INFOWATCH®

ЭКСПЕРТНЫЙ ПОДХОД К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФАКТЫ ОБ INFOWATCH

15 лет на рынке информационной безопасности

2 000 клиентов из 20-ти отраслей в 20-ти странах

Технологическое лидерство, подтверждённое патентами

Сертификация на соответствие требованиям ФСБ, ФСТЭК и отраслевых стандартов

Представительства в 15-ти регионах СНГ

37 из 50-ти крупнейших компаний России используют решения InfoWatch

КЛИЕНТЫ

НЕФТЕГАЗОВЫЙ СЕКТОР

Газпром ВНИИГАЗ

СлавНефть

Транснефть

ОАО «ВНИПИгаздобыча»

ЭНЕРГЕТИКА

e.on

ИНТЕР РАО
КАШИРСКАЯ ГРЭС

ТВЭЛ
Топливная компания Росатома

ОДК

ПРОМЫШЛЕННОСТЬ

Московский вертолетный завод им. М.Л. Миля

ОСК
Объединенная судостроительная корпорация

Kira

Оборонпром
Объединенная промышленная корпорация

ТЕЛЕКОММУНИКАЦИИ

МТС

БАНКИ

Сбербанк
Всегда рядом

Райффайзенбанк

Банк Форштадт

Банк Кольцо Урала

Связь Банк

HOME CREDIT BANK

СТРАХОВЫЕ КОМПАНИИ

СОГАЗ
Страховая группа

ВСК
Страховой дом

ГОСУДАРСТВЕННЫЙ СЕКТОР

Федеральная налоговая служба

Федеральная таможенная служба

Министерство обороны Российской Федерации

Фонд социального страхования

ТРАНСПОРТ И ЛОГИСТИКА

Росжелдорпроект

Газпром авиа

SPSR express

МЕДИЦИНА И ФАРМАЦЕВТИКА

STADA

НИАРМЕДИК

ТОРГОВЛЯ

FIX price

Магнит

О'КЕЙ

KUPIVIP.RU

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Конкурентоспособность компаний в ближайшем будущем будет определяться уровнем их цифровизации. Цифровые технологии меняют бизнес-модели, повышают эффективность бизнес-процессов и открывают новые рыночные возможности. Цифровые преобразования становятся одним из главных факторов мирового экономического роста.

Даже в традиционных отраслях уже применяются методы анализа больших данных для извлечения новой информации, повышения эффективности операционной деятельности и качества управленческих решений.

Информация и данные — жизненно важные ценности организации в цифровую эпоху. По мнению аналитиков Gartner, к 2022 году 90% организаций будут явно идентифицировать в своих стратегических документах информацию как критический ресурс, а применение аналитики — как одну из важнейших компетенций.

Новые возможности означают и новые риски, требующие использования современных средств защиты против эволюционирующих киберугроз.

Компания InfoWatch разрабатывает технологии и продукты для снижения рисков информационной безопасности, защиты и анализа корпоративных данных для компаний, которые видят своё будущее цифровым.

РЕШЕНИЯ INFOWATCH

Безопасность корпоративных данных и анализ информационных потоков

Защита информации ограниченного доступа и персональных данных (DLP), мониторинг действий сотрудников, визуальная аналитика информационных потоков для выявления рисков и угроз информационной безопасности, инструменты для проведения расследований и поиска путей повышения операционной эффективности.

- InfoWatch Traffic Monitor
- InfoWatch Vision
- InfoWatch Person Monitor
- InfoWatch EndPoint Security

Кибербезопасность АСУТП

Защита информации в технологических сетях промышленных объектов и обеспечение требований 187-ФЗ.

- InfoWatch ARMA

Защита веб-приложений от внешних атак

Непрерывная автоматическая защита критических веб-приложений от внешних атак (OWASP 10, DDoS) на основе технологий искусственного интеллекта.

