

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ

на основе технологий контекстного анализа

реализация в крупной производственной компании

Защита персональных данных (ПДн): актуальность проблемы



30% —
рост числа
скомпрометированных ПДн



20% —
умышленные действия
внутреннего нарушителя



11,5–42
млн рублей —
средний ущерб от утечки



НОВЫЕ ШТРАФЫ
и радикальное увеличение
размеров ответственности

Защита ПДн: проблематика

Классические способы защиты ПДн	Почему эти способы неэффективны?
<ul style="list-style-type: none">• системы анализируют содержимое писем, сообщений в мессенджерах, файлов в облачных хранилищах и на съёмных носителях• словари определяют тематику документа по ключевым словам• цифровые отпечатки идентифицируют файлы по цифровому следу• регулярные выражения определяют объекты защиты по внешним признакам: количеству символов• просмотр событий «вручную»: специалист ИБ может обнаружить ПДн, только если откроет документ	<ul style="list-style-type: none">• ПДн плохо поддаются классификации, что приводит к ложным срабатываниям• базы данных сотрудников постоянно меняются• конфиденциальная информация похожа на публичную• общие правила политик безопасности, где нет связей между ПДн и легитимными электронными адресами для конкретного субъекта ПДн

Защита ПДн: интеллектуальная система защиты ПДн сотрудников

Решение	разработка интеллектуального инструмента на базе системы защиты данных InfoWatch Traffic Monitor, который «распознаёт» ценность той или иной порции данных
Принцип работы	инструмент «забирает» контекст из любых корпоративных информационных систем (КИС) — ABS, ERP, CRM и других, в зависимости от специфики бизнеса
Результат	реализация автоматической политики ИБ с тысячами правил, которая принимает решение, исходя из ценности каждого контрагента и документа

Поддержка отечественных
ОС и БД



Интеграция с российскими
системами из реестра
Минцифры



Бизнес: крупная производственная компания

20 000 сотрудников



цель

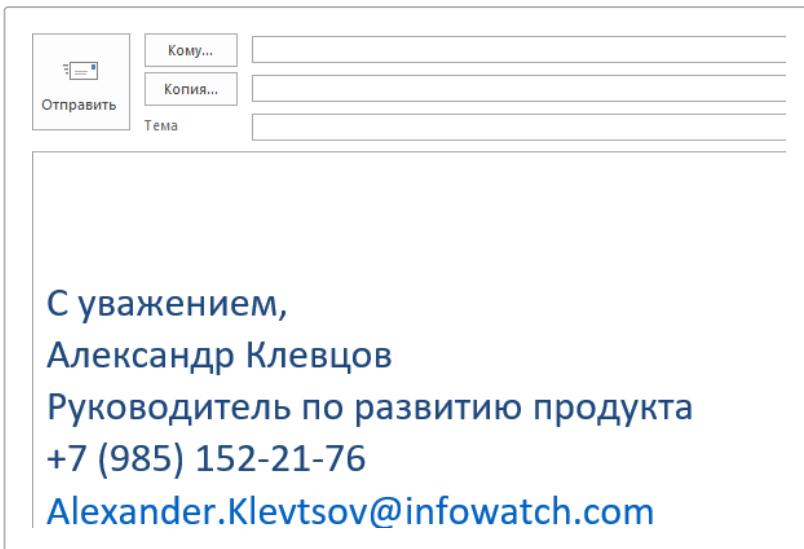
Защитить
персональные
данные
сотрудников:
паспортные
данные, ИНН,
СНИЛС, счета,
зарплатные
ведомости,
договоры ДМС

задачи

- блокировать отправку ПДн посторонним лицам
- разрешить сотрудникам свободно распоряжаться своими ПДн
- снизить трудозатраты на расследования и мониторинг
- уменьшить количество ложных срабатываний системы (40 000 в месяц до старта проекта)

Бизнес: проблематика

Система может срабатывать
на каждую подпись к письму



Конфиденциальная информация
похожа на публичную

Смирнова Мария, ул. Пришвина, 10, кв. 99,
+79857733378 12:42 ✓✓

Иванов Петр, ул. Свободы, дом 1к1, кв. 188,
+79853377739 12:42 ✓✓

Два идентичных сообщения
Одно — личная переписка с репетитором
Другое — утечка данных VIP-клиента

40 000 ложных срабатываний каждый месяц

рассылка зарплатного листка сотрудникам

Огромный ресурс ИБ для снижения ложных срабатываний.

Сотни тысяч объектов защиты в десятках тысяч политик безопасности нужно было настроить специалистам ИБ

1 сотрудник =
5–10 объектов защиты ПДн

20 000 сотрудников =
100–200 тысяч объектов защиты

Интеллектуальная система защиты ПДн сотрудников: принцип работы

Автоматическая политика =
содержит миллионы правил,
обновляющихся автоматически

Решение понимает бизнес-контекст = синхронизируется
с бизнес-системами CRM, ABS и др.

Данные из информационной системы
сравниваются с перехваченным
файлом или перепиской



**Поиск в перехваченном
письме данных одного
клиента** = ~0,001 сек

Данные сотрудника могут быть отправлены только ему — паспортные, полис, ИНН, СНИЛС, ДМС, договоры, зарплатные листки. При этом сотрудник своими данными может распоряжаться как хочет.

Интеллектуальная система защиты ПДн сотрудников: принцип работы



40 000 → 200 в месяц

снизились ложные срабатывания

85% ↓

снизились трудозатраты на расследование и мониторинг; служба безопасности сфокусировалась на критических инцидентах, импортозамещении и защите от кибератак

100% блокировка

нелегитимных отправок ПДн сотрудников без ущерба легитимным бизнес-процессам

Тиражируемость системы и возможность применения в других отраслях



Госорганы

защита ПДн сотрудников и граждан, номенклатуры закупок



Финсектор

защита ПДн клиентов, сотрудников, контрагентов, финансовой аналитики и отчёtnости



Транспорт

защита ПДн сотрудников и граждан, контрагентов, поставщиков, номенклатуры закупок, маршрутов



Ритейл

защита ПДн клиентов, сотрудников, поставщиков, контрагентов, прайс-листов, номенклатуры



Медицина и фармацевтика

защита ПДн пациентов, врачей, персонала, поставщиков, контрагентов, прайс-листов, номенклатуры услуг и препаратов



Промышленность, энергетика, нефтегазовая отрасль

защита ПДн сотрудников, поставщиков, контрагентов, номенклатуры производства, прайс-листов и финансовой отчёtnости



Оборонно-промышленный комплекс

защита ПДн сотрудников, поставщиков, контрагентов, номенклатуры производства