Архитектура подхода к снижению рисков обработки данных:

вклад каждого в общее дело

Константин Коротнев

Deputy CISO

О чем мы сегодня поговорим?

- Контекст обработки данных, вызовы и риски.
- Подход к снижению рисков обработки данных.
- Роль каждой из заинтересованных сторон при снижении рисков обработки данных.

Анализ контекста обработки данных: вызовы

Большое количество накопленных данных в разных БД и (часто) без определенного владельца

Ограниченная область покрытия средствами защиты и процессами ИБ

Сложности отслеживания и контроля внешних и внутренних потоков данных, в т.ч. между средами, системами, командами, ЮЛ и партнерами

Расползание данных по ИТ-инфраструктуре

Увеличение количества атак (~ + 30%) на компании и количества утечек персональных данных (~60% атак)

Ужесточение ответственности за утечки персональных данных – оборотные штрафы до 500 млн рублей и 3% от оборота

Ответственность за нарушения при организации обработки персональных данных

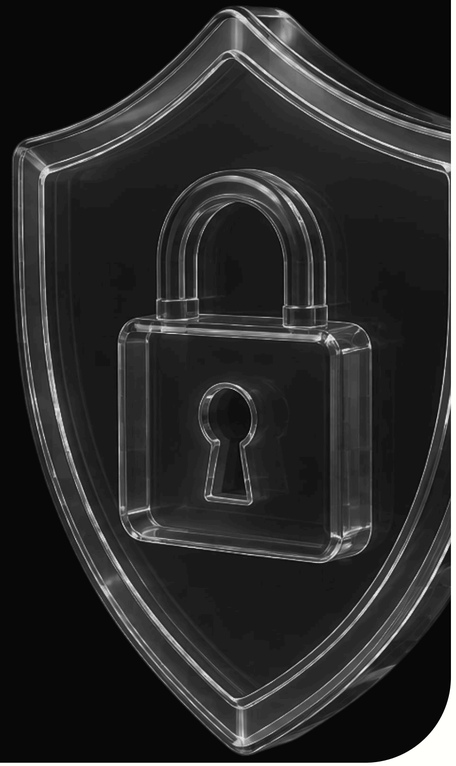
Сложная юридическая структура и большое количество совместно работающих с данными ЮЛ в группах компаний

Критическая зависимость бизнеса от транзакционной и аналитической обработки ПДн и обмена ими с партнерами и подрядчиками

Сложность ИТ-инфраструктуры и слабости в инвентаризации ИТ-активов, используемых для хранения и обработки данных и потоков данных

Риски при обработке персональных данных

Риски утечки персональных данных



Оборотные штрафы
до **500 млн рублей**

Риски нарушения законодательства при обработке ПДн

Штрафы
до **18 млн рублей**

Подход к снижению рисков обработки перс. данных

Комплекс мер

Минимизация сбора, хранения и обработки данных

Privacy by default

Изменение архитектуры хранения и обработки данных

Централизация хранения ПДн
Внедрение анонимизации, псевдоминизации, токенизации
Ограничение передачи ПДн между средами
Инвентаризация
Контроль и упорядочивание информационных потоков

Security by design

Реализация средств защиты и процессов ИБ с фокусом на защиту ПДн

NGFW, AV, SOC, SIEM, IDS/IPS, AM, PAM, SAST, DAST, DLP, IM, VM, RM

Организация обработки ПДн

Законные основания, права субъектов, Политики, регламенты по ПДн, взаимодействие с регуляторами

Privacy by design

Автоматизация процессов организации обработки и защиты ПДн

Privacy management

Минимизация сбора, хранения и обработки данных

- Данные, собранные во время маркетинговых акций – хранение после завершения акций, отсутствие владельцев
- Данные для поддержки антифрода – хранение после проведения необходимых проверок
- Бесконечное хранение данных соискателей и результатов проверок кандидатов, которым было отказано в трудоустройстве
- Сбор паспортных данных когда они не нужны
- Сбор полных ФИО когда необходимы только Имя, e-mail и номер телефона
- Privacy by default

Изменение архитектуры хранения и обработки данных – централизация хранения ПДн

Централизация хранения ПДн в единой системе для транзакционных (поддерживающих операции) систем

Отказ от хранения ПДн в бизнес-системах, замена на корпоративные ID или токены, загрузка только при необходимости

Контроль интеграций через шины и очереди и минимизация передачи ПДн

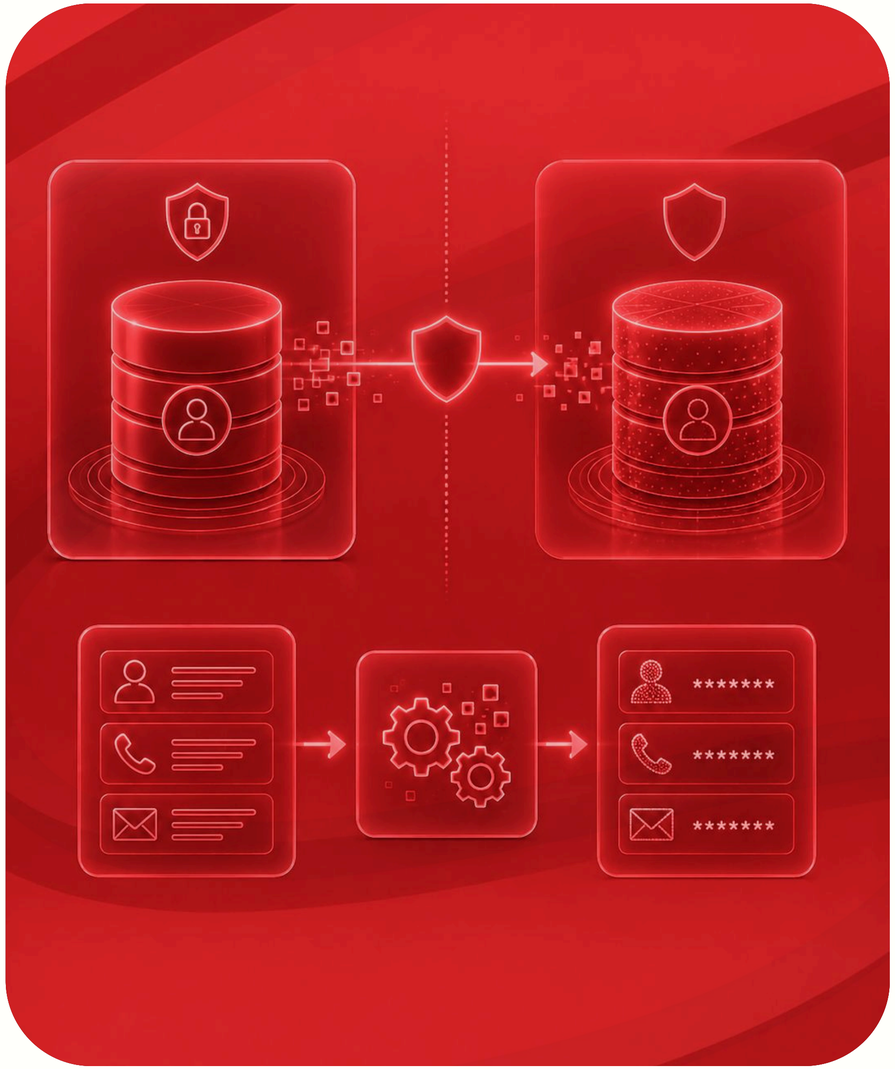
Идентификация (выявление) новых БД с ПДн в продуктивном контуре

Поиск и идентификация БД с ПДн, маскирование или обезличивание ПДн в тестовых средах и средах разработки

Интеграция между бизнес-системами не на основе прямых ПДн (ФИО, телефон, email), а с помощью корпоративных ID

Изменение архитектуры бизнес-систем и отказ от обработки на backend ПДн, которые необходимы только на frontend для формирования интерфейса сайта или МП

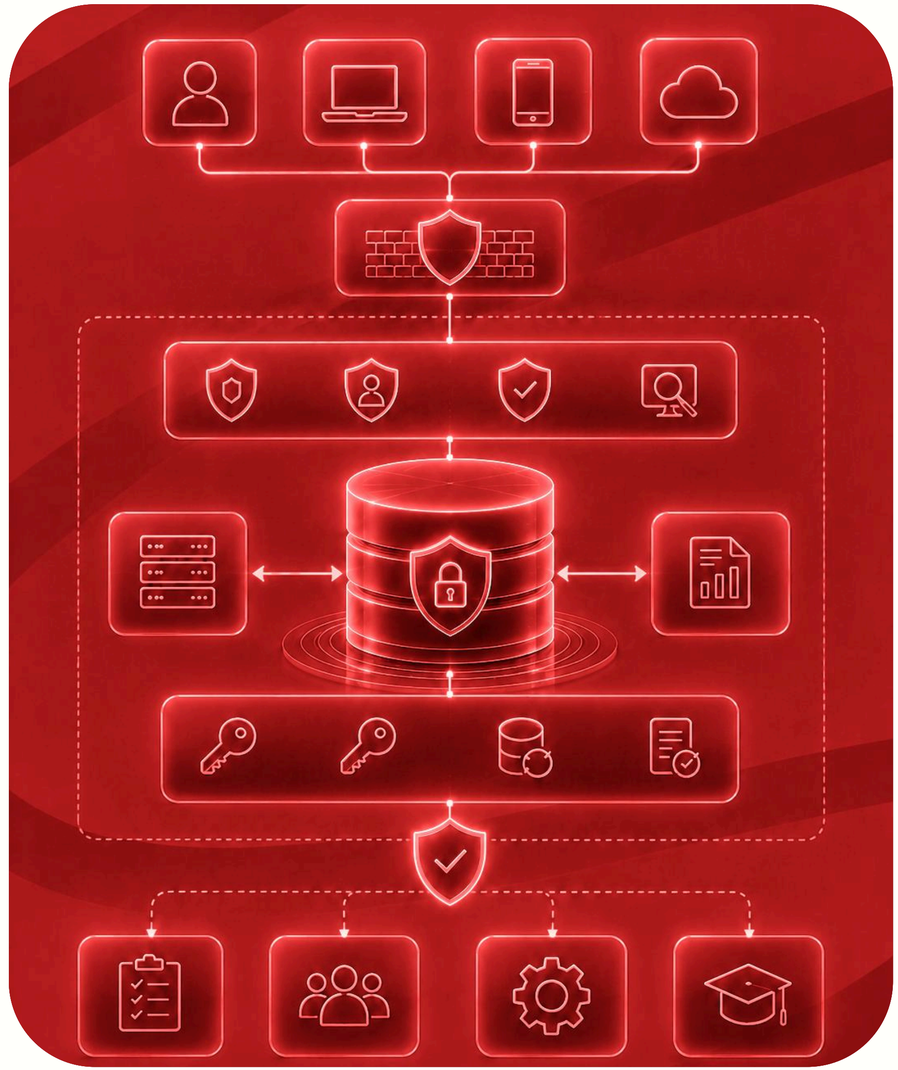
Изменение архитектуры хранения и обработки данных – разделение сред и обезличивание ПДн



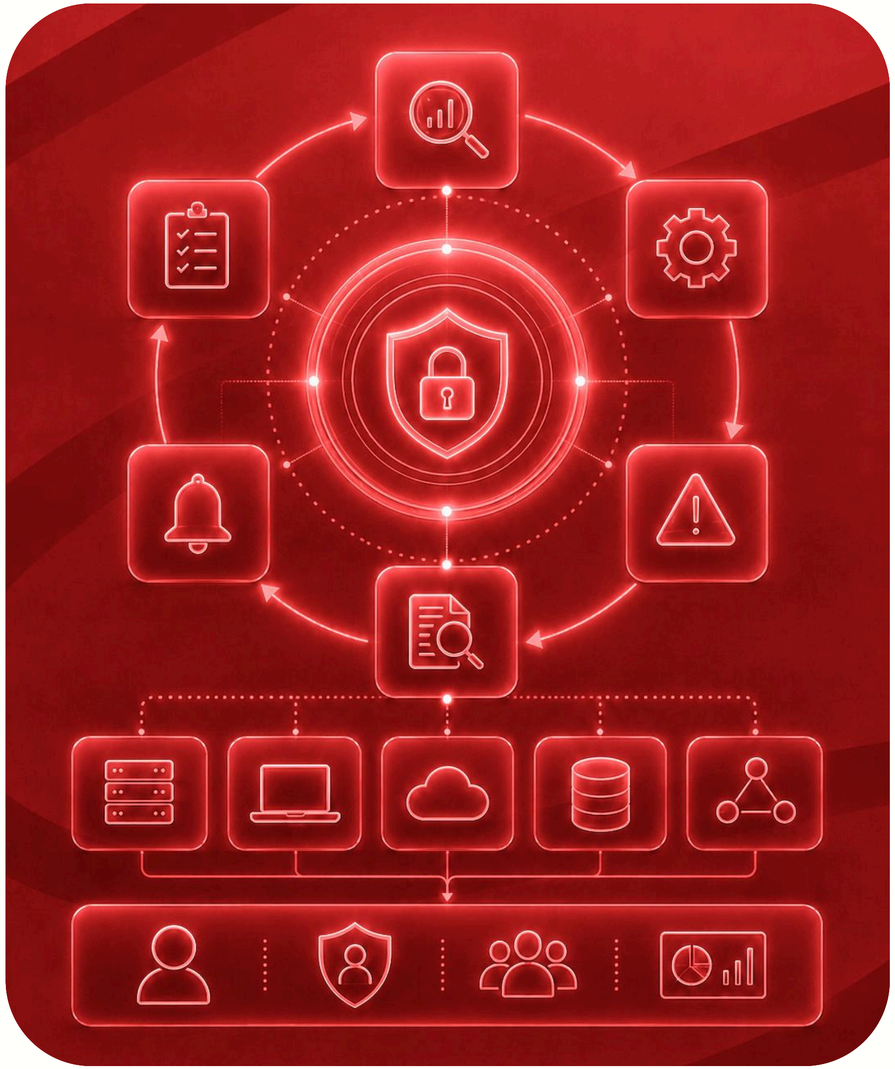
- Разделение сред (PROD, DEV, TEST, prePROD)
- Минимизация доступа разработчиков и поддержки к БД в продуктивных контурах
- Контроль и обезличивание при передаче ПДн в тестовые среды и среды разработки
- Ограничение обработки ПДн в аналитических системах
- Обезличивание, анонимизация, псевдонимизация, токенизация ПДн при выгрузке ПДн из аналитических систем и создания аналитических отчетов
- Дата-контракты с обезличиванием ПДн при выгрузке из хранилищ данных
- Резервное копирование с защитой бекапов от записи

Реализация средств защиты и процессов ИБ с фокусом на защиту ПДн - архитектура

- Сегментация сети и контроль сетевого доступа (NGFW, микросегментация, HBF)
- Управление и контроль доступа: разделение доступов к приложениям, БД, ОС, инфраструктуре
- Безопасность БД: роли, контроль доступа, DBF
- Управление привелигированным доступом (PAM)
- Шифрование ПДн при хранении
- Создание выделенных сегментов с apriori реализованным базовым набором контролей ИБ
- Безопасная архитектура при интеграции с 3-ми сторонами и контроль передачи ПДн



Реализация средств защиты и процессов ИБ с фокусом на защиту ПДн – операции и контроль



- Безопасность приложений, безопасная разработка и управление уязвимостями (SSDLC, SAST, DAST, SCA)
- Мониторинг и реагирование на инциденты (SOC)
- Защита web-приложений и API (WAF)
- 2FA на доступных из Internet ресурсах и на критичных бизнес-приложениях
- Контроль взаимодействия и передачи ПДн в LLM
- Интеграция DLP с корпоративными порталами и средствами файлового обмена, доступными из Internet
- Интеграция DLP с белыми списками контрагентов

Организация обработки ПДн

- Взаимодействие с регулятором и надзорными органами
- Управление запросами Субъектов ПДн
- Поддержание актуальности документации по ПДн (Политики, процедуры, МУ, RoPa, уведомления в РКН, приказы на ОДЛ и т.д.)
- Обеспечение наличия законных оснований для обработки и передачи ПДн 3-м лицам (оферты, Согласия,)
- Контроль обработки ПДн
- Консультирование команд по обработке ПДн
- Требования по ПДн в соглашениях с 3-ми лицами (Договоры, поручения, NDA)
- Ознакомление персонала с документами и покушение осведомленности
- Управление артефактами получения Согласий и\или акцепта оферт
- Privacy by design

Автоматизация процессов организации обработки и защиты ПДн

Внедрение системы класса Privacy Management для автоматизации операций по организации обработки и защиты ПДн и обеспечения логической связности и целостности документов и процессов:

- **Согласия**
- **Оферты**
- **Политики**
- **Перечни 3-х лиц**
- **Уведомления в Роскомнадзор**
- **Модели угроз**

Роль каждой из заинтересованных сторон при снижении рисков обработки ПДн

Бизнес-подразделения и продуктовые команды – минимизация сбора и хранения ПДн, privacy by default, реализация требования privacy by design в продукте, использование централизованных систем для хранения ПДн и ID вместо прямых ПДн для интеграции бизнес-систем

Подразделение ИТ, инфраструктура – реализация централизованного хранения ПДн, создание защищенных сегментов, реализация процессов разграничения доступа к элементам ИТ-инфраструктуры

Подразделение ИБ - Реализация средств защиты и процессов ИБ с фокусом на защиту ПДн

Офис DPO – организация и автоматизация обработки и защиты ПДн, стратегическое управление снижением рисков при обработке ПДн

HR – повышение осведомленности, обучение и ознакомления сотрудников с обязательными документами по организации обработки и защите ПДн, подписание Согласий на обработку ПДн с сотрудниками

Контакт-центр, служба заботы о Клиентах – коммуникации с Субъектами ПДн и трансляция их запросов и ответов от профильных подразделений

Проектный офис – управление проектными активностями по снижению рисков при обработке ПДн

Спасибо за внимание

готов ответить на ваши вопросы

Константин Коротнев, CISSP

Deputy CISO

E-mail: Konstantin.Korotnev@hoff.ru