- InfoWatch Attack Killer

Анализ исходного кода приложений

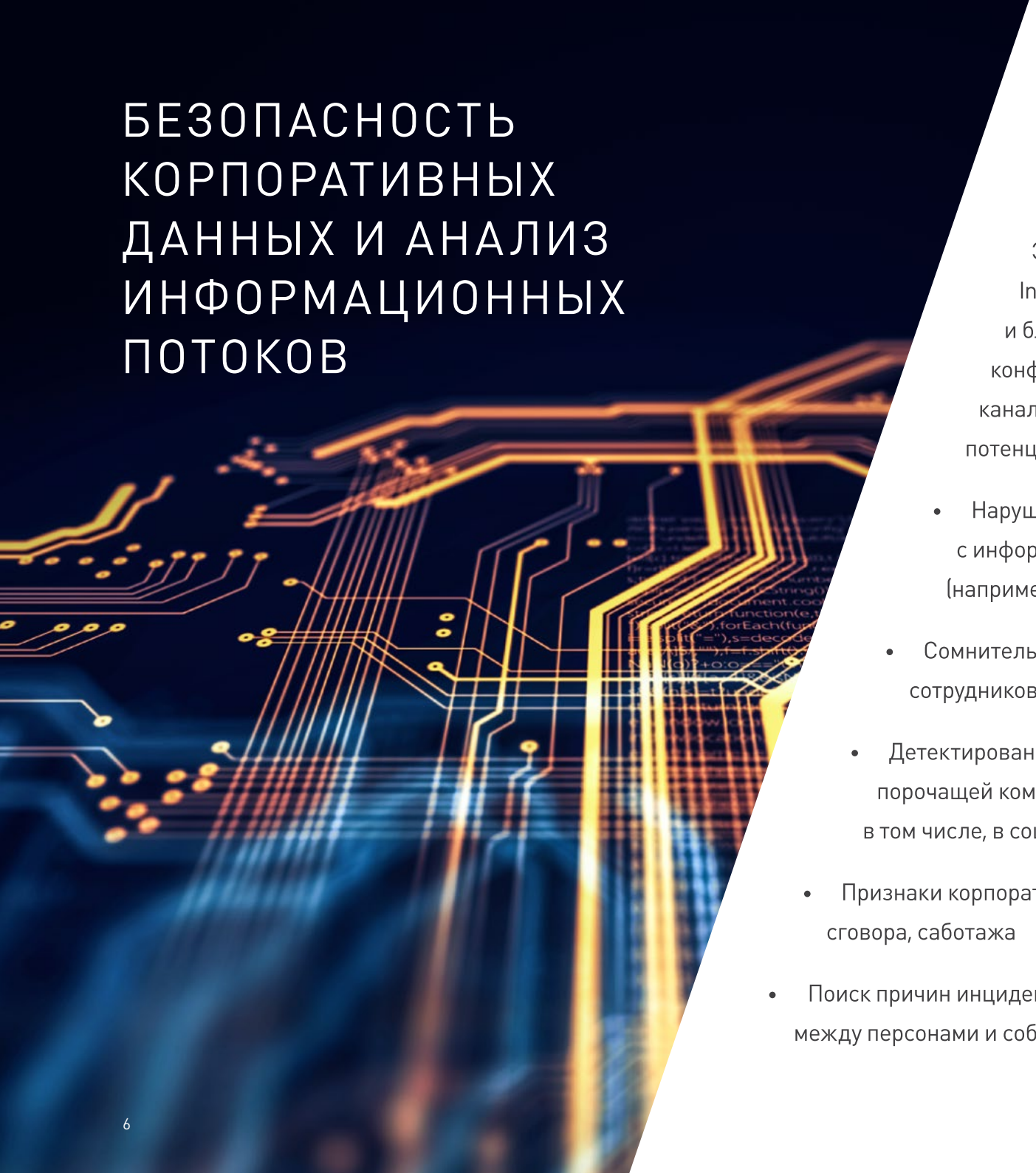
Поиск и устранение уязвимостей в исходном коде приложений.

- InfoWatch Appercut

Консалтинг, внедрение и обучение

Эксперты InfoWatch Consulting, инженеры внедрения и специалисты из Академии InfoWatch помогут найти решение любых нестандартных задач заказчика, проведут аудит, подготовят документацию, выполнят настройку и интеграцию, обучат персонал и помогут сформировать стратегию развития ИБ в организации.

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ДАННЫХ И АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ



InfoWatch Traffic Monitor — DLP-система, предотвращающая утечку данных за пределы организации.

За счёт анализа информационных потоков InfoWatch Traffic Monitor не только детектирует и блокирует попытки распространения конфиденциальных данных через любые каналы коммуникаций, но и выявляет другие потенциальные угрозы:

- Нарушения требований регулятора к обращению с информацией ограниченного доступа (например, 152-ФЗ, GDPR)
- Сомнительные действия или аномальное поведение сотрудников
- Детектирование распространения клеветнической, порочащей компанию или её руководство информации, в том числе, в социальных сетях
- Признаки корпоративного мошенничества, конфликта интересов, сговора, саботажа
- Поиск причин инцидентов, установление скрытых взаимосвязей между персонами и событиями

Самая технологичная DLP-система

- **Контролирует все каналы передачи данных,** от корпоративной почты до мессенджеров, веб-почты, облачных хранилищ, локальных и сетевых принтеров, съёмных носителей и соцсетей
- **Устанавливается в разрыв,** тем самым возможна блокировка передачи конфиденциальных данных, а не только фиксация нарушений
- **Надёжно работает под большими нагрузками,** что доказано проектами на сотни тысяч рабочих мест
- **Продвинутые технологии анализа дают высокую точность детекта,** малое количество ложных срабатываний и позволяют выявлять сложные документы, например, фрагменты чертежей, документы с печатью на основе шаблона, выгрузки из баз данных, заполненные от руки бланки и многое другое
- **Интегрирована с бизнес-системами,** например, SAP и Office 365, потому что данные создаются и используются в бизнес-приложениях

