КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

06 СЕНТЯБРЯ 2018
ВЛАДИВОСТОК

#CODEIB

РАМКИ VS ПЕРИМЕТР

Самойленко Никита

Менеджер по работе с клиентами
И партнерами в ДФО

ТЕЛЕФОН: +7 (962) 227-42-45

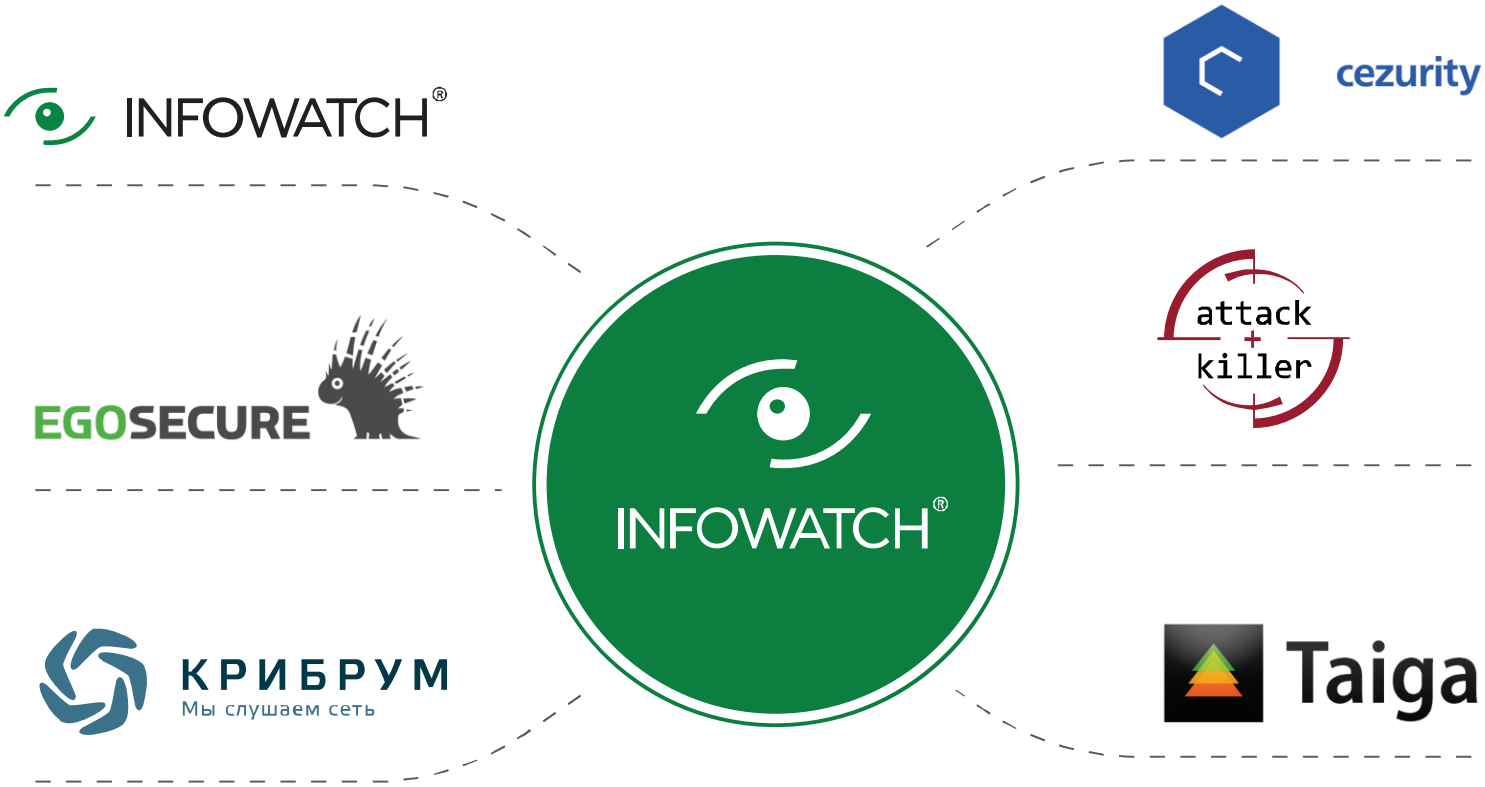
INFOWATCH®

EMAIL: **Nikita.Samoylenko@infowatch.com**

ГРУППА КОМПАНИЙ INFOWATCH

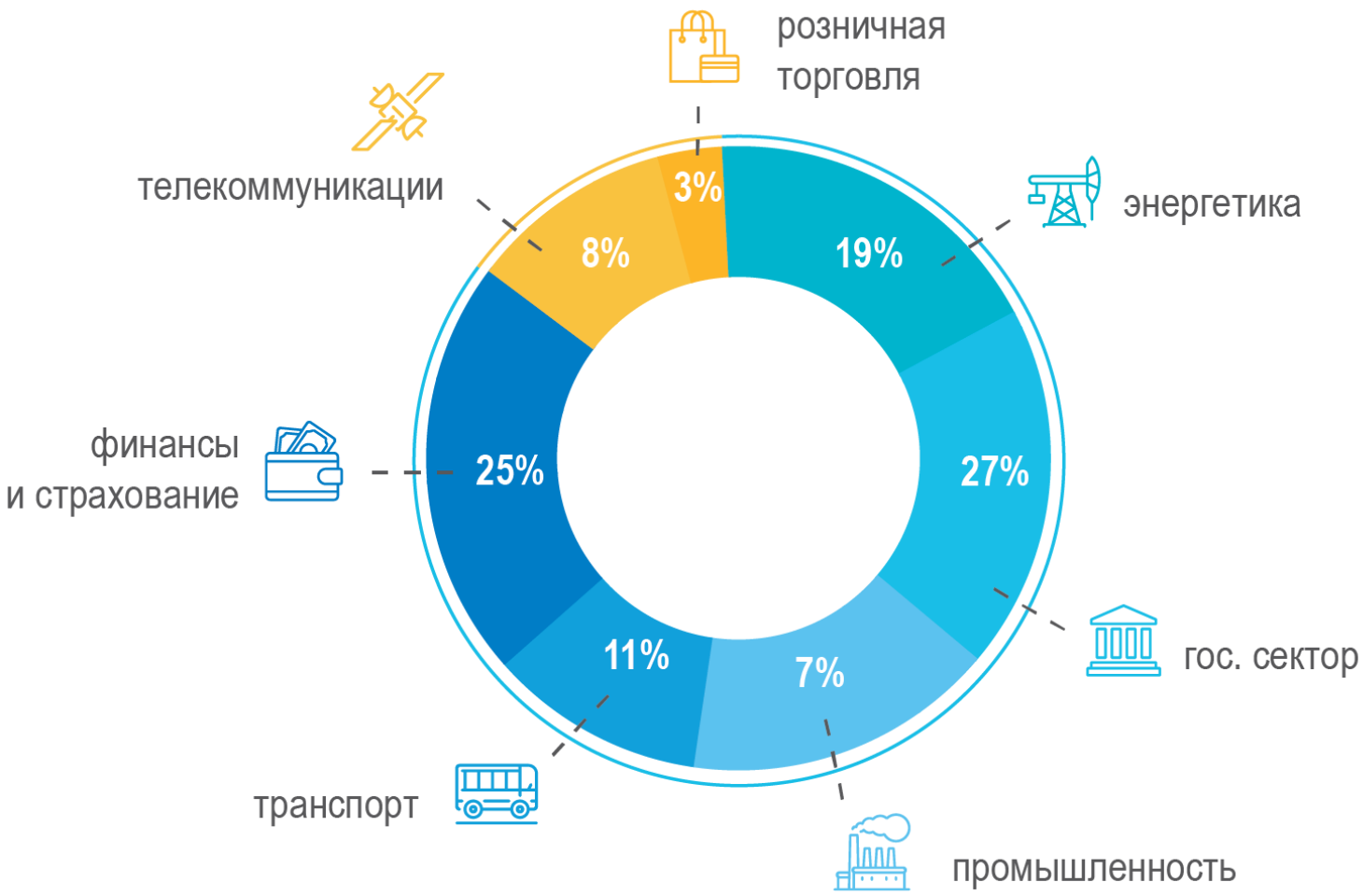
