SOFTLEX · ЧЕК-ЛИСТ ДЛЯ ВЛАДЕЛЬЦЕВ БИЗНЕСА

Персональные данные: 12 точек, где может произойти утечка

Как быстро проверить, где в компании хранятся персональные данные, кто имеет к ним доступ и какие организационные и технические дыры чаще всего приводят к утечкам.

Чек-лист для первичной самопроверки и выявления зон риска.
Не заменяет юридический аудит и проверку соответствия требованиям законодательства.

Блок 1. Где находятся персональные данные

Четыре пункта, которые помогают понять реальный периметр данных. Если вы не знаете, где лежат ПД, вы не можете нормально контролировать их защиту.

☐ 1. Составлен список всех мест хранения ПД

Зафиксируйте, где находятся данные сотрудников, клиентов и кандидатов: 1С, CRM, HR-системы, облачные диски, почта, мессенджеры, ноутбуки, серверы, резервные копии и тестовые стенды.

Почему важно: *данные часто оказываются не только в основной системе, но и в десятках выгрузок, копий и рабочих таблиц.*

☐ 2. Проверены общие папки и ссылки

Проверьте облачные папки и документы с режимом «доступ по ссылке». Уберите публичные ссылки и доступы, которые больше не нужны.

Почему важно: *ссылка может продолжать работать после увольнения сотрудника или передачи файла другому человеку.*

☐ 3. Проверены личные устройства сотрудников

Выясните, хранятся ли базы, выгрузки, сканы документов и другие ПД на личных ноутбуках, телефонах и внешних накопителях.

Почему важно: *после копирования данных на личное устройство компания теряет часть контроля над их хранением и удалением.*

☐ 4. Проверены архивы и резервные копии

Определите, где лежат старые базы и бэкапы, кто имеет к ним доступ и сколько времени они хранятся.

Почему важно: *удаление файла из рабочей системы не означает, что его копий больше нигде нет.*

Блок 2. Кто имеет доступ

Четыре пункта про права сотрудников, подрядчиков и контроль массовых выгрузок.

☐ 5. Права сотрудников соответствуют их задачам

Проверьте, что сотрудник получает доступ только к тем данным и системам, которые нужны ему для работы. Отдельно проверьте административные права.

Почему важно: *чем шире доступ, тем больше данных может быть скомпрометировано при одной ошибке или компрометации аккаунта.*

☐ 6. Доступы уволенных сотрудников отзываются в день увольнения

Проверьте почту, CRM, облака, VPN, HR-системы, репозитории и другие сервисы. Убедитесь, что нет активных сессий и общих аккаунтов, которыми бывший сотрудник может продолжать пользоваться.

Почему важно: *старый доступ — один из самых простых способов получить доступ к данным без взлома.*

☐ 7. Доступ подрядчиков оформлен и контролируется

Составьте список внешних команд и специалистов, которые получают доступ к ПД. Проверьте договор поручения обработки / договор с условиями об обработке ПД, объём доступа, место хранения данных и порядок его прекращения.

Почему важно: *передача обработки подрядчику не означает, что бизнес перестаёт отвечать за организацию процесса обработки.*

☐ 8. Массовые выгрузки из CRM и других систем видны

Проверьте, фиксируются ли крупные экспорты данных: кто выгрузил, когда, сколько записей и из какой системы.

Почему важно: *обычный экспорт может выглядеть как рабочая операция, пока из системы не выгружается вся база.*

Блок 3. Что происходит с данными технически

Четыре пункта, где чаще всего появляются технические дыры: тестовые среды, мессенджеры, защита и реакция на инцидент.

☐ 9. В тестовых средах нет реальных ПД без необходимости

Проверьте, используются ли реальные данные клиентов и сотрудников в тестовой среде. Если используются, настройте обезличивание или замену данных перед загрузкой.

Почему важно: *152-ФЗ требует, чтобы объём обрабатываемых данных соответствовал заявленным целям; для тестов обычно достаточно обезличенных или синтетических данных. Тестовый сервер часто защищён слабее продакшна и может иметь более широкий круг пользователей.*

☐ 10. ПД не пересылаются через личные мессенджеры и неконтролируемые каналы

Определите, отправляют ли сотрудники паспорта, зарплатные ведомости, базы клиентов и другие ПД через личный Telegram, почту или другие каналы вне корпоративного контура, если это не предусмотрено политикой обработки и не обеспечено необходимыми мерами защиты.

