



PACIFICA

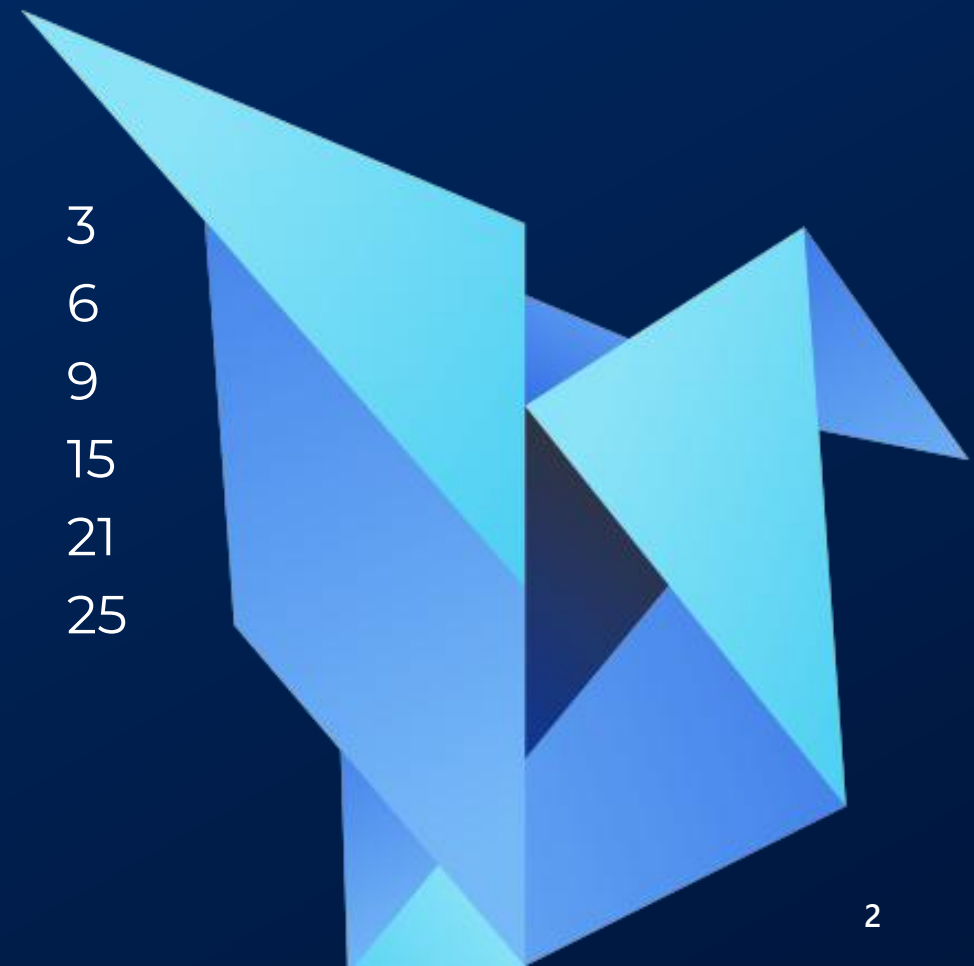
A NOVENTIQ Company

Персональные данные под угрозой: утечки и методы защиты

Максим КАРМЫКОВ – Специалист по кибербезопасности

Содержание

▪ Что такое персональные данные?.....	3
▪ Кибератаки и утечки ПД	6
▪ Ошибки, последствия, реальные примеры.....	9
▪ Методы защиты ПД.....	15
▪ Решения и кейсы PACIFICA	21
▪ Заключение	25



Почему это важно

Сегодня персональные данные – это не просто цифры и буквы. Это ценность, сравниваемая с деньгами или даже с нефтью.

Каждый из нас оставляет цифровой след: в соцсетях, при покупках, при использовании онлайн-сервисов. И любая утечка данных может иметь серьёзные последствия – от финансовых потерь, до утраты доверия клиентов.

По статистике, более **60% компаний хотя бы раз сталкивались с утечкой данных**. Поэтому вопрос защиты информации – это не только про IT, это вопрос репутации и выживания бизнеса.



Что такое персональные данные?