ГРУППА КОМПАНИЙ INFOWATCH

СОСТАВ ХОЛДИНГА



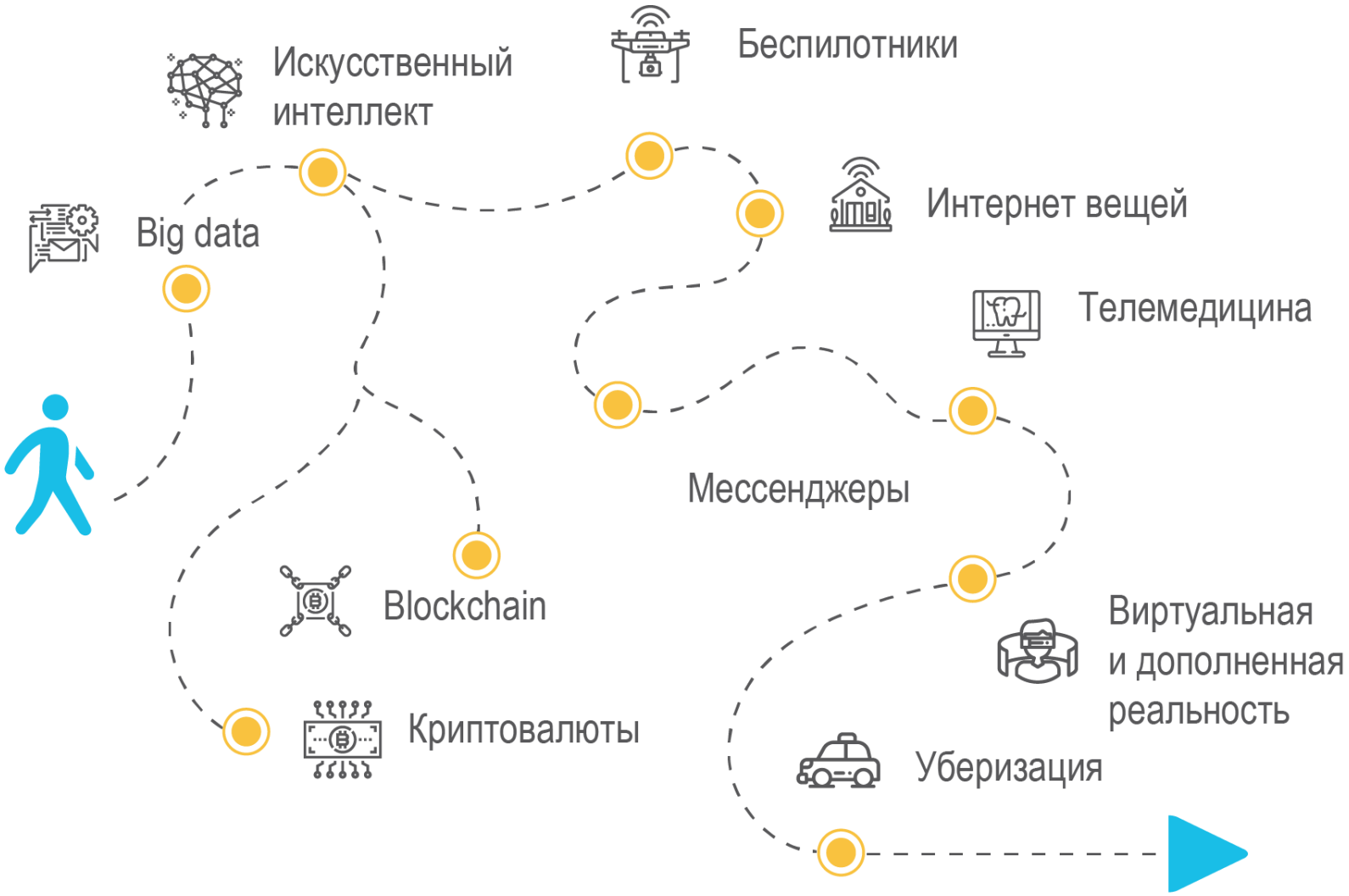
ГРУППА КОМПАНИЙ INFOWATCH

ОТРАСЛИ КЛИЕНТОВ



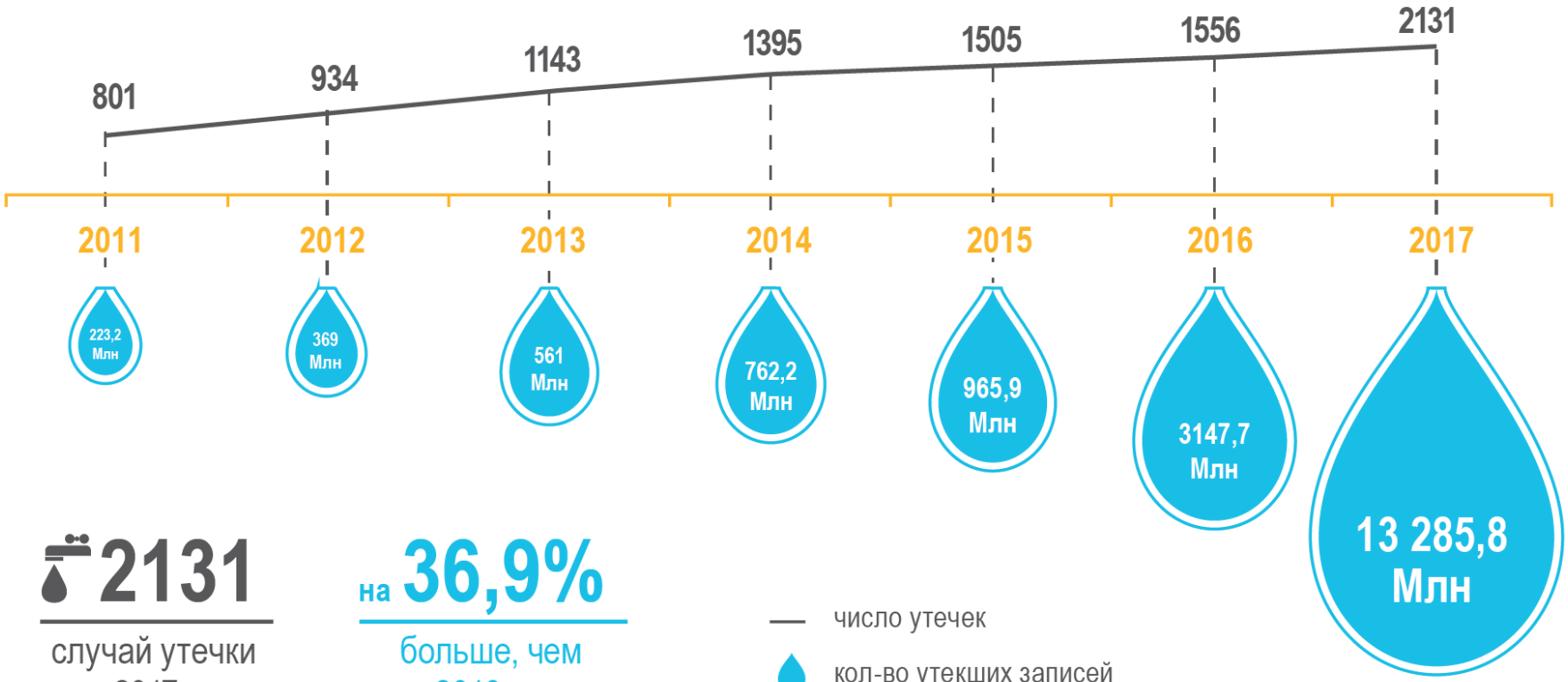
УТЕЧКИ ИНФОРМАЦИИ

INFOWATCH®



УТЕЧКИ ИНФОРМАЦИИ

INFOWATCH®



2131

случай утечки за 2017 год

на 36,9%

больше, чем в 2016 году

— число утечек

кол-во утекших записей

по данным Аналитического Центра InfoWatch, 2018

РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО ОТРАСЛЯМ

INFOWATCH®

по данным Аналитического Центра InfoWatch, 2018

ЭФФЕКТИВЕН ЛИ ПОДХОД К БЕЗОПАСНОСТИ?

INFOWATCH®

Добавление источников (каналов) чаще всего опаздывает

Всегда найдется «самый умный» и хитрый

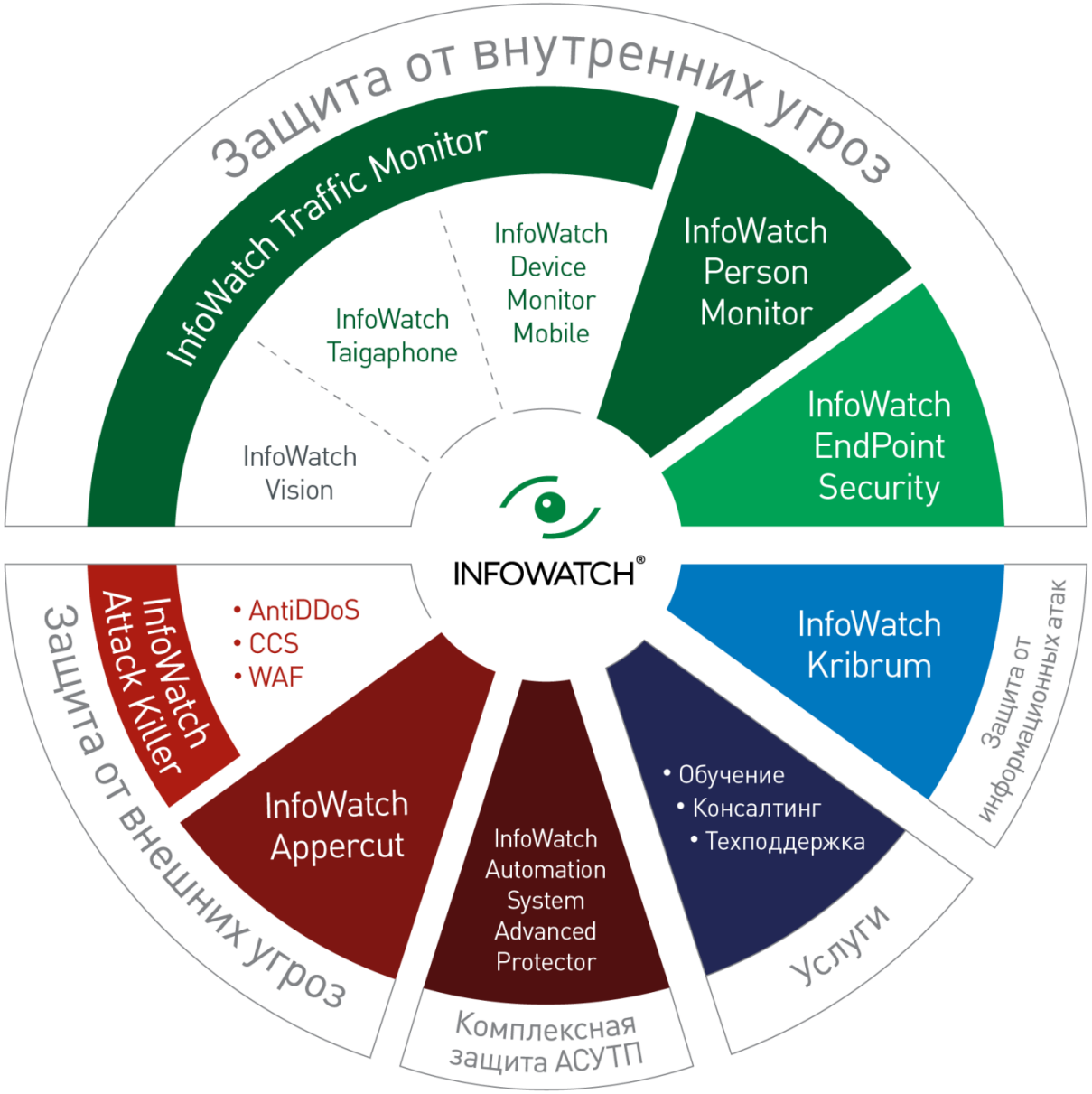
Постоянный выбор - блокировка или непрерывность бизнес-процессов?