Почему важно: *после передачи данных в личный канал компания теряет часть технического контроля над их распространением.*

☐ 11. Критичные системы защищены дополнительными механизмами

Проверьте MFA, разграничение прав, защиту резервных копий, журналирование действий, регулярный пересмотр прав и другие меры для систем, где хранится большой объём ПД.

Почему важно: *одного пароля недостаточно, если через один аккаунт можно получить всю клиентскую или кадровую базу.*

☐ 12. Есть понятный план действий при инциденте

Заранее определите, кто фиксирует инцидент, кому он передаётся, кто отвечает за расследование и подготовку уведомления Роскомнадзору, а также где хранятся необходимые документы и логи.

Почему важно: *при утечке время критично. Искать ответственного и вспоминать процедуру уже после инцидента — плохой сценарий.*

Проверьте: каждый сотрудник должен знать хотя бы одно простое действие — кому сообщить, если он обнаружил утечку или ошибочно отправил ПД не тому человеку.

Как читать результат

• **10–12 пунктов выполнено:** базовый контур контроля есть. Проверьте детали и поставьте регулярную ревизию доступов.

• **7–9 пунктов выполнено:** есть зоны риска. В первую очередь проверьте доступы, увольнения, подрядчиков и тестовые среды.

• **4–6 пунктов выполнено:** персональные данные, скорее всего, уже живут вне полностью контролируемого контура. Начните с инвентаризации и закрытия открытых доступов.

• **0–3 пункта выполнено:** критическая ситуация. Сначала определите, где находятся ПД и кто имеет к ним доступ, затем переходите к техническим и организационным мерам.

Важно: один невыполненный пункт не означает автоматически нарушение закона. Чек-лист нужен для выявления зон риска, которые стоит отдельно проверить с ответственным за ПД и юристом.

Что делать дальше

1. **Пройдите чек-лист с ответственным за персональные данные и IT.** Это поможет увидеть расхождение между формальными документами и тем, как данные реально используются.
2. **Составьте список красных флагов.** В первую очередь закройте публичные ссылки, доступы бывших сотрудников и реальные ПД в тестовых средах.
3. **Проверьте массовые выгрузки.** Определите, кто и когда может скачать большой объём данных из CRM, HR-системы или другого хранилища.
4. **Зафиксируйте процедуру инцидента.** Назначьте ответственных и заранее определите порядок эскалации и подготовки уведомлений регуляторам.
5. **Повторяйте проверку регулярно.** Доступы, подрядчики и системы меняются — чек-лист имеет смысл проходить не один раз.

Приоритеты, если времени мало

Если нужно быстро закрыть самые опасные точки, начните с этих шести:

Сделать в первую очередь:

- Пункт 2: убрать публичные ссылки на файлы с ПД
- Пункт 6: отозвать доступы бывших сотрудников
- Пункт 9: убрать реальные ПД из тестовых сред
- Пункт 10: прекратить передачу ПД через личные каналы

Затем:

- Пункт 8: включить контроль массовых выгрузок
- Пункт 12: назначить ответственного за инциденты и подготовить порядок действий

Нормативная база

- **Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»** — основные требования к обработке и защите персональных данных, включая обязанности оператора и действия при нарушениях.
- **КоАП РФ, ст. 13.11** — административная ответственность за нарушения законодательства о персональных данных, включая специальные составы за неправомерную передачу, предоставление, распространение или доступ к ПД и повторные нарушения.
- **УК РФ, ст. 272.1** — уголовная ответственность за незаконные использование и/или передачу, сбор и/или хранение компьютерной информации, содержащей персональные данные.
- **Федеральный закон от 30.11.2024 № 420-ФЗ** — внес изменения в КоАП РФ, в том числе ввёл специальные составы ответственности за утечки персональных данных.
- **Федеральный закон от 30.11.2024 № 421-ФЗ** — ввёл статью 272.1 УК РФ.

Кто это составил

Softlex — продуктовая ИТ-компания, делаем веб-сервисы, мобильные приложения и интеграции. Наша часть начинается там, где требования к безопасности нужно превратить в работающий цифровой процесс: разграничить доступы, автоматизировать операции с данными, обезличить тестовые среды и убрать лишние ручные выгрузки.

Этот чек-лист предназначен для первичной самопроверки бизнеса и не заменяет юридический аудит или проверку соответствия требованиям законодательства.

Если после чек-листа останутся вопросы по вашему процессу, напишите:
Степан Гуцан, @Stepan_Gutsan · hello@softlex.pro · softlex.pro