



# PACIFICA

A NOVENTIQ Company

## Внутренние угрозы и способы предотвращения утечки информации

---

Роман ГУГНЯК – Архитектор кибербезопасности

# 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 намеренные действия сотрудников.
- **Недостаточная защита сервисов:** слабые пароли, отсутствие шифрования.



# Кто такие инсайдеры?

**Инсайдер** – это сотрудник, подрядчик или партнер, имеющий доступ к корпоративной информации и ресурсам.

## Типы:

- Злонамеренный
- Халатный/небрежный

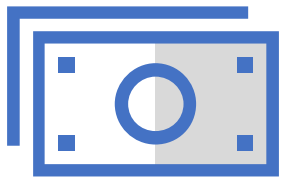
## Основные мотивы:

- Деньги
- Месть
- Идеология
- Шантаж
- Ошибки и незнание правил

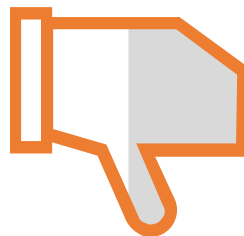


# \$4.92M

Средняя стоимость злонамеренных инсайдерских атак<sup>1</sup>



Дорогостоящие  
штрафы



Испорченная  
репутация



Потеря  
клиентов и  
доходов

# Почему инсайдеры опасны



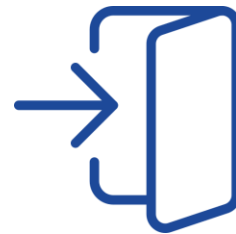
Труднее обнаруживаются



Разнообразие сценариев



Понимает, какие именно данные ценны



Прямой доступ к информационным системам

# Что могут делать инсайдеры и к чему это приводит

## Действия инсайдеров



Кража данных



Удаление или порча данных



Случайная утечка



Запуск ПО, отключение защиты



Передача учетной записи



Подключение устройства к ПК/сети

## Последствия



Утечка коммерческой тайны, потеря конкурентных преимуществ



Остановка бизнес-процессов, нарушение SLA, затраты на восстановление



Заражение сети вредоносным ПО



Использование легитимной УЗ для атак



Удаленное подключение к сети

## Пример 1: Уволенный сотрудник



- **Что произошло:**

Уволенный сотрудник сохранил доступ и за 40 минут удалил 21 ГБ данных (20000 файлов, включая ПО для защиты от ransomware)

- **Ущерб:**

Потеря критичных данных, риски для безопасности

- **Выводы:**

- Немедленно отзывать доступ при увольнении
- Контроль действий в критичных системах

## Пример 2: Coinbase



- **Что произошло:**

Подкуп внешних агентов поддержки → утечка данных <1% пользователей (имена, аккаунты, частичные SSN)

- **Ущерб:**

Попытка вымогательства \$20 млн, репутационные риски

- **Выводы:**

- Жесткий контроль подрядчиков
- Zero Trust и ограничение прав

## Пример 3: Сотрудники банка продают данные клиентов



- **Что произошло:**

Сотрудники крупных банков продавали данные клиентов через Telegram

- **Ущерб:**

Массовые утечки персональных данных, мошенничество

- **Выводы:**

- Мониторинг аномалий и каналов утечки
- Повышение зарплат и мотивации для снижения риска

## Пример 4: Файлы города Даллас удалены из-за ошибки

- **Что произошло:**

Сотрудник удалил 22 ТБ данных (видео и материалы полиции) из-за нарушения процедур

- **Ущерб:**

Потеря доказательств, срыв расследований

- **Выводы:**

- Обучение персонала
- Автоматизация процессов передачи данных





Повышение и сохранение лояльности сотрудников

NDA (соглашение о конфиденциальности)

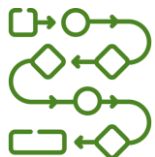


Политика использования корпоративных ресурсов



Обучение сотрудников

Организация рабочих процессов для минимизации рисков ошибок



Разграничение и минимизация прав доступа

# Технические средства защиты – DLP

- Система, контролирующая перемещение конфиденциальных данных внутри компании и за ее пределы.
- **Ключевые функции:**
  - Поиск мест хранения конфиденциальной информации.
  - Мониторинг и блокировка передачи данных по каналам (почта, мессенджеры, облака, USB).
  - Контроль печати, копирования и скриншотов.
  - Анализ контента (по ключевым словам, шаблонам, классификации).
  - Запись действий пользователей для расследования.
- **Как предотвращает инсайдерские атаки:**
  - Злонамеренные действия: блокировка выгрузки баз, копирования на флешки.
  - Небрежность: предупреждения при отправке письма не тому адресату.

# Технические средства защиты – SIEM

- Платформа для сбора, корреляции и анализа событий безопасности из разных источников.
- **Ключевые функции:**
  - Агрегация логов (AD, почта, VPN, DLP, базы данных).
  - Корреляция событий для выявления аномалий.
  - Реагирование в реальном времени (алерты, сценарии).
  - Хранение и анализ истории для расследований.
- **Как предотвращает инсайдерские атаки:**
  - Обнаружение аномального поведения (массовая выгрузка данных, доступ в нерабочее время).
  - Корреляция нескольких признаков (подключение USB + выгрузка файлов + отправка на почту).
  - Интеграция с DLP и UEBA для поведенческого анализа.

# Технические средства защиты – UEBA

- Технология, анализирующая поведение пользователей и систем для выявления аномалий.
- **Ключевые функции:**
  - Профилирование поведения (нормальные паттерны активности).
  - Анализ аномалий (время входа, объем данных, новые ресурсы).
  - Оценка риска (скоринг действий).
  - Интеграция с ИТ, ИБ и бизнес-системами.
- **Как предотвращает инсайдерские атаки:**
  - Обнаружение скрытых угроз (злонамеренные действия под легитимной учеткой).
  - Выявление скомпрометированных учетных записей.
  - Снижение ложных срабатываний за счет контекста.

PACIFICA

A NOVENTIQ Company



## Заключение

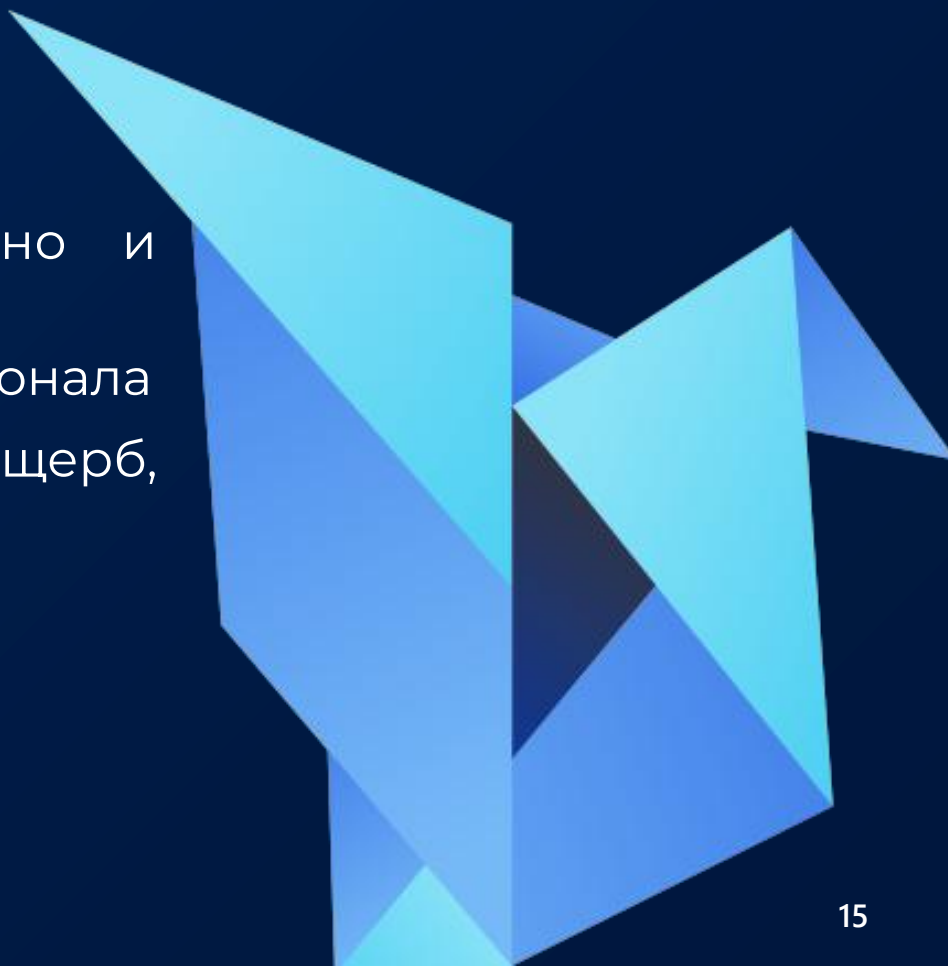
Инсайдеры – это не только злоумышленники, но и небрежные сотрудники

Основные риски: кража и потеря данных, ошибки персонала

Последствия: финансовые потери, репутационный ущерб, юридические санкции

**Защита = комплекс мер:**

- Политики и обучение сотрудников
- Технические решения: DLP, SIEM, UEBA
- Контроль доступа и принцип Zero Trust



PACIFICA

A NOVENTIQ Company

