INFOWATCH®

НОМИНАЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

КЕЙС

Как Банк построил защиту чувствительной информации на качественно новом уровне с помощью технологий машинного обучения

Угрозы, которых не видно

Цитаты из «Исследования по утечкам конфиденциальной информации в финансовом секторе, мир — Россия, 2022», Экспертно-аналитический центр InfoWatch, 2023

INFOWATCH®

Картина с защищённостью данных в банках в целом кажется позитивной

> *Российская банковская система оказалась лучше готова к новому «кибершторму», чем мировая*

Но если присмотреться...

> *Примерно половина всех утечек в российской финансовой сфере приходится на банки*

ну и что?

> *Внутренние сотрудники всё чаще помогают хакерам получить исходные данные для атаки. <...> Доля умышленных утечек внутреннего характера в России в прошлом году составила 70%*

и не такое видели

> *Растёт латентность инцидентов внутреннего характера*
>
> То есть внутренние нарушения остаются незамеченными службой безопасности. Тайное остаётся тайным

запахло жареным!

Почему тайное остаётся тайным?

INFOWATCH®

Для защиты от утечек большинство банков использует системы класса DLP*

* от англ. Data Loss Prevention — система предотвращения утечек информации

Принцип работы всех DLP, какими мы их знали раньше: «Я защищаю то, о чём знаю»

Служба безопасности проводит аудит, узнаёт, какие документы подлежат защите и настраивает политики безопасности в DLP-системе, исходя из этого знания.

Новые документы появляются постоянно. Где гарантия, что ни один документ с чувствительной информацией не ускользнул от вас в процессе аудита?

Слабое место

Если в трафике банка ходит документ, о котором службе безопасности неизвестно, что его надо защищать, DLP-система «проспит» его утечку.

Насколько это серьёзно?

До 30% документов в среднем находятся под защитой традиционных DLP-систем в компаниях

Остальные 70% документов и действий с ними составляют «серую зону». Если данные «текут» оттуда, ничего, кроме удачи, не спасёт

Перед службой безопасности встаёт вопрос «пойти туда — не знаю куда, принести то — не знаю что»!

* от англ. Data Loss Prevention — система предотвращения утечек информации

На практике: проблема, с которой столкнулся Банк*

INFOWATCH®

Банк

— 3 000+ сотрудников

— 20+ лет на рынке

— DLP-система отрабатывает 2 млн. событий в неделю

*Из соображений конфиденциальности название Банка обезличено

Что случилось?

Группа сотрудников выводит за периметр документы. Накопилось 4 000 документов в «серой зоне».

Возник риск неконтролируемой утечки информации. Ущерб от её потери невозможно оценить

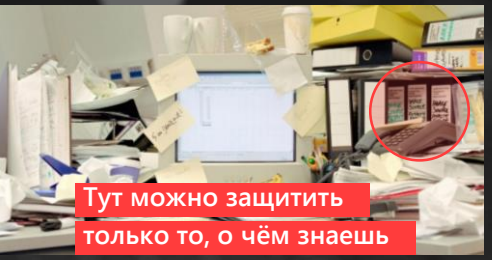
Банк вовремя предпринял меры для восстановления полноты контроля над чувствительной информацией

В чём проблема?

Двум сотрудникам службы безопасности придётся работать 30 часов, чтобы разобрать 4 000 документов вручную.

Это непозволительная трата ресурса и негарантированный результат

На практике: решение, которое разработал InfoWatch



InfoWatch совершил революцию в подходе к работе DLP:

