводим журнал учёта с привязкой к ФИО, дате и цели обработки.

- ✕ **Открытый RDP 3389 наружу**
  Порт торчит в интернет «чтобы работать из дома» — это брутфорс и вход шифровальщика. Закрываем с периметра, доступ только через VPN.

- ✕ **Общий пароль на базу данных**
  Вся компания заходит под одним «1234», а в политике «доступ у трёх человек» — расхождение документа и факта РКН фиксирует сразу.

- ✕ **Данные хранятся бессрочно**
  ПДн уволенных и бывших клиентов лежат в базе годами. Ст.5 и 21 требуют удалять по достижении цели — настраиваем сроки хранения.

- ✕ **Модель угроз за 300к или полный игнор**
  80-страничный документ для 15 РМ — деньги в трубу, как и полный игнор. Для УЗ-4 нужен простой документ по ПП №1119 и Приказу №21.

- ✕ **Defender по умолчанию без консоли**
  Не видно, где не встали обновления баз. Ставим управляемый АВЗ (KES/Dr.Web) с центральной консолью — это группа мер АВЗ Приказа №21.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Положение об обработке ПДн, приказ об ответственном, согласия по ст.9
- Уведомление о начале обработки подано через pd.rkn.gov.ru
- Закрыт RDP 3389 наружу, убраны общие пароли к базам данных

НОРМАЛЬНО

- Модель угроз и УЗ по ПП №1119, базовый набор мер Приказа ФСТЭК №21
- Управляемый антивирус (KES/Dr.Web) с единой консолью на всех РМ
- Парольная GPO ≥8/90 дн/блокировка 5, без прав локального админа
- Регламент реагирования на инцидент (24/72 ч) на одну страницу

ХОРОШО

- Аудит и сбор логов на сервере как доказательная база масштаба утечки
- Бэкапы Veeam/WSB по схеме 3-2-1 с проверкой восстановления
- КриптоПро CSP 5.0 (КС1) и ГОСТ-TLS для отчётности с госорганами
- Ежегодная сверка пакета документов с реальными процессами

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Подано ли уведомление о начале обработки ПДн в РКН через pd.rkn.gov.ru?
- [ ] Есть ли Положение об обработке ПДн и приказ о назначении ответственного за ПДн?
- [ ] На сайте форма сбора данных с не пред-проставленным чекбоксом и ссылкой на политику?
- [ ] Определён ли уровень защищённости ИСПДн по ПП №1119 (для типового офиса — УЗ-4)?
- [ ] Стоит ли на всех РМ управляемый антивирус с центральной консолью (KES/Dr.Web)?
- [ ] Задана ли парольная GPO: длина ≥8, смена 90 дн, блокировка после 5 попыток?
- [ ] Закрыт ли RDP 3389 с периметра, а доступ извне идёт только через VPN?
- [ ] Есть ли регламент реагирования на утечку со сроками 24 и 72 часа?
- [ ] Настроен ли аудит и сбор логов на сервере для доказательства масштаба инцидента?
- [ ] Удаляются ли ПДн уволенных и бывших клиентов по достижении цели обработки?

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 пакет документов по ПДн и подаём уведомление в РКН за одну-две недели
- Определяем уровень защищённости и модель угроз по ПП №1119 без 80-страничной воды
- Разворачиваем управляемый антивирус, парольные GPO и разграничение доступа в 1С
- Закрываем периметр: убираем открытый RDP, поднимаем VPN, настраиваем бэкапы 3-2-1
- Пишем регламент реагирования 24/72 ч и настраиваем логи как доказательную базу

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

01 152-ФЗ «О персональных данных» (ст.9, 18.1, 19, 21, 22) (pravo.gov.ru — ред. 2025)

02 ПП РФ №1119 — уровни защищённости ПДн в ИСПДн (pravo.gov.ru — 2012)

03 Приказ ФСТЭК России №21 — состав и содержание мер защиты (fstec.ru — 2013)

04 Приказ РКН №180 — форма уведомления об обработке ПДн (rkn.gov.ru — 2022)

05 Портал персональных данных: реестр операторов, форма инцидента (pd.rkn.gov.ru — 2025)

06 КриптоПро CSP 5.0 — классы КС1/КС2/КС3, ГОСТ Р 34.10-2012 (cryptopro.ru — 5.0 R3)

07 Kaspersky Endpoint Security / KSC — сертификаты ФСТЭК (support.kaspersky.ru — 12.x/15.x)

Основано на официальной документации продуктов и нашей практике внедрения.