

# INFOWATCH TRAFFIC MONITOR

Предотвращение  
утечек информации  
и контроль  
информационных  
потоков



InfoWatch Traffic Monitor — DLP-система нового поколения, которая с помощью технологий искусственного интеллекта предотвращает утечку конфиденциальной информации, в автоматизированном режиме актуализирует политики безопасности и помогает прогнозировать риски ИБ

2019

2022

Защита от утечек данных

Выявление неправомерных действий сотрудников

Соблюдение требований регуляторов

Риск-менеджмент как направление развития

Технологии искусственного интеллекта

Гибкость и адаптивность

Цифровая  
трансформация:  
новые вызовы ИБ

Одним из следствий цифровой трансформации за последние пять лет стало осознание ценности информации как критически важного ресурса и аналитики данных — как ключевой компетенции. Службы информационной безопасности компаний, вставших на путь цифровизации, неизбежно становятся частью этого процесса. Ориентируясь на новые потребности, специалисты ИБ выбирают современные методы и инструменты работы.



## Защита от утечек данных

За 2020 вследствие одной утечки, в среднем, было скомпрометировано 4,62 млн записей. Финансовый ущерб компаний по причине утечек данных публикуется редко, репутационный ущерб, зачастую, обходится дороже. DLP-система InfoWatch Traffic Monitor обеспечивает надёжную защиту конфиденциальных данных: это лучшее ИБ-решение 2021 по версии TAdviser. InfoWatch Traffic Monitor включена в Market Guide for DLP 2020 от аналитического агентства Gartner.



## Выявление неправомерных действий сотрудников

С помощью анализа коммуникаций выявляются подозрительные и деструктивные действия сотрудников: тендерное мошенничество, использование инсайдерской информации для личного обогащения, конфликт интересов, саботаж и т. д. InfoWatch Traffic Monitor даёт инструменты для выявления и расследования таких нарушений.



## Соблюдение требований регуляторов

Приостановка деятельности организации вследствие несоблюдения требований регуляторов даже на один день может грозить многомиlionными убытками. InfoWatch Traffic Monitor помогает соответствовать требованиям 152 ФЗ, GDPR, 395 ФЗ ст. 26, 224 ФЗ, ФСБ, ФСТЭК и другим нормативным актам.



## Риск-менеджмент как направление развития

Выявление уже случившегося инцидента и анализ данных для определения причин произошедшего — первые два уровня зрелости работы с данными. Новая парадигма ИБ — прогнозирование рисков на основе анализа больших данных — свидетельствует о переходе компаний на третий уровень зрелости работы с информацией. В этом помогают инструменты визуальной и предиктивной аналитики в составе InfoWatch Traffic Monitor.



## Технологии искусственного интеллекта

Растущий объём данных, более сложная структура коммуникаций, фактическое отсутствие защищённого периметра требуют более высокого уровня автоматизации и качественно нового уровня анализа данных. Мы 15 лет применяем ИИ для анализа контента. Наша свежая разработка — автоматизация настроек политик безопасности с помощью искусственного интеллекта.



## Гибкость и адаптивность

Цифровизация увеличивает количество цифровых активов, повышает ценность информации. Растёт число сотрудников, имеющих доступ к конфиденциальным данным. Возможности анализа ландшафта корпоративных коммуникаций, актуализация настроек системы определяют качество защиты.

# DLP-система нового поколения: гибкость и готовность к быстрым изменениям



## Контентный анализ текстовых и графических документов с помощью ИИ

2000 сотрудников создают примерно 2 миллиона событий DLP-системы в день. Точность детектирования позволяет избежать затрат времени специалистов службы ИБ на обработку ложноположительных срабатываний и не пропустить важные инциденты.

- **Защита текстовых документов с обучением на данных заказчика.** Автоматическое обучение на документах заказчика с помощью ИИ. Достаточно «показать» системе набор документов одной тематики, и она автоматически обучается классифицировать похожие документы как относящиеся к этой же категории
- **Защита изображений любого типа с помощью машинного зрения.** Анализ изображений для их классификации и поиска конфиденциального содержимого. Позволяет искать и контролировать в информационном потоке изображения любого содержания, даже если было изменено разрешение, расширение файла и т. п. InfoWatch Traffic Monitor «понимает», что изображено на любой картинке
- **Защита персональных и других именованных данных.** Детектирование персональных и других именованных данных (список клиентов, прайс-листы, складские остатки и т. п.) с помощью запатентованной технологии защиты данных из корпоративных БД. Для анализа 10 000 000 записей требуется менее 0,1 секунды
- **Категоризация всех документов компании.** DLP-система защищает только те категории документов, которые ей «известны». То есть в отношении которых были настроены политики безопасности. Как правило, политиками безопасности покрыты около 20–30% от общего числа документов — те, о необходимости защиты которых было известно при настройке системы. Остальной массив данных компании остается вне поля зрения специалистов ИБ. InfoWatch Data Explorer — автоматизированный анализ информационного поля и категоризация документов. Модуль позволяет исследовать все документы компании, отнести их к тому или иному типу и соответственно актуализировать политики безопасности