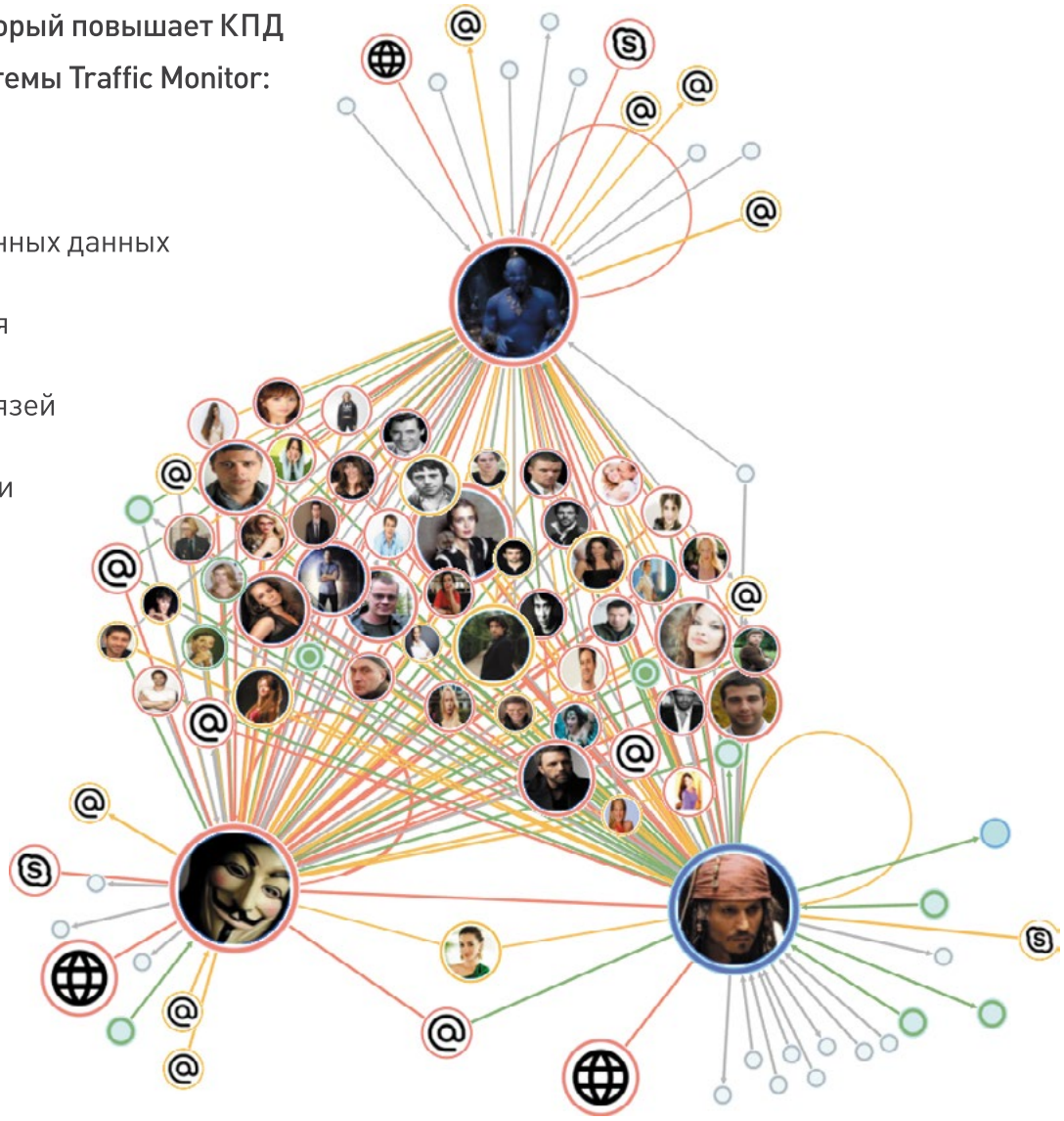
АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ

InfoWatch Vision — **инструмент визуального анализа данных, который повышает КПД использования и расширяет возможности применения DLP-системы Traffic Monitor:**

- Возможность оценить ситуацию по компании в целом
- Мгновенно обновляемые отчёты независимо от объёма выбранных данных
- Удобное исследование гипотез при проведении расследования
- Выявление рисков, поиск аномалий, установление скрытых связей
- Определение путей распространения информации по компании

Огромный массив данных, собираемых DLP-системой, доступен в виде наглядных визуальных отчётов:

- Граф связей на пятьдесят тысяч узлов
- Единая система фильтров для построения необходимых срезов данных
- Общая статистика и её детализация до отдельных событий
- Динамически пополняемое цифровое досье

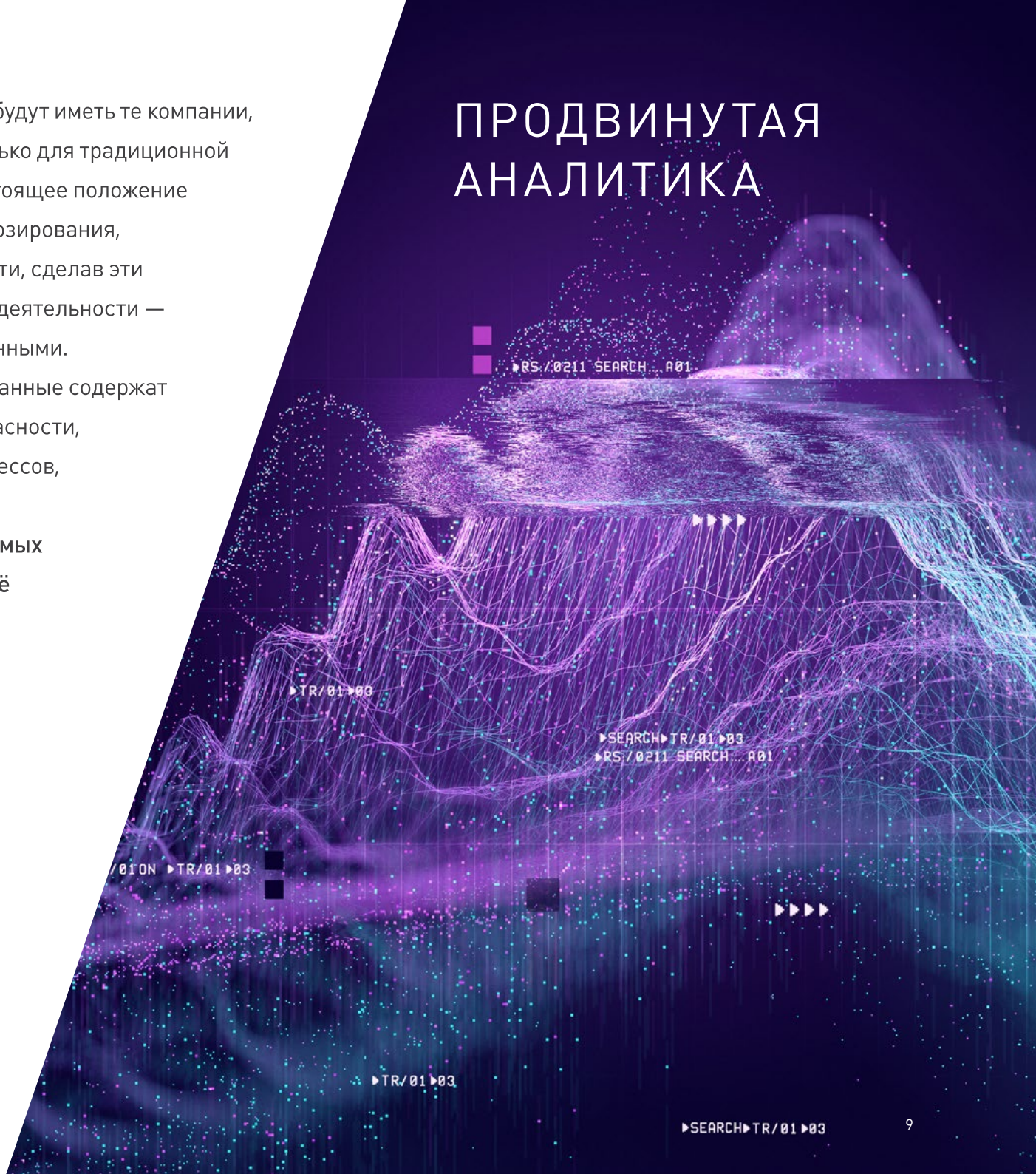


ПРОДВИНУТАЯ АНАЛИТИКА

Конкурентное преимущество в цифровом мире будут иметь те компании, которые научились использовать данные не только для традиционной отчётности, которая отражает прошлое или настоящее положение компании. Применять анализ данных для прогнозирования, оптимизации затрат и повышения эффективности, сделав эти процессы неотъемлемой частью операционной деятельности — новый уровень зрелости процессов работы с данными. Циркулирующие внутри и вокруг организации данные содержат сигналы не только о нарушениях политик безопасности, но и о показателях эффективности бизнес-процессов, потенциальных рисках и новых возможностях.

Анализ информационных потоков, контролируемых DLP-системой, позволяет расширить область её применения в сторону:

- Оценки эффективности горизонтального и проектного взаимодействия
- Поиска узких мест в коммуникациях внутри компании
- Оценки реакции на изменения
- Выявления неформальных лидеров и узких специалистов
- Анализа эффективности процессов



МОНИТОРИНГ ДЕЙСТВИЙ СОТРУДНИКОВ

InfoWatch Person Monitor — система мониторинга персонала, которая собирает данные обо всех действиях сотрудников на рабочем месте и предоставляет отчёты для служб информационной или кадровой безопасности.

90% УТЕЧЕК ИНФОРМАЦИИ — ПРЕДНАМЕРЕННЫЕ*

Специалист ИБ включает Person Monitor, когда в фокусе расследования оказывается конкретный сотрудник и необходимо:

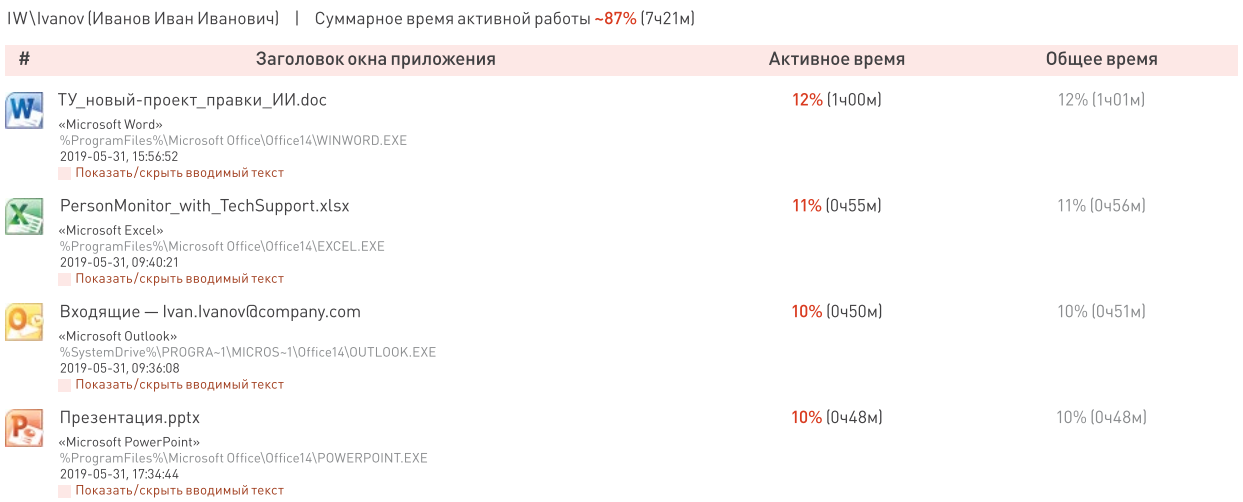
- Поминутно восстановить все активности сотрудника в течение рабочего дня
- Получить полную картину событий в ходе инцидента
- Собрать доказательства причастности и выявить мотивы