- **Персональные данные** – это любая информация о человеке (субъекте персональных данных), позволяющая прямо или косвенно его идентифицировать. К ним относятся: ФИО, номер паспорта, адрес, дата рождения, сведения о работе, здоровье, а также биометрические данные, такие как фотография или отпечатки пальцев.
- Отличие от **конфиденциальной информации** в том, что персональные данные всегда связаны именно с личностью. Конфиденциальная же информация – более широкий термин.

Категории персональных данных:

- **Общие:** ФИО, дата рождения, место жительства, номер телефона, фотография, электронная почта.
- **Специальные:** политические взгляды, расовая или национальная принадлежность, религиозные и философские убеждения.
- **Биометрические:** отпечатки пальцев, ДНК, слепок голоса, рисунок радужной оболочки глаза.
- **Набор цифр:** номер паспорта или удостоверения личности, номер банковского счета и карты, ИИН.



Рост количества кибератак и утечек данных

- Количество кибератак в мире ежегодно увеличивается на 20-30%.
- Утечки данных становятся всё масштабнее: десятки миллионов записей оказываются в открытом доступе.
- Средний ущерб от инцидента безопасности для компании превышает 4 млн долларов (по данным IBM).
- Основные причины: фишинг, слабые пароли, ошибки сотрудников, уязвимости в программном обеспечении.
- Тренд последних лет – рост кибератак на государственные структуры, банки и критическую инфраструктуру.

Основные угрозы безопасности данных

- **Хакерские атаки:** взломы баз данных, кража логинов и паролей.
- **Фишинг и социальная инженерия:** когда жертву обманывают, заставляя самостоятельно раскрыть данные.
- **Внутренние утечки:** ошибки или действия сотрудников.
- **Недостаточная защита сервисов:** слабые пароли, отсутствие шифрования.



Типовые сценарии кибератак

- **Фишинг**

Сотрудник получает письмо от «банка» или «коллеги», открывает вложение → вирус устанавливается → атакующий получает доступ к корпоративной почте и документам.

- **Утечка через сотрудника**

Менеджер скачивает клиентскую базу на флешку для «удобства работы из дома» → флешка теряется → данные оказываются в открытом доступе.

- **Атака через подрядчика**

Поставщик подключается к сети компании по VPN → его учетная запись скомпрометирована → злоумышленник получает доступ к внутренним системам компании.

- **Социальная инженерия**

Звонок «от ИТ-службы»: у сотрудника запрашивают пароль для проверки → учетная запись перехвачена → происходит кража данных и денег.

- **Для компаний:** финансовые потери, штрафы, судебные иски.
- **Для клиентов:** мошенничество, кража личности, потеря денег.
- **Для бренда:** падение доверия и репутационный удар.

Например, в последние годы многие крупные компании сталкивались с громкими утечками, и восстановление доверия их клиентов занимало годы.

Ошибки компаний при защите данных

- Ставка только на антивирус
- Игнорирование внутренних рисков
- Отсутствие обучения персонала
- Недооценка регуляторных требований
- Фрагментарная защита
- Слишком широкий доступ по умолчанию



Поведение пользователей – главный риск!

- **80% утечек данных** связаны с человеческим фактором.
- Сотрудники используют **слабые** или **одинаковые пароли**.
- Пересылают рабочие документы через **личную почту** и **мессенджеры**.
- Открывают **фишинговые письма** и **вложения**, не проверяя отправителя.
- Часто нарушают правила безопасности **из-за спешки** или **удобства**.

Даже самые современные технологии не работают без обучения сотрудников и строгой корпоративной политики безопасности.

Реальные случаи утечек ПД в Мире

- **Mother of All Breaches (MOAB)** – *январь 2024*
Крупнейшая утечка в истории: 26 млрд записей, собранных из множества источников (Tencent QQ, Weibo, Myspace и др.).
- **National Public Data** – *январь 2024*
2,9 млрд записей, включая адреса, номера социального страхования и другую личную информацию. Утечка у американского брокера данных.
- **Alibaba Cloud** – *июль 2022*
1,1 млрд записей. Утечка через облачный сервис: имена, ID, телефоны, адреса, сведения о судимостях.
- **LinkedIn** – *июнь 2021*
700 млн профилей пользователей выставлены на продажу: имена, e-mail, телефоны и другая контактная информация.

Реальные случаи утечек ПД в Казахстане

- **Утечка данных 16,3 млн граждан** (*июнь 2025*)

Это одна из крупнейших утечек ПД в истории Казахстана.