Отсутствие единой системы контроля

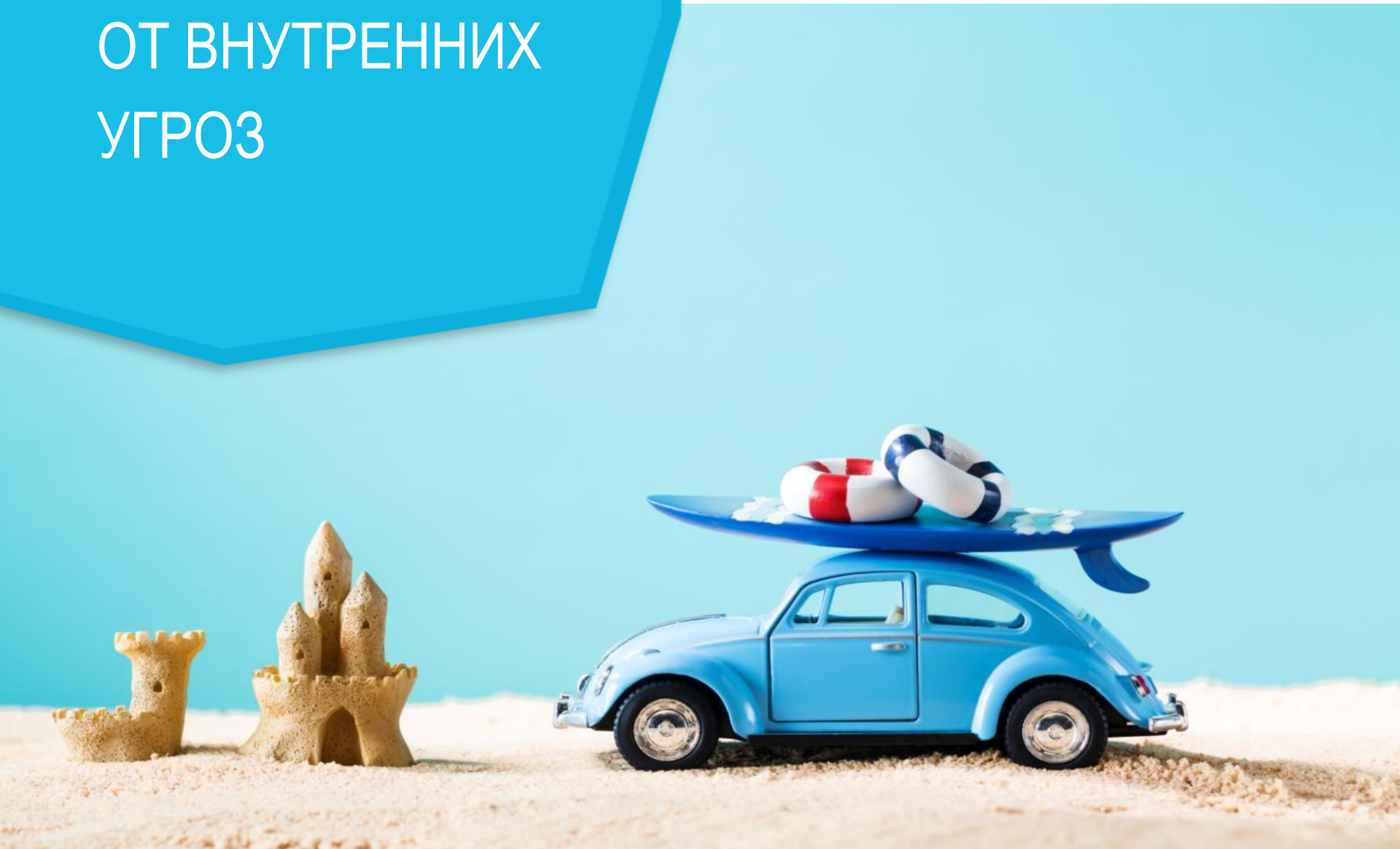
СЛОЖНО
СОЗДАТЬ
ВСЕОБЪЕМЛЮЩУЮ
СИСТЕМУ ЗАЩИТЫ

НО

МОЖНО
МИНИМИЗИРОВАТЬ
РИСКИ, НУЖЕН
НОВЫЙ ПОДХОД!


Защита от внутренних угроз
InfoWatch Traffic Monitor
InfoWatch Device Monitor Mobile
InfoWatch Taigaphone
InfoWatch Vision
InfoWatch Person Monitor
InfoWatch EndPoint Security
INFOWATCH®
Защита от внешних угроз
InfoWatch Attack Killer
• AntiDDoS
• CCS
• WAF
InfoWatch Appercut
InfoWatch Automation System Advanced Protector
Комплексная защита АСУТП
Услуги
• Обучение
• Консалтинг
• Техподдержка
InfoWatch Kribrum
Защита от информационных атак

ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ



ПЕРЕДАЧА ИНФОРМАЦИИ КОНКУРЕНТАМ

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Руководитель отдела продаж
и компания-конкурент

СЦЕНАРИЙ:

Начальник отдела продаж крупной организации в течение двух лет **передавал конкурентам информацию** об условиях продаж, ценах, отношениях с клиентами и т.п.

ПОСЛЕДСТВИЯ:

убытки

60 млн

рублей

КРАЖА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Ведущий инженер

СЦЕНАРИЙ:

Ведущий инженер, занимающийся крупной сделкой, решил договориться с конкурентами и **продать проектную документацию**. Переписка велась по личной почте с корпоративного ноутбука сотрудника

ПОСЛЕДСТВИЯ:

потенциальный ущерб – более 100 млн руб.

КОРРУПЦИЯ В АДМИНИСТРАТИВНОМ АППАРАТЕ

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Семейная пара: чиновница и владелец строительной компании

СЦЕНАРИЙ:

Чиновница использовала свое должностное положение для проведения **подставных тендеров** по строительству и реконструкции.
Работая в администрации города, она **передавала конфиденциальные сведения** мужу, владельцу строительной компании

ПОСЛЕДСТВИЯ:

скандал, уголовное преследование, подрыв репутации первых лиц администрации города

НАРУШЕНИЕ ЗАКОНА О ЗАЩИТЕ ПДн

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Сотрудница отдела кадров

СЦЕНАРИЙ:

Служащая государственной компании скопировала на USB-носитель данные анкет

1000 сотрудников

для последующей перепродажи на черном рынке

ПОСЛЕДСТВИЯ:

подрыв репутации должностных лиц, штрафные санкции за нарушение конфиденциальности ПДн

КОРРУПЦИЯ, МОШЕННИЧЕСТВО

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Сотрудник отдела закупок

СЦЕНАРИЙ:

Один из менеджеров отдела закупок **подделывал товарные накладные** и получал на складе готовую **продукцию в обход кассы**. Данная схема была обнаружена при проверке заполненных форм накладных

ПОСЛЕДСТВИЯ:

потенциальный ущерб – 1 млн руб.