**По данным Аналитического центра InfoWatch*

Максимум информации о действиях пользователя

- Входящие и исходящие сообщения электронной почты
- Коммуникации во всех популярных мессенджерах
- Скриншоты и видео с экрана, изображения с камеры, звук микрофона
- Статистика использования приложений, контроль вводимого текста с клавиатуры
- Контроль операций с файлами, передача файлов через файлообменники и веб-почту
- Факт присутствия на рабочем месте и время, проведённое за компьютером

Удобные наглядные отчёты о результатах служебного расследования



IW\Ivanov (Иванов Иван Иванович) | Суммарное время активной работы ~87% (7ч21м)

#	Заголовок окна приложения	Активное время	Общее время
	ТУ_новый-проект_правки_ИИ.doc «Microsoft Word» %ProgramFiles%\Microsoft Office\Office14\WINWORD.EXE 2019-05-31, 15:56:52 Показать/скрыть вводимый текст	12% (1ч00м)	12% (1ч01м)
	PersonMonitor_with_TechSupport.xlsx «Microsoft Excel» %ProgramFiles%\Microsoft Office\Office14\EXCEL.EXE 2019-05-31, 09:40:21 Показать/скрыть вводимый текст	11% (0ч55м)	11% (0ч56м)
	Входящие — Ivan.Ivanov@company.com «Microsoft Outlook» %SystemDrive%\PROGRA~1\MICROS~1\Office14\OUTLOOK.EXE 2019-05-31, 09:36:08 Показать/скрыть вводимый текст	10% (0ч50м)	10% (0ч51м)
	Презентация.pptx «Microsoft PowerPoint» %ProgramFiles%\Microsoft Office\Office14\POWERPOINT.EXE 2019-05-31, 17:34:44 Показать/скрыть вводимый текст	10% (0ч48м)	10% (0ч48м)

DLP-система может предотвратить утечку информации ограниченного доступа из организации и просигнализировать об инциденте.

Система мониторинга персонала дополняет картину исчерпывающей информацией о действиях конкретного сотрудника, раскрывает контекст и позволяет собрать доказательства.

Совместное использование двух систем создаёт полноценную защиту интересов организации.

КОНТРОЛЬ ИТ-ИНФРАСТРУКТУРЫ

InfoWatch EndPoint Security — система контроля программной и аппаратной части рабочих станций.

Полный контроль над тем, что происходит на рабочих станциях

- Контроль неизменности аппаратной части рабочих станций
- Контроль и оптимизация используемого программного обеспечения
- Безопасность данных, покидающих периметр компании
- Обеспечение замкнутости инфраструктуры
- Оптимизация энергопотребления

Возможности

- Контроль и аудит изменений конфигурации рабочих станций
- Контроль запуска приложений на рабочих станциях, ограничение использования ПО и мониторинг фактического использования
- Система позволяет управлять доступом пользователей к устройствам и портам, которые могут применяться для переноса информации
- Аудит действий пользователя на рабочей станиции
- Шифрование информации, копируемой на внешние накопители, в облако, в сетевые папки
- Функция гарантированного уничтожения информации без возможности её восстановления
- Управление энергопотреблением, производительностью и режимом работы рабочих станций

ИНТЕГРАЦИЯ DLP-СИСТЕМЫ СО СТОРОННИМИ ПРИЛОЖЕНИЯМИ

Благодаря интеграции InfoWatch Traffic Monitor с внешними приложениями повышается уровень информационной безопасности организации и снижается нагрузка на офицера ИБ.

Интеграция с бизнес-приложениями: SAP, MFlash, WorksPad

Интеграция InfoWatch Traffic Monitor с бизнес-приложениями позволяет защищать данные, которые создаются и используются внутри этих приложений, и обрабатывать их в соответствии с политиками безопасности компании.

Интеграция с SIEM- и IRM-системами: MaxPatrol, RuSIEM, Комрад, Neurodat, ArcSight, QRadar, Tivoli, RVision

InfoWatch Traffic Monitor может передавать инциденты ИБ в SIEM- и IRM-системы для их обработки офицером безопасности в общем потоке, что облегчает его работу и повышает уровень безопасности благодаря наличию полной картины и возможности сопоставить события из разных систем.

Интеграция с сетевым оборудованием: Cisco, EtherSensor, CheckPoint

Интеграция с сетевыми устройствами позволяет получать трафик для анализа без развёртывания дополнительного оборудования, тем самым снижается стоимость и трудоёмкость внедрения DLP и общая стоимость владения системой.

Интеграция с помощью API

InfoWatch Traffic Monitor поддерживает API, позволяющий независимым вендорам и клиентам интегрировать с DLP-системой свои решения для обеспечения безопасности содержащихся в них данных, мониторинга, обучения сотрудников и решения других задач.

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ ОТ ВНЕШНИХ АТАК

InfoWatch Attack Killer — непрерывная автоматическая защита веб-приложений на основе технологий искусственного интеллекта.

90% САЙТОВ ИМЕЮТ УЯЗВИМОСТИ С ВЫСОКОЙ И СРЕДНЕЙ СТЕПЕНЬЮ РИСКА

- Защита от всех видов атак: включая OWASP TOP-10, атак с использованием роботов, DDoS, атак нулевого дня, атак на пользователей
- Непрерывность бизнес-процессов и доступность веб-ресурсов
- Безопасность на всём жизненном цикле приложения
- Полностью автоматическая работа системы требует минимального сопровождения, благодаря этому снижается стоимость владения и влияние человеческого фактора

Особенности InfoWatch Attack Killer

- **Искусственный интеллект** единого центра управления средствами защиты и **использование машинного обучения** позволяют выявить неизвестные атаки и автоматически адаптировать к ним правила защиты, для сопровождения системы нет необходимости в дорогостоящих экспертах
- **Непрерывный поиск уязвимостей и автоматический выпуск виртуальных патчей** для предотвращения возможности их эксплуатации позволяет быстрее разворачивать обновления, например, с новым функционалом, не дожидаясь полного тестирования приложения
- **Распределённая сеть фильтров,** непрерывно выявляющих и предотвращающих DDoS-атаки
- **Единый простой интерфейс** требует не более двух часов для освоения. Пользователь получает понятные настраиваемые отчёты с рекомендациями

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ БИЗНЕС-ПРИЛОЖЕНИЙ

InfoWatch Appercut — система анализа исходного кода приложений, которая позволяет обнаружить уязвимости и даёт рекомендации по их устранению.

90% КОМПАНИЙ ДОРАБАТЫВАЮТ БИЗНЕС-ПРИЛОЖЕНИЯ ПОД СВОИ ЗАДАЧИ С ПОМОЩЬЮ ШТАТНЫХ ПРОГРАММИСТОВ ИЛИ ОТДАЮТ ЭТУ ЗАДАЧУ НА АУТСОРСИНГ

- Быстрая проверка качества исходного кода и ясная картина рисков при приёмке результатов заказной разработки ПО, в том числе доработок 1С
- Интеграция InfoWatch Appercut в процесс безопасной разработки (Secure SDLC) позволяет выявлять уязвимости на ранних стадиях проекта и за счёт этого получить качественный безопасный продукт
- Необходимый инструмент DevOps поддерживает современные методологии разработки и может быть встроен в процессы continuous integration / delivery

Возможности InfoWatch Appercut

- **Поддерживает 20 языков программирования,** включая 1С, Java, PHP, JavaScript, C# и другие
- **Проверка на соответствие требованиям** международных стандартов PCI DSS и HIPAA, лучшим практикам CERT и OWASP, рекомендациям SDLC, а также рекомендациям производителей платформ 1С, SAP, Oracle, Microsoft
- **Автоматические отчёты о найденных уязвимостях** (doc, docx, pdf, html) и рекомендации по их устранению
- **Интеграция со средами разработки:** системами контроля версий и системами отслеживания ошибок позволяет эффективно организовать командную работу
- **Не требует специальных знаний и навыков** для эксплуатации

КИБЕРБЕЗОПАСНОСТЬ АСУТП

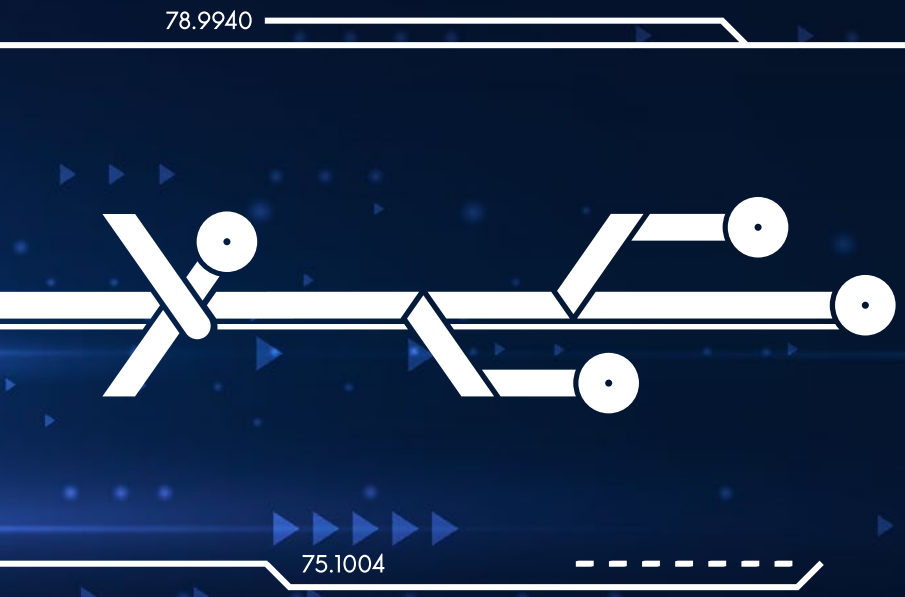
InfoWatch ARMA — первый отечественный промышленный межсетевой экран для защиты информации в технологических сетях промышленных объектов.

50% — РОСТ ЧИСЛА ВЫЯВЛЕННЫХ УЯЗВИМОСТЕЙ SCADA-СИСТЕМ В ПЕРВОМ ПОЛУГОДИИ 2018*

48% ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ РОССИИ БЫЛО АТАКОВАНО КИБЕРПРЕСТУПНИКАМИ**

*По сравнению с аналогичным периодом предыдущего года, исследование TrendMicro

**По данным аналитиков «Лаборатории Касперского»



Какие задачи решает

- Закрывает значительную часть технических мер защиты, предусмотренных приказом ФСТЭК России от 14 марта 2014 № 31
- Создает замкнутую безопасную среду
- Обеспечивает защиту от таргетированных атак
- Выявляет аномальную активность и предотвращает вторжения

Преимущества

Единственный промышленный межсетевой экран отечественного производства:

- Работа на уровнях L2/L3
- Статическая и динамическая маршрутизация трафика
- Поддержка Network Address Translation (NAT) и Proxy
- Передача событий ИБ в SOC и SIEM

КОНСАЛТИНГ И ВНЕДРЕНИЕ

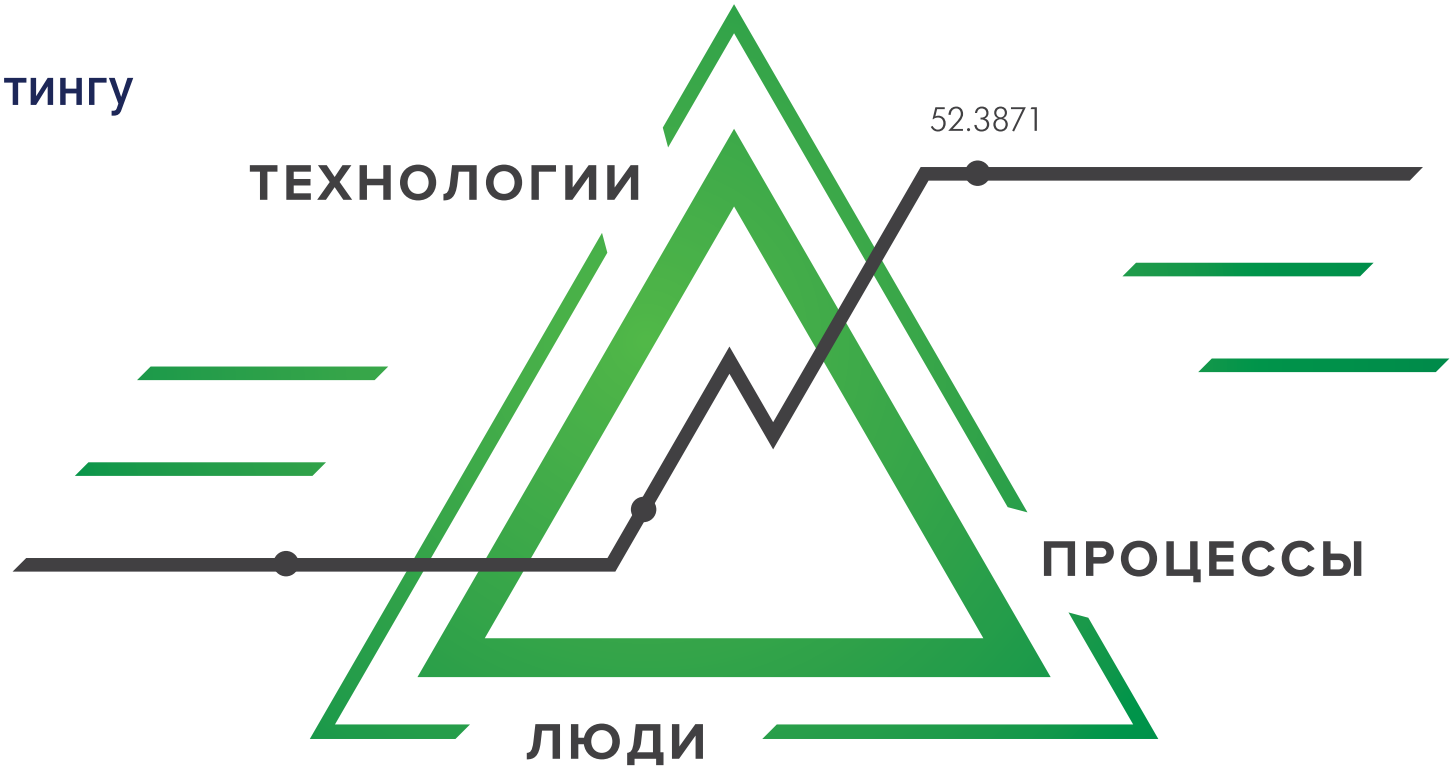
Максимальная отдача от внедряемых решений

Во-первых, опыт экспертов компании InfoWatch, понимание современного ландшафта угроз, знание отраслевой специфики и методик работы позволяют спроектировать, внедрить и оптимизировать системы обеспечения информационной безопасности для наилучшего соответствия целям и задачам организации.

Во-вторых, заказчики получают экспертизу в построении правильных процессов, необходимые знания для их поддержания и совершенствования, а также помощь в формировании долгосрочной стратегии развития ИБ организации.

- Использование лучших практик при внедрении и настройке даёт эффективную защиту уже на старте
- Проверенная методология позволяет использовать возможности решения на 100%
- Формируется юридическая база для легитимного применения систем DLP и Employee Monitoring
- Измеримые показатели позволяют оценить качество функционирования процессов обеспечения информационной безопасности

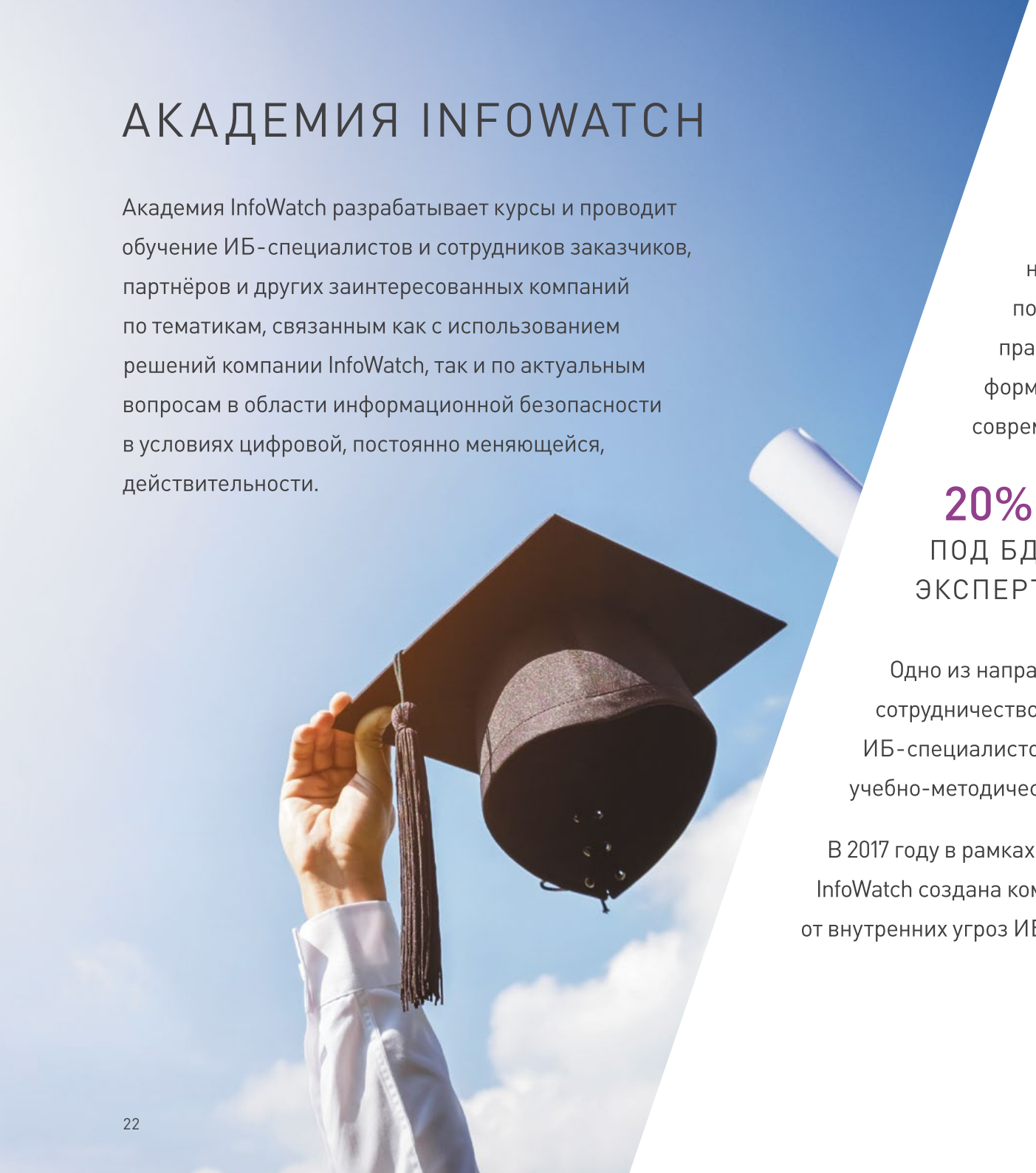
Услуги в рамках проекта по консалтингу



- Выявление информации ограниченного доступа, категоризация и оценка её важности
- Формирование процесса жизненного цикла обработки чувствительных данных и обеспечение его легитимности
- Создание настроек DLP-системы на основе результатов аудита, выстраивание процесса обнаружения и реагирования на инциденты
- Формирование ключевых метрик эффективности работы системы и методики их измерения
- Разработка концепции развития защиты от утечек в соответствии с общей стратегией развития организации

АКАДЕМИЯ INFOWATCH

Академия InfoWatch разрабатывает курсы и проводит обучение ИБ-специалистов и сотрудников заказчиков, партнёров и других заинтересованных компаний по тематикам, связанным как с использованием решений компании InfoWatch, так и по актуальным вопросам в области информационной безопасности в условиях цифровой, постоянно меняющейся, действительности.



Академия выросла из внутреннего образовательного проекта компании InfoWatch, который существует более 12 лет. Многолетние методические наработки обеспечивают глубокое погружение в выбранную тематику, практико-ориентированный подход гарантирует формирование навыков, необходимых современному ИБ-специалисту.

20% ТЕОРИИ И 80% ПРАКТИКИ ПОД БДИТЕЛЬНЫМ РУКОВОДСТВОМ ЭКСПЕРТОВ ИБ

Одно из направлений работы Академии InfoWatch — сотрудничество с учебными заведениями в области подготовки ИБ-специалистов, для чего разработаны специализированные учебно-методические комплексы.

В 2017 году в рамках World Skills Russia экспертами InfoWatch создана компетенция «Корпоративная защита от внутренних угроз ИБ».

КАКАЯ КАРТИНА ОТКРОЕТСЯ ВАМ?

InfoWatch — ведущий российский разработчик решений для обеспечения информационной безопасности организаций. Мощная академическая база, лучшие инженеры, математики и лингвисты на протяжении 15-ти лет 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 2000 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 в качестве и уникальности технологий, но и в чувстве уверенности, которое дает InfoWatch, когда сопровождает своих клиентов на всех этапах проектных работ.

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
+7 495 22-900-22
infowatch.ru

/InfoWatchOut
/InfoWatch

Полное или частичное копирование материалов возможно только при указании ссылки на источник — сайт infowatch.ru — или на страницу с исходной информацией