## Универсальный перехватчик файлов

Не зависит от протокола приложения, способа шифрования и специфики передачи данных конкретным приложением.



## Автоматизация настроек политик безопасности

При внедрении и последующей настройке политик безопасности нужно понимать, какая информация и как распространяется в компании и за её пределы. Автоматизированный анализ информационного поля позволяет категорировать все документы, выявить их маршруты, ликвидировать все серые зоны, непокрытые политиками безопасности.



## Автоматическое прогнозирование рисков и скоринг

Анализ действий сотрудников с помощью ML-методов позволяет выявить отклонения от привычного паттерна поведения, аномальную или подозрительную активность. Специалист службы ИБ получит уведомление о возможных рисках с учётом их потенциальной опасности.



## Контроль использования данных на личных устройствах сотрудников

Если в организации используются облачные сервисы, а сотрудники могут работать с личных устройств, трафик циркулирует вне защищённого контура компании, и точки его перехвата отсутствуют. Интеграция с облачными сервисами позволяет контролировать движение данных — в том числе понимать, какая информация попадает на личные устройства сотрудников.



## Контроль копирования конфиденциальных документов внутри корпоративной инфраструктуры в ненадлежащее хранилище

Конфиденциальный документ может быть выложен на сетевое хранилище, где он будет доступен более широкому кругу сотрудников, чем предполагает его уровень конфиденциальности. Мониторинг и блокировка перемещения файлов между элементами сетевой инфраструктуры предотвращает такие нарушения.



## Защита данных DLP-системы

DLP-система аккумулирует огромное количество данных. Ролевая модель, позволяющая гибко настроить политики доступа сотрудников отдела ИБ к той или иной информации, обеспечивает защиту данных, собранных DLP-системой.

# Какая картина откроется вам?

По статистике InfoWatch, в 87% случаев в ходе пилотного проекта организации обнаруживают нарушения, которые требуют принятия немедленных мер.

Свяжитесь с экспертами InfoWatch для запуска пилотного проекта в вашей организации:

[sales@infowatch.ru](mailto:sales@infowatch.ru)  
+7 495 22 900 22

[tm.infowatch.ru](http://tm.infowatch.ru)

Сопровождение проектных работ на всех этапах.

Техническая поддержка при пуско-наладке и эксплуатации системы.

Постоянное развитие и новые релизы каждого продукта, в среднем, 2 раза в год.



InfoWatch — ведущий российский разработчик решений для обеспечения информационной безопасности организаций. Мощная академическая база, лучшие инженеры, математики и лингвисты с 2003 года обеспечивают технологическое преимущество InfoWatch в области защиты предприятий от современных киберугроз, информационных и инсайдерских атак.

Признанный эксперт и лидер рынка России и СНГ в области защиты корпоративных данных InfoWatch успешно выполнил более 3000 проектов для коммерческих и государственных организаций в 20-ти странах мира.

Две трети из 50-ти крупнейших компаний России (в соответствии с рейтингом «Эксперта») доверили InfoWatch выполнение масштабных и, зачастую, нестандартных проектов, связанных с информационной безопасностью. Причина такого доверия — не только высокое качество и уникальность технологий, но и чувство уверенности, которое возникает от сотрудничества с InfoWatch благодаря сопровождению клиентов на всех этапах проектных работ.

/InfoWatchOut

/InfoWatch



Министерство  
обороны Российской  
Федерации



Федеральная  
таможенная  
служба



Фонд  
социального  
страхования



Федеральная  
налоговая  
служба



HOME  
CREDIT  
BANK

Райффайзен  
БАНК

МТС БАНК

СОГАЗ  
СТРАХОВАЯ ГРУППА



МОСКОВСКИЙ ВЕРТОЛЕТНЫЙ  
ЗАВОД ИМ. М.Л. МИЛЯ

СУХОЙ

ОДК

О'КЕЙ

SPSR  
EXPRESS

МАГНИТ

STADA

НИАРМЕДИК  
Сеть семейных клиник