- **Утечка из микрофинансовой платформы** (*март 2024*)

Свыше 2 миллионов записей клиентов, включая казахстанцев, а также данные по России, Филиппинам и Вьетнаму – были обнаружены в открытом доступе.

- **Прецедент с ГТС** (*2021-2022*)

Выявлен несанкционированный доступ в инфраструктуру операторов связи, ЕНПФ и Air Astana. Причиной стала слабая защита в ГТС; инцидент расследуется КНБ.

```
KZ_Leak cat leak_summary.md
# Утечка данных: автоматический анализ

- Дата анализа: **2025-06-16 11:33:43**
- Исходный файл: **Жители Казахстан 16kk.csv**
- Общее количество записей: **16,302,107**
- Уникальных ИИН: **15,851,699**
- Уникальных номеров телефонов: **16,901,555**

## 🏠 Топ-20 самых популярных фамилий

| № | Фамилия | Кол-во |
|---|---|---|
| 1 | СЕРІК | 34,476 |
| 2 | АХМЕТОВА | 31,112 |
| 3 | АХМЕТОВ | 26,180 |
| 4 | КИМ | 26,125 |
| 5 | МАРАТ | 22,965 |
| 6 | АМАНГЕЛДІ | 19,931 |
| 7 | БОЛАТ | 19,239 |
| 8 | МҰРАТ | 19,196 |
| 9 | ҚАЙРАТ | 18,197 |
| 10 | ОМАРОВА | 18,189 |
| 11 | НҰРЛАН | 16,939 |
| 12 | ОСПАНОВА | 16,524 |
| 13 | ОМАРОВ | 15,294 |
| 14 | ТАЛҒАТ | 15,244 |
| 15 | АЛИЕВА | 14,889 |
| 16 | АСҚАР | 14,599 |
| 17 | СУЛЕЙМЕНОВА | 13,982 |
| 18 | АЛИЕВ | 13,892 |
| 19 | СЕРІКБАЙ | 13,814 |
| 20 | ОСПАНОВ | 13,799 |

KZ_Leak cat leak_summary.md
# Утечка данных: автоматический анализ

- Дата анализа: **2025-06-16 11:33:43**
```

Утечки персональных данных – ближе, чем кажется

- Персональные данные регулярно попадают в открытый доступ.
- Существуют даже **неформальные каналы**, например, Telegram-боты, где любой человек может проверить минимум информации о себе.
- Это показывает **масштаб проблемы**: если такие данные доступны в мессенджере, то представьте, что в руках у киберпреступников.

Адреса

КАЗАХСТАН, АСТАНА ГОРОД, АСТАНА,
УЛИЦА Х [REDACTED]
ЭТ. 7, АДРЕС: [REDACTED]
ЭТАЖ [REDACTED]

РЕСПУБЛИКА: КАЗАХСТАН, ГОРОД
РЕСП.ЗНАЧ.: АСТАНА, УЛИЦА: ЖУМАБАЕВА,
ДОМ: 14

Краткая сводка

Личности

КАРМЫКОВ МАКСИМ [REDACTED] 3

Телефон

77778825033

Email

KARMYKOV@INBOX.RU 60%

KARMYKOVMAKSIM@GMAIL.COM 40%



Методы защиты персональных данных

Как защититься? Здесь важно действовать комплексно:

- **Технические меры:** шифрование, защита каналов связи, резервное копирование.
- **Организационные меры:** контроль доступа, обучение сотрудников, аудит процессов.
- **Правовые меры:** соответствие закону о персональных данных, прозрачная политика конфиденциальности.

Важно понимать: не существует одной «волшебной кнопки». Защита строится системно.