КАК ЗАЩИЩАТЬСЯ

INFOWATCH®

Контроль исходящего трафика

на наличие конфиденциальных данных

Блокировка передачи подозрительных сообщений

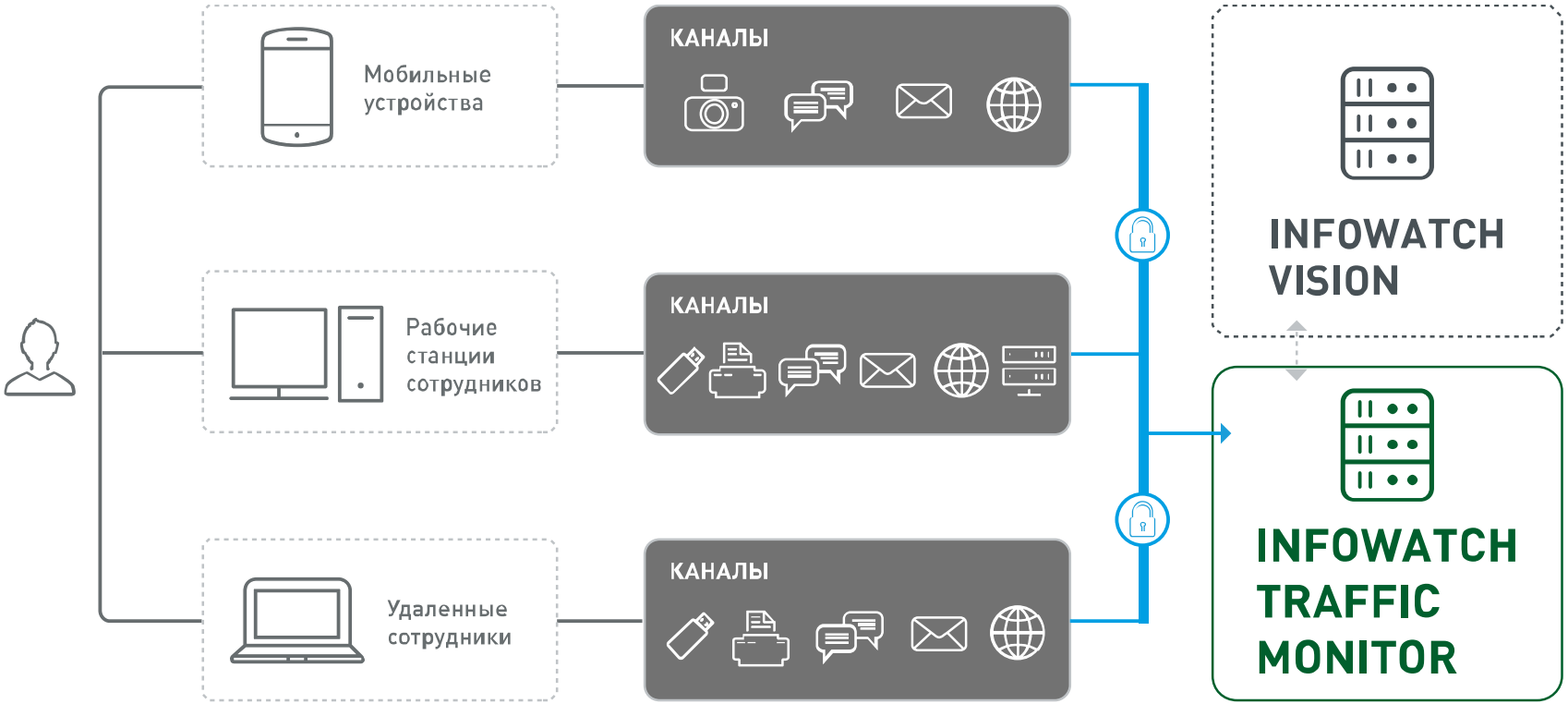
при обнаружении нарушений

Ведение базы инцидентов

для проведения расследований и доказательства вины злоумышленника

КОМПЛЕКСНОЕ РЕШЕНИЕ

INFOWATCH®



INFOWATCH TRAFFIC MONITOR

INFOWATCH®

Решение для борьбы с внутренними угрозами и неправомерными действиями сотрудников, которые приводят к утечкам информации и финансовым потерям

- **Автоматическая классификация** информационных потоков
- **Мониторинг** и анализ данных
- **Выявление мошеннических схем**, нацеленных на кражу информации
- **Безопасное хранение** данных для анализа и проведения расследований

ЧТО НОВОГО В INFOWATCH TRAFFIC MONITOR

ВОЗМОЖНОСТИ:

- Инструменты расследования и коммуникаций
- Astra Linux
- Менеджер запросов и отчетов
- Поддержка концепции BYOD
- Подсветка результатов анализа

РЕЛИЗ СОДЕРЖИТ

БОЛЕЕ 20 ДОРАБОТОК И УЛУЧШЕНИЙ

INFOWATCH VISION

INFOWATCH VISION

Модуль InfoWatch Traffic Monitor

Инструмент офицера безопасности для выявления потенциально опасных связей сотрудников и расследования инцидентов в режиме реального времени

- **Выявление подозрительных связей** сотрудников
- Мгновенный доступ **к деталям любой** подозрительной **активности**
- Представление **отчетности в режиме реального времени** для любого среза информации

СХЕМА РАБОТЫ INFOWATCH VISION

1. Все панели **связаны между собой** и отображают **единый срез данных**

2. Офицер безопасности формирует срез данных с помощью **интерактивных графиков**

3. Просмотр **конкретных событий** по сформированной выборке осуществляется **на панели «Досье»**

INFOWATCH DEVICE MONITOR MOBILE

INFOWATCH DEVICE MONITOR MOBILE

Модуль DLP-решения InfoWatch Traffic Monitor

Агентское решение для устройств на базе Android

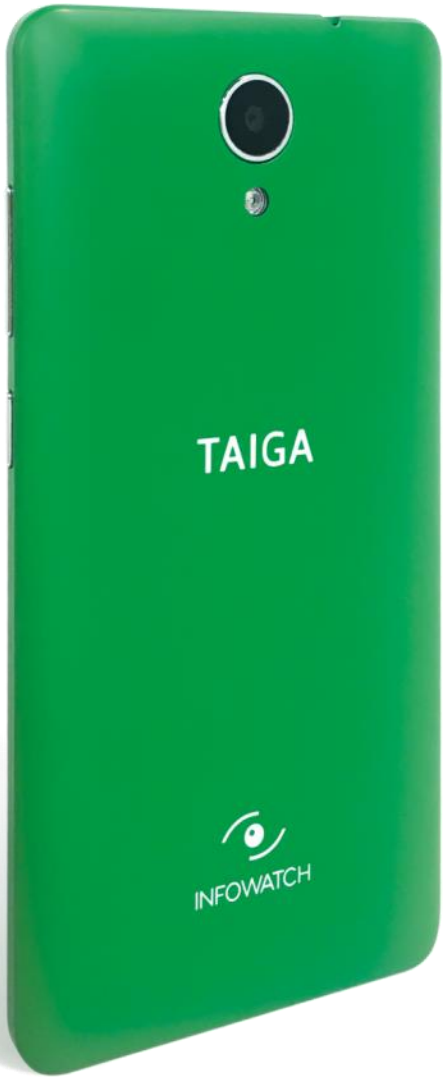
- **Контроль каналов** коммуникаций сотрудников на мобильных устройствах
- **Контроль перемещения** информации внутри и вовне периметра безопасности
- **Автоматическая классификация** и анализ данных
- **Безопасное расширение периметра** корпоративной сети