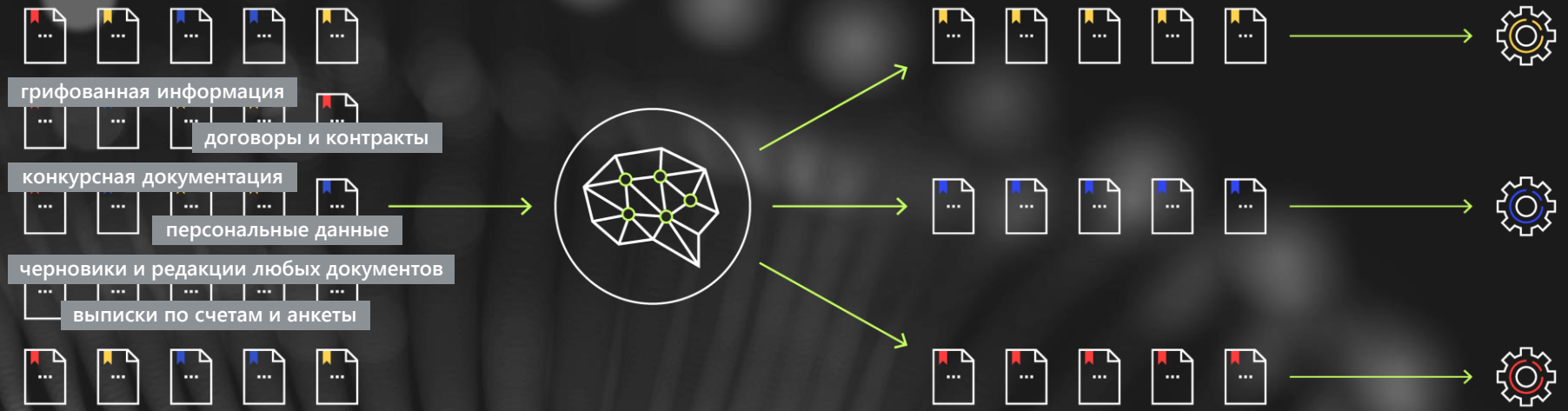
«Защищать то, о чём я знаю»

↓

«Защищать то, о чём я ещё не знаю»

Банк стал регулярно и автоматизировано разбирать «серую зону»

Работа с «серой зоной» в DPL-системе InfoWatch Traffic Monitor: как это устроено?



Неисследованный поток данных

Специальный встроенный модуль раскладывает по категориям все документы, учитывая их смысл

Документы по категориям, с тегами и аннотациями для удобного поиска и ознакомления

Модуль автоматизированного обучения — чтобы защищать новые категории данных

Банк начал регулярно работать с «серой зоной»: первые результаты

Разложили не размеченные политиками документы на категории с помощью встроенного модуля DLP-системы InfoWatch Traffic Monitor

Выявили новую категорию документов, о которой было не известно, и обучили DLP-систему — проекты кредитных договоров перестали быть слепым пятном для DLP

Настроили политики безопасности с учётом работы отделов Банка с данными документами

Актуальность политик безопасности = актуальность защиты

Результат — полнота контроля и защиты, отвечающая вызову нынешнего времени

Банк получил возможность контролировать чувствительную информацию в «серой зоне» и теперь обновляет политики безопасности еженедельно. Это драматически отличается от практики работы в DLP-системах с традиционным подходом, когда успехом считается, если политики безопасности обновляются раз в полгода

Итоги: как Банк перешёл на качественно новый уровень защиты чувствительной информации

INFOWATCH®

Регулярный разбор «серой зоны»:
1 день работы технологий машинного обучения вместо 30 часов работы двух сотрудников

Всегда актуальные политики безопасности:
обновляются раз в неделю, а не раз в полгода

Служба безопасности получила возможность контролировать все информационные активы Банка, а не только те, о которых известно

С минимальными трудозатратами разобраться в новых событиях и документах и держать документооборот и бизнес-процессы под контролем

Подробнее — в выступлении «DLP в финансовой организации: опыт клиента InfoWatch»

О компании InfoWatch

20
лет на рынке информационной безопасности

+30%
инвестиций в разработку и НИОКР ежегодно

500+
сотрудников в компании

28
патентов на технологии

700+
клиентов в финансовой орасли

135+
аналитических отчётов в год

100+
технологических партнёров

5000+
обученных специалистов ИБ

Наталья Касперская

Президент и основной владелец ГК InfoWatch. Соучредитель и генеральный директор «Лаборатории Касперского». Руководитель рабочей группы «Информационная безопасность» национальной программы «Цифровая экономика РФ»

САМЫЕ СВЕЖИЕ НАГРАДЫ,

которые получили продукты InfoWatch

TADVISER Государство. Бизнес. Технологии — **«Лучшее ИБ-решение»**
TAdviser, 2021

CNews — **«Инновация года в ИБ»**
CNews FORUM Кейсы, 2022