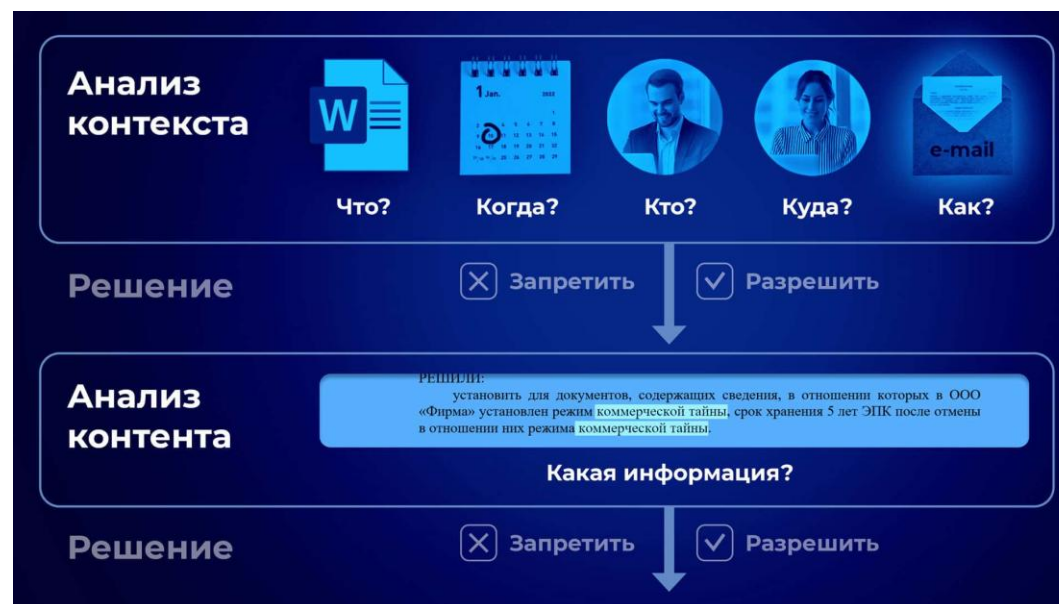
Технические средства защиты персональных данных

- DLP (Data Loss Prevention)
- SIEM (Security Information and Event Management)
- NGFW (Next-Generation Firewall)
- PAM (Privileged Access Management)
- EDR/XDR
- Шифрование и токенизация
- Резервное копирование и BCP
- Системы управления уязвимостями (Vulnerability Management)



Как работает DLP на практике

1. Пользователь пытается отправить данные
2. DLP перехватывает действие пользователя
3. Анализ содержимого
4. Сопоставление с политиками безопасности
5. Реакция системы
6. Уведомление службы безопасности



Технические средства защиты персональных данных

- «Технические меры – это фундамент защиты. Но максимальный эффект достигается только при комплексном подходе: технологии + процессы + обучение»



Роль руководства

- Стратегическое решение
- Выделение бюджета
- Формирование культуры безопасности
- Ответственность за последствия
- Контроль и мониторинг



Что нас ждёт дальше?

- Рост роли искусственного интеллекта – как в кибератаках, так и в защите.
- Ужесточение законодательства: государство требует от компаний больше ответственности.
- Персональные данные становятся новым видом капитала – тем, чем управляют и что защищают наравне с финансами.

Рекомендации для бизнеса и пользователей

Несколько практических советов:

- **Для компаний:** внедряйте политику информационной безопасности, обучайте сотрудников, проводите регулярные проверки.
- **Для пользователей:** используйте сложные пароли, включайте двухфакторную аутентификацию, будьте осторожны с подозрительными письмами и звонками.

РАСІFІСА: Ваша киберзащита от утечек данных

Мы не просто ставим «замки» на ваши системы – мы выстраиваем целостную стратегию защиты, которая:

- **Снижает риски утечек до минимума** – благодаря DLP и PAM мы контролируем доступ и предотвращаем утечки критичных данных.
- **Обеспечивает мгновенное реагирование на атаки** – SIEM и XDR позволяют обнаруживать и реагировать на инциденты в реальном времени.
- **Защищает инфраструктуру 24/7** – NGFW и EDR блокируют сложные кибератаки на периметре и внутри сети.
- **Помогает избежать штрафов и репутационных потерь** – соответствие требованиям регуляторов и защита персональных данных клиентов.

РАСІFІСА – это интегратор, который превращает набор решений в единую экосистему защиты данных под ключ.

PACIFICA: реальный кейс

Задача:

Крупная финансовая компания столкнулась с риском утечки конфиденциальных данных сотрудников и клиентов через почту и мессенджеры.

Решение PACIFICA:

- Внедрение системы **DLP** для контроля всех каналов передачи данных.
- Настройка политик безопасности: запрет отправки персональных данных вне корпоративного контура.
- Обучение сотрудников безопасным методам работы с информацией.

Результат:

- Снижение риска утечки на **80% в первые 3 месяца**.
- Выявлено и предотвращено более **500 попыток несанкционированной передачи данных**.
- Компания избежала штрафов и сохранила доверие клиентов.

О компании



ОБОРОТ
1,5
МЛРД. ₴



2
ОФИСА



БОЛЕЕ
20
АВТОРИЗАЦИЙ
ВЕНДОРОВ



>15 ЛЕТ
НА РЫНКЕ
ИБ



20
СПЕЦИАЛИСТОВ



БОЛЕЕ
100
КЛИЕНТОВ



СООТВЕТСТВИЕ
СТАНДАРТУ
ISO
27001

Направления деятельности



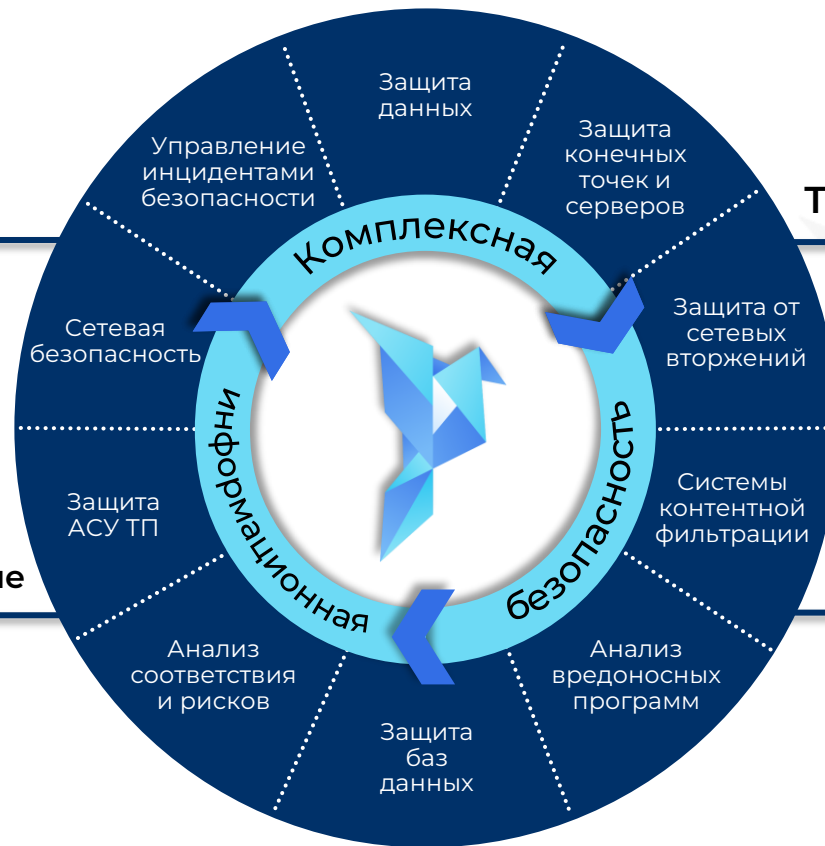
Аудит и консалтинг

- ▶ Подготовка к аудиту в соответствии с международными стандартами (ISO 27001, PA/PCI DSS)
- ▶ Консультации по вопросам обеспечения информационной безопасности



Проектирование и внедрение

- ▶ Проектирование и внедрение систем информационной безопасности
- ▶ Консалтинг построения центра управления инцидентами (ОЦИБ)
- ▶ Защита центров обработки данных (ЦОД)



Техподдержка и аутсорсинг



- ▶ Поддержка и сопровождение систем информационной безопасности (СИБ)
- ▶ Оптимизация ИБ-инфраструктуры, ИБ-аутсорсинг, облачные ИБ-сервисы

Обучение



- ▶ Проведение тренингов и обучающих семинаров менеджеров и технических специалистов ИБ
- ▶ Обучение специалистов ИБ по собственным программам

ТОО «ПАЦИФИКА» предоставляет комплекс решений и услуг, позволяющих нашим клиентам выстраивать систему обеспечения информационной безопасности «с нуля» или оптимизировать существующую

Заключение

Защита персональных данных – это непрерывный процесс. Каждый день появляются новые угрозы, и задача компаний – всегда быть на шаг впереди.

PACIFICA готова быть вашим партнёром в этом.



PACIFICA

A NOVENTIQ Company