INFOWATCH TAIGAPHONE

INFOWATCH®

INFOWATCH TAIGAPHONE

Является частью DLP-системы **InfoWatch Traffic Monitor** и помогает предотвращать утечки корпоративных данных по беспроводным каналам связи



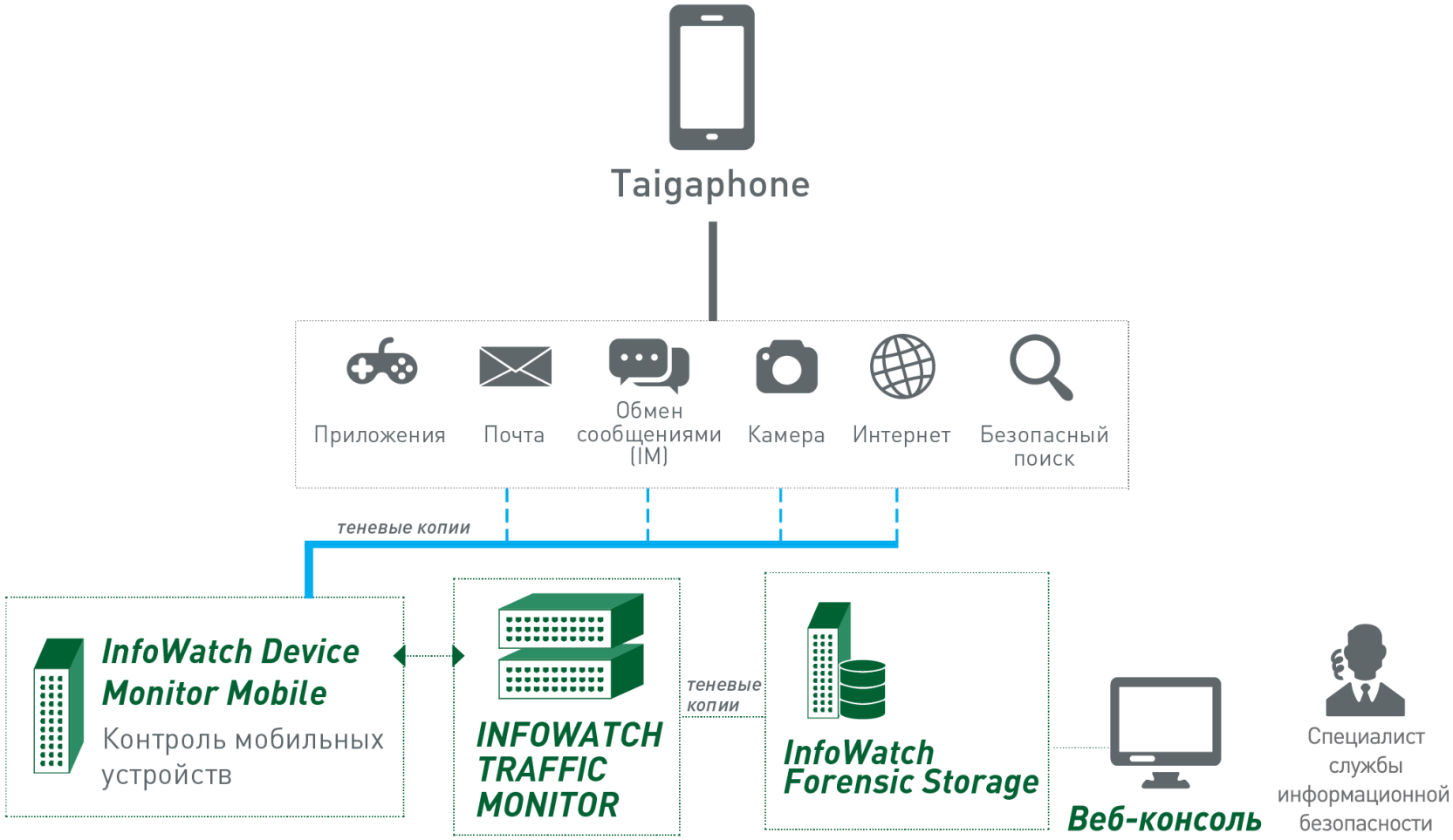
РЕШАЕМЫЕ ЗАДАЧИ

- Безопасное **расширение периметра** корпоративной сети
- Контроль **каналов коммуникаций** сотрудников на смартфоне
- **Доверенное устройство** для мобильных сотрудников
- **Предотвращение утечек** конфиденциальных данных с устройства

InfoWatch Taigaphone –

смартфон с прошивкой на базе Android, интегрированный с InfoWatch Traffic Monitor

СХЕМА РАБОТЫ INFOWATCH TAIGAPHONE



ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

Для риск-менеджеров, ИБ-, ИТ-специалистов, сотрудников отдела экономической безопасности:

- Контроль всех информационных потоков
- Своевременное выявление внутренних угроз и минимизация рисков
- Наглядные отчеты, показывающие реальную ситуацию в компании
- Точная идентификация нарушителей

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

Для руководителей бизнеса, топ-менеджеров:

- Сокращение возможных финансовых и репутационных потерь
- Предотвращение воровства, мошенничества, коррупции
- Вовлечение всех бизнес-подразделений компании в управление безопасностью корпоративных данных
- Готовые отраслевые решения и преднастроенные политики

КОНТРОЛЬ СОТРУДНИКОВ

ПОЧЕМУ ЭТО ВАЖНО

INFOWATCH®

до 40% времени

может уходить на переключение между задачами

до 30% времени

уходит у сотрудника на просмотр соцсетей, понижая общую производительность бизнеса на 13%

до 205 дней в году

люди не работают из-за прокрастинации, выходных, праздничных дней и отпусков

НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ РЕСУРСОВ

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Сотрудники организации

СЦЕНАРИЙ:

Сотрудники регулярно использовали принтеры для печати личных документов, не выключали компьютеры перед уходом, устанавливали на компьютеры произвольное ПО

ПОСЛЕДСТВИЯ:

лишние расходы на электричество, материалы, замену и обслуживание принтеров

НЕЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ ВРЕМЕНИ

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Сотрудники госорганизации

СЦЕНАРИЙ:

Служащие не справлялись с обработкой потока заявок. В ходе внутреннего расследования выяснилось, что **40% рабочего времени** они тратили на **развлекательные сайты** и социальные сети

ПОСЛЕДСТВИЯ:

низкие показатели работы, жалобы граждан, урезание бюджета

КАК ЗАЩИЩАТЬСЯ

INFOWATCH®

Проводить аудит

используемого ПО и действий сотрудников

Выявлять уязвимые места и контролировать

используемые приложения

Шифровать файлы

для защиты от умышленной или случайной передачи третьим лицам

INFOWATCH ENDPOINT SECURITY

INFOWATCH

INFOWATCH ENDPOINT SECURITY

Автоматизированная система непрерывного мониторинга, диагностики и защиты, которая шифрует корпоративные данные и выявляет слабые места в компании

- **Контроль доступа** сотрудников к внешним устройствам и файлам
- **Шифрование данных** и безопасная работа в облачных хранилищах
- **Мониторинг рабочей активности** сотрудников
- **Аудит** использования инфраструктуры компании

INFOWATCH PERSON MONITOR

INFOWATCH

INFOWATCH PERSON MONITOR

Инструмент мониторинга рабочих процессов компании и выявления резервов сокращения нецелевых расходов

- **Анализирует** рабочую активность персонала
- **Помогает принимать** обоснованные управленческие и кадровые **решения**
- **Позволяет быстро расследовать инциденты** и привлекать нарушителей к ответственности
- **Помогает корректировать расходы** на закупку программного обеспечения

ЧТО НОВОГО В INFOWATCH PERSON MONITOR

ВОЗМОЖНОСТИ:

- Новый мобильный агент: перехват URL, звонков и много другого, активность пользователя
- Отчеты «Геолокация» и «Лента активности»
- Выявление майнеров информация об использовании CPU/GPU
- Поддержка Skype for Desktop, WebSkype
- Получение уведомлений в Telegram

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

Для риск-менеджеров, ИБ-, ИТ-специалистов, сотрудников отдела подбора персонала :

- Точная идентификация нарушителей и нелояльных сотрудников
- Мониторинг рабочей активности
- Контроль внутренних ресурсов компании и ИТ-инфраструктуры

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

Для руководителей бизнеса, топ-менеджеров:

- Целесообразное расходование ФОТа
- Сокращение нецелевого использования ресурсов компании
- Снижение риска непреднамеренной потери и кражи данных

ЗАЩИТА ОТ ВНЕШНИХ АТАК

ПОЧЕМУ ЭТО ВАЖНО

INFOWATCH

30% сайтов

содержат известные уязвимости

в 10 раз

снизилась минимальная стоимость DDoS-атаки за последние четыре года

в 43% случаев

DDoS-атака является лишь прикрытием для других вредоносных операций

6 млн рублей

составляет средний ущерб от одной атаки для компаний малого и среднего бизнеса

По данным Qrator Labs, Wallarm, anti-malware.ru, «Лаборатории Касперского»

АТАКА НА ИТ-РЕСУРСЫ ОРГАНИЗАЦИИ

INFOWATCH®

ДЕЙСТВУЮЩИЕ ЛИЦА:

Группа хакеров

СЦЕНАРИЙ:

Группа хакеров **взломала сервер** департамента Министерства обороны.

Злоумышленники **опубликовали данные** по обеспечению государственного оборонного заказа

ПОСЛЕДСТВИЯ:

ущерб репутации, финансовые потери

КАК ЗАЩИЩАТЬСЯ

INFOWATCH®

Выявлять уязвимости

в программном коде заказного ПО

Обнаруживать слабые места

в веб-инфраструктуре

Использовать технические средства защиты

от внешних атак на веб-ресурсы организации

INFOWATCH ATTACK KILLER

INFOWATCH
ATTACK KILLER

Система непрерывной защиты веб-ресурсов. Решение минимизирует человеческий фактор и обеспечивает своевременную защиту от постоянно развивающихся технологий взлома

- **Автоматическое обнаружение** и предотвращение DDoS-атак
- **Обнаружение уязвимостей** веб-инфраструктуры
- **Автоматизированный контроль** качества исходного кода программ
- **Обеспечение доступности** веб-ресурса

INFOWATCH ATTACK KILLER

INFOWATCH APPERCUT

Система автоматизированного контроля исходного кода бизнес-приложений на соответствие требованиям по безопасной разработке программного обеспечения

- **Проверка качества кода** и поиск уязвимостей еще на этапе программирования
- **Автоматическое создание отчетов** о найденных уязвимостях и формирование задачи для программистов
- **Обеспечение безопасного ввода в эксплуатацию** и обновление программного обеспечения

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

Для риск-менеджеров, ИБ-, ИТ-специалистов, сотрудников отдела экономической безопасности:

- Совместная интеграция решений по защите от различных внешних атак
- Выявление уязвимостей в разрабатываемом ПО
- Простота управления и настройки решения

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

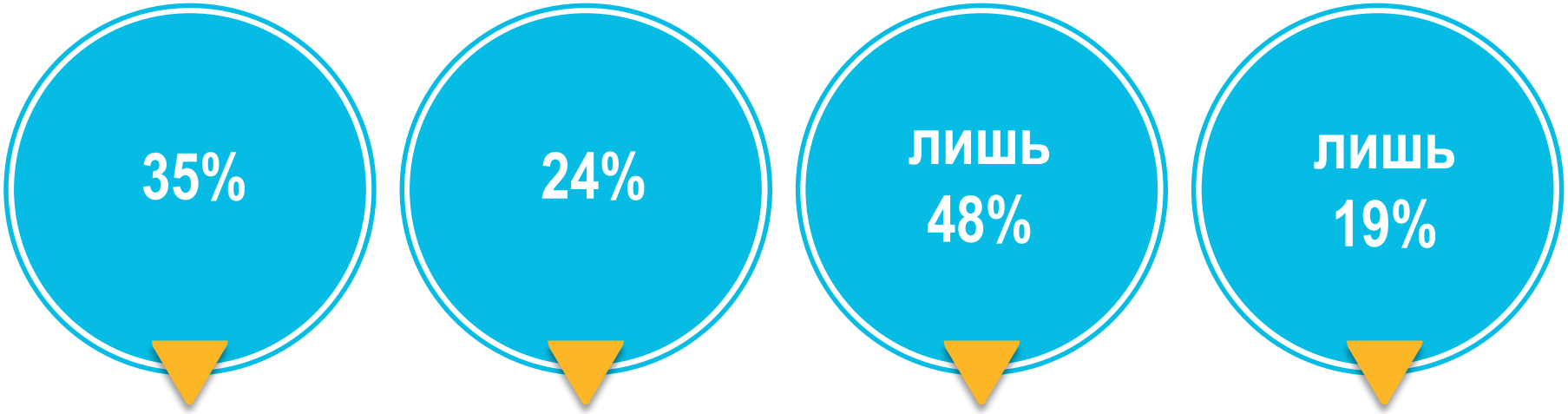
Для руководителей бизнеса, топ-менеджеров:

