

*Как обеспечить
безопасность ПДн и не
стать мемом в глазах
клиентов*



Директор по КБ: Беляев Дмитрий Александрович



Обо мне



➤ТОП-25 CISO России

➤ Более 11 лет в практической ИБ

➤ Имею 3 образования (ИБ, юриспруденция, безопасная разработка)

➤ Имею более 150 сертификатов/дипломов и благодарностей по тематике ИБ

➤ 2хПобедитель в рейтинге ТОП-100 Лидеров ИТ (GlobalCIO) – 2023/2025

➤ Руководил пятью стартапами по ИБ и командой из более 100 человек.

➤ Член клуба 4CIO;

➤ Член клуба GlobaCIO;

➤ Успешный проект: **Айда Гулять**

➤ Основатель клуба [RTCL] [The Club of Russia's Top Cybersecurity Leaders].

➤ Имею за плечами более 90 выступлений на публику суммарной численностью >6000 человек (PHDay Fest, TADVISER, ТБ Форум, Территория Безопасности, CISO Форум, CNews, ITsec, Security Summit, Код ИБ, ТБ, SmartGoPro и т.д)

➤ Амбассадор платформы «Цифровой прорыв» в 2021-2022

➤ Медийный охват >200.000 человек за год

Дмитрий Александрович Беляев
Директор по Кибербезопасности (CISO)



ВАЖНО



При подготовке
данного материала ни
один DPO не
пострадал



Но это не точно...



Современные ИБ-отделы всё чаще становятся героями мемов

— и причиной тому реальные инциденты, которые кажутся абсурдными даже для искусственного интеллекта



ГОД В ЦИФРАХ, КОТОРЫЕ НЕ ПОВЕРИЛ БЫ

ДАЖЕ СНАТГРТ:

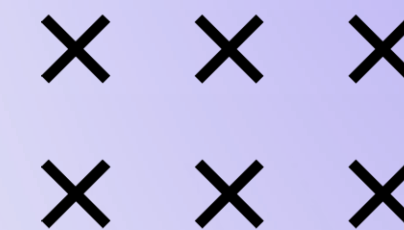
- 1 триллион рублей потерь российского бизнеса от кибератак за 2023-2024 годы;
- 259 утечек баз данных только по данным Роскомнадзора за 2024 год;
- 103 инцидента и около 50 млн записей на конец октября 2025 года;
- 70% успешных атак реализуется политически мотивированными группировками;
- До 50% взломов происходит через подрядчиков.



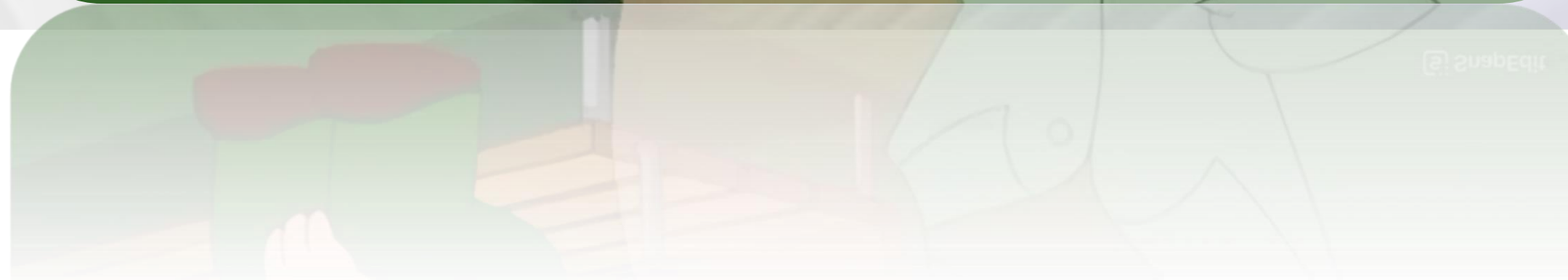
CISO



DPO



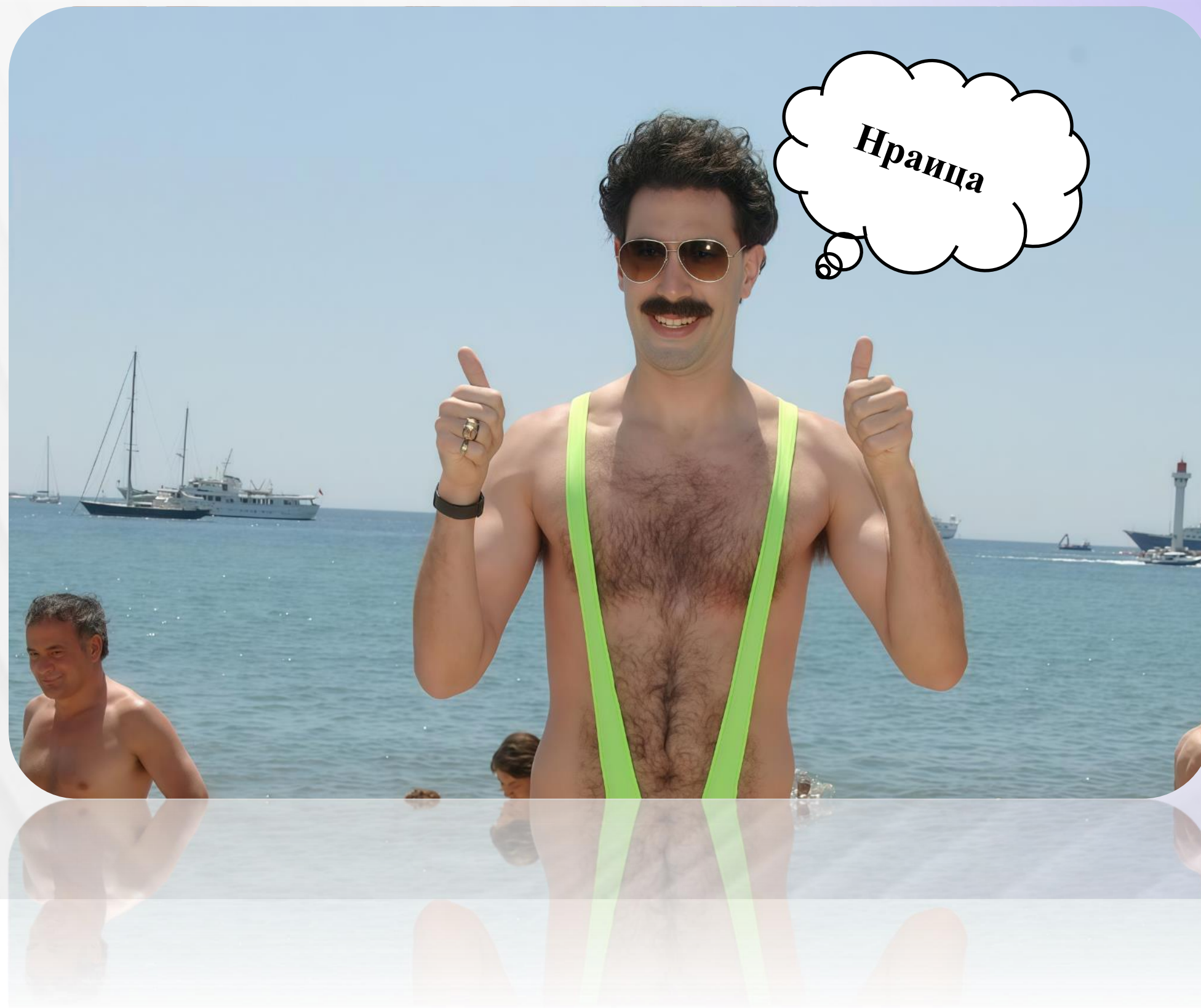
«Раньше мы боялись
хакеров из подвалов.
Теперь они сидят в офисах
наших IT-подрядчиков» —
реальное наблюдение
экспертов Solar 4RAYS



ЧЕЛОВЕЧЕСКИЙ ФАКТОР: КОГДА ИБ-ОТДЕЛЫ СТАНОВЯТСЯ ГЕРОЯМИ АНЕКДОТОВ



- **Яндекс.Еда (2022)** — утечка 49,4 млн записей «из-за недобросовестных действий одного сотрудника». Результат: пользователи получили через суд по 5000 рублей вместо требуемых 100 000
- **20% российских сотрудников** до сих пор имеют доступ к системам с прошлых мест работы
- **«Логическая бомба» в планировщике задач** работала 2 года после первоапрельской шутки — админы просто забыли её удалить





➤ **Производственный комплекс** остановлен

полевой мышью, закоротившей электрощитовую

➤ **Админ** с паролем «Розовая кошечка 777» на

критически важной системе переливания крови

➤ **Телеком-оператор** потерял 90% данных из-за

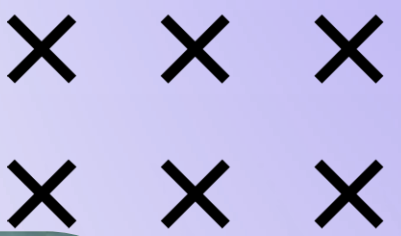
червя, но спасся благодаря забывчивости

айтишников — один сервер «выпал» из поля

зрения хакеров



ЧТО ТАМ ИНТЕРЕСНОГО В СУДЕБНОЙ ПРАКТИКЕ?



➤ Безумие;

➤ Садомия;

➤ Декаданс;

В 2024 году стало известно о 135 утечках персональных данных граждан России, в общей сложности в сеть попали 710 млн записей. За первую половину 2025 года утечек было 35, а общее количество записей в них составило 39 млн.



- **Гордыня:** Инженер «дочки» «Россетей» удаленно со своего ноутбука отключил электроснабжение в 38 населенных пунктах;
- **Алчность:** Консультант мобильной связи нарушила уголовную статью о КИИ, пытаясь выполнить план Tele2;
- **Гнев:** Уволился и удалил файлы. Бывший сисадмин оборонного предприятия оспаривает приговор о воздействии на критическую инфраструктуру;
- **Лень:** Программиста, подделавшего данные о вакцинации в ИТ-системе, осудили на 3,5 года по статье УК о КИИ;
- **Похоть:** И снова про номер телефона. Гражданке Екатеринбурга отказали в иске к газетным изданиям, за размещение её номера телефона в рубрике «досуг», по жалобе на звонки с предложением оказания сексуальных услуг.



Как насчет проработать риски перехода в облачные хранилища?

- Ошибка №1. Недостаточное планирование;
- Ошибка №2. Неправильный выбор облака;
- Ошибка №3. Пренебрежение безопасностью;
- Ошибка №4. Неоптимизированные процессы;
- Ошибка №5. Игнорирование автоматизации;
- Ошибка №6. Отсутствие тестирования аварийного восстановления;
- Ошибка №7. Неучет масштабируемости;
- Ошибка №8. Отсутствие резервного копирования;
- Ошибка №9. Полный перенос данных без фильтрации;
- Ошибка №10. Отсутствие обучения для сотрудников.





Особое внимание — облачным хранилищам, как новой "головной боли" для юристов и комплаенс-отделов



➤ **66% юристов** смущает проблема конфиденциальности в облаках

➤ **52% беспокоят** этические вопросы использования

➤ **47% не знают**, где физически хранятся данные их компании

➤ **35% боятся** персональной правовой ответственности

➤ **31% опасаются** штрафов и санкций



➤ **152-ФЗ** требует локализации персональных данных россиян на территории РФ

➤ **Штрафы выросли** до 500 млн рублей с мая 2025 года

➤ **Облачные провайдеры НЕ** являются операторами ПДн — ответственность лежит на клиенте

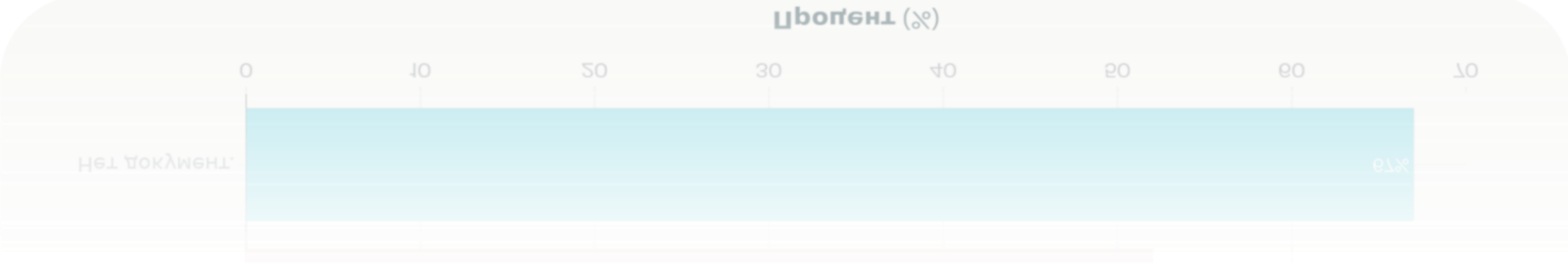
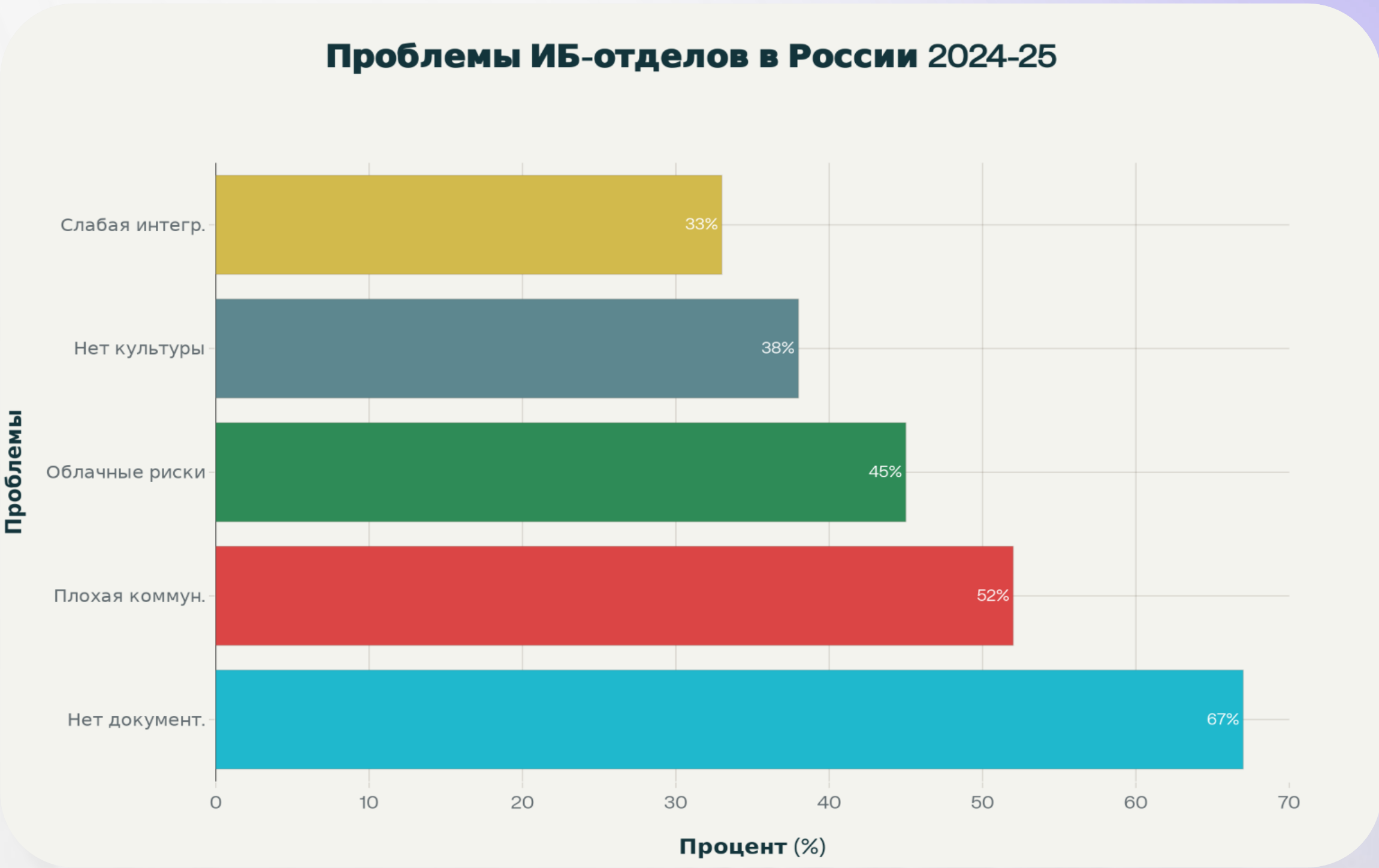
➤ **21% российских компаний** атаковали через облачные хранилища в I квартале 2025 года (рост в 2 раза за год)

➤ **90% атакованных** через облака — представители МСБ

➤ **Лидеры по атакам:** e-commerce (28%), финтех (12%), IT/телеком (по 10%)



Разбор ошибок ИБ-отделов:
отсутствие документирования,
неправильно построенные процессы и
коммуникация, недооценка рисков
облачного хранения.





*67% российских ИБ-отделов не имеют
формализованных процессов
реагирования на инциденты*

*Когда политики ИБ создаются
по шаблонам без привязки к
реальным процессам*

*Ошибка в топе причин
провальных реакций на кибератаки*





➤ **Несо согласованность действий ИТ и ИБ — ошибка**

при реагировании на инциденты

➤ **Время реагирования** увеличивается многократно

из-за отсутствия единого процесса

➤ **52% компаний** страдают от неправильно

построенной коммуникации между отделами



ВАЖНО



- Даже при миллиардных бюджетах на ИБ системы рушатся из-за элементарных уязвимостей (пример «Аэрофлота»)
- Один топ-менеджер с неизменным паролем годами может обнулить всю защиту
- Культура безопасности важнее любого отчета по аудиту



Итоги года

× × ×
× × ×

ГЛАВНОЕ УМЕТЬ

ДЕЛАТЬ ВЫВОДЫ

ДЕЛАТЬ ВЫВОДЫ

- Юристы правы — облачные хранилища действительно создают новые правовые риски, подтвержденные судебной практикой
- ИБ-отделы систематически повторяют одни и те же ошибки в документировании и процессах
- Корпоративная культура решает больше, чем технологии — это доказывают реальные кейсы
- Человеческий фактор остается главной уязвимостью, несмотря на развитие технических средств защиты

- **Рыночная аналитика** фиксирует резкий рост общего объема слитых строк данных (до ~13 млрд за 8 месяцев) при меньшем числе публичных кейсов, что говорит о смещении в сторону очень крупных и «тихих» утечек.
- **Ужесточение административной ответственности**, включая оборотные штрафы до 3% выручки, уже показывает эффект: число выявляемых нарушений в области сбора и обработки данных во втором полугодии заметно ниже, чем в первом.
- **Формальные показатели Роскомнадзора** улучшаются, но объективный объем компрометации данных и уровень угроз растут, поэтому 2025 год — не про «победу над утечками», а про переход к режиму жесткой ответственности и вынужденной зрелости в управлении ПДн.



«Дураки учатся на своих ошибках, а
умные — на чужих»

Теодор Рузвельт



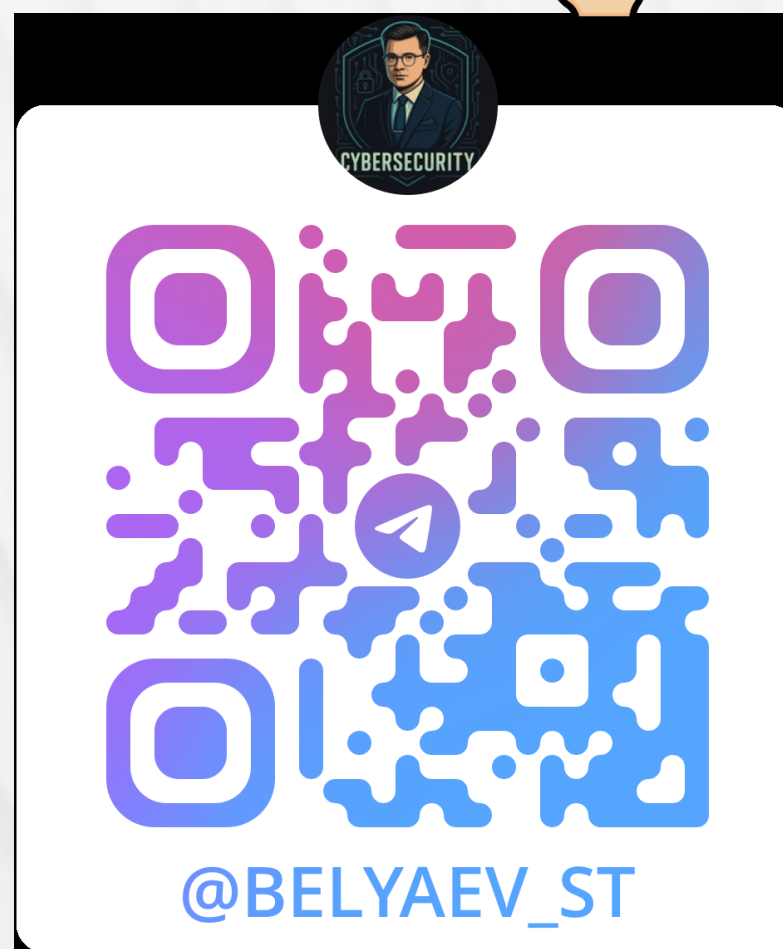
Контакты



**Беляев Дмитрий
Александрович**

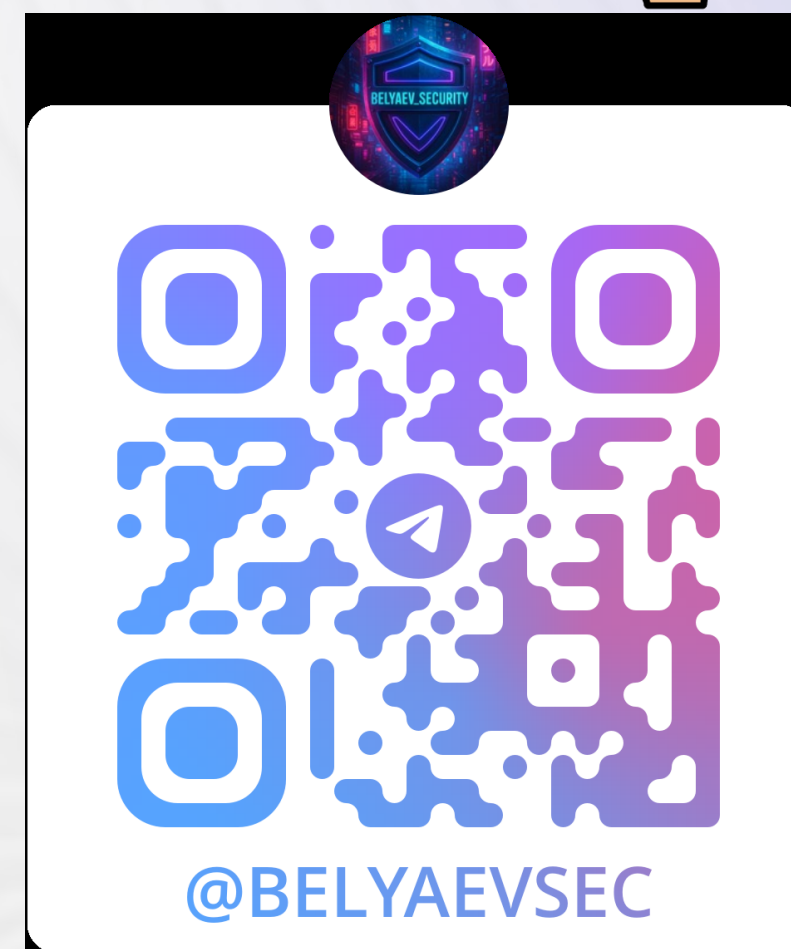
➤ Канал «**Belyaev Security Talks** 🗨»:
Редкий экспертный контент;
Оригинальные статьи; Разборы;
Кейсы; Личная экспертиза;
Менторство.

SUBSCRIBE



➤ Канал «**BELLYAEV_SECURITY**»:
Твой проводник в мир защищенной
информации (новости, статьи,
экспертиза, юмор)

SUBSCRIBE



E-mail: da.belyaev@mail.ru

Сайт: <https://belyaev.expert/>

Телеграм: [@BELLYAEV_SECURITY_bot](https://t.me/BELLYAEV_SECURITY_bot)