- Непрерывность бизнес-процессов и доступность ресурсов компании
- Сокращение затрат на разработку приложений
- Обеспечение целостности конфиденциальных данных

КОМПЛЕКСНАЯ ЗАЩИТА АСУТП

ПОЧЕМУ ЭТО ВАЖНО

INFOWATCH



предприятий считают вымогательство главным вектором атаки на АСУТП

организаций считают контроллеры со встраиваемой системой наибольшим риском

предприятий приводят внутренние стандарты ИБ в соответствие с NIST Cyber Security Framework

организаций уверены, что их АСУТП не была успешна атакована за последние 12 месяцев

По данным SANS 2017 State of ICS Security Survey

КАК ЗАЩИЩАТЬСЯ

INFOWATCH®

Обеспечить межсетевое экранирование

на канальном, сетевом, транспортном и прикладном уровне

Провести инвентаризацию устройств

выявить слабые места технологической сети

Построить схему средств защиты

включая все узлы и агрегаты ИТ-системы

INFOWATCH AUTOMATION SYSTEM ADVANCED PROTECTOR

INFOWATCH

INFOWATCH ASAP

Специализированный программно-аппаратный комплекс, предназначенный для создания систем защиты АСУТП и адаптированный к использованию в технологических сетях

ПАК InfoWatch ASAP может функционировать в двух основных режимах:

- **Фоновый** — выполняет мониторинг трафика, подаваемого на вход ПАК InfoWatch ASAP, и информирует оператора об инцидентах
- **Активный** — предотвращает вредоносное воздействие

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

Для риск-менеджеров, ИБ-, ИТ-специалистов, сотрудников отдела подбора персонала :

- Выявление атак на отказ средств автоматизации
- Обнаружение вторжений и аномалий технологического процесса
- Выявление несанкционированного подключения устройств в технологическую сеть

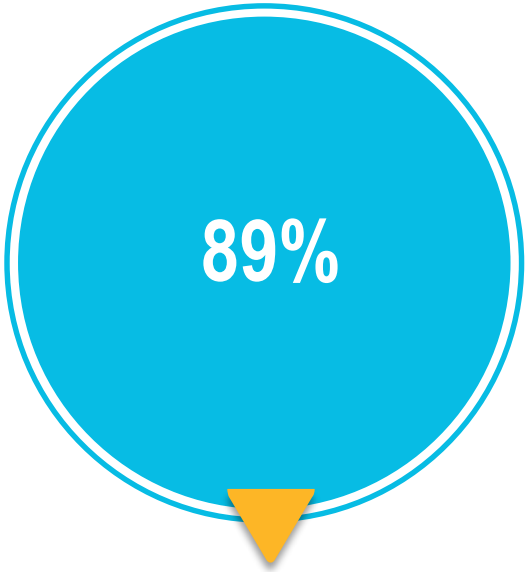
ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

Для руководителей бизнеса, топ-менеджеров:

- Формирование требований к системе защиты АСУТП
- Обеспечение непрерывности технологических процессов и процессов производства

ЗАЩИТА ОТ ИНФОРМАЦИОННЫХ АТАК

ПОЧЕМУ ЭТО ВАЖНО



пользователей Интернета в России имеют аккаунты в соцсетях

русскоязычных сообщений в сутки в русскоязычных аккаунтах

в день пользователь в среднем проводит в социальных сетях

КАК ЗАЩИЩАТЬСЯ

INFOWATCH®

Отслеживать информационные атаки

о ситуации в регионе, персоне и организации

Вовремя публиковать опровержения

и разъяснять суть атаки

Отслеживать распространение негатива

о бренде, должностных лицах, сотрудниках

INFOWATCH KRIBRUM

INFOWATCH KRIBRUM

Автоматизированная система мониторинга и анализа социальных медиа

- **Отслеживает обсуждения** персоны/ компании/ продукта в Сети, информационные атаки и «вбросы»
- **Определяет источники и каналы распространения** негативной информации
- **Выявляет неэтичное поведение** сотрудников в Сети

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

INFOWATCH®

Для риск-менеджеров, ИБ-, ИТ-специалистов, сотрудников отдела подбора персонала :

- Контроль коммуникаций сотрудников в социальных сетях
- Выявление подозрительной активности и инцидентов информационной безопасности
- Структурирование различной информации, возможность оперативной обработки негативных отзывов

ПРЕИМУЩЕСТВА КОМПЛЕКСНОГО РЕШЕНИЯ

Для руководителей бизнеса, топ-менеджеров:

- Быстрое реагирование на инциденты
- Управление репутацией бренда и ключевых лиц компании
- Прозрачная история общения с клиентов во всех каналах

ПОЧЕМУ INFOWATCH

КОМПЛЕКСНОЕ РЕШЕНИЕ

INFOWATCH®

- **Учитывает особенности** бизнес-процессов компании: предустановленные политики, базы контентной фильтрации отрасли
- **Защищает критически важную информацию** и персональные данные клиентов
- **Выявляет нелояльных сотрудников** и злоумышленников, сговоры, мошеннические схемы
- **Снижает репутационные риски**, связанные с возможными утечками информации в социальных сетях
- Техническая **поддержка и обучение** специалистов компании в центре InfoWatch
- **Эксперты в области** информационной безопасности с более чем 1500 успешных внедрений

ПОЧЕМУ INFOWATCH

INFOWATCH®

Один из лидеров рынка защиты данных более 15 лет

Сертификаты ФСБ и ФСТЭК

Отечественная разработка

Помогает соответствовать требованиям законодательства РФ

ЭТИ КОМПАНИИ УЖЕ ИСПОЛЬЗУЮТ НАШИ РЕШЕНИЯ

INFOWATCH®

Банки и финансы

СБЕРБАНК Всегда рядом
Райффайзен БАНК
Связь Банк
Банк Кольцо Урала
HOME CREDIT BANK
Банк Москвы
БелгазпромБанк

Государственный сектор

Федеральная Таможенная Служба
Министерство обороны Российской Федерации
Федеральная налоговая служба
Фонд Социального Страхования
Правительство Тульской области

Фармацевтика

STADA CIS
акрихин Люди заботятся о Людях
НИАРМЕДИК

Энергетика

РУСЭНЕРГО РЕСУРС
ЭЛЕКТРОГЕНЕРАЦИЯ ИНТЕР РАО КАШИРСКАЯ ГРЭС
e·on
ТВЭЛ
РУСЭНЕРГОСБЫТ

Нефтегазовый сектор

Газпром автоматизация
СлавНефть
Газпром ВНИИГАЗ
Транснефть
СНГ
ЛУКОЙЛ НЕФТЯНАЯ КОМПАНИЯ

Транспорт и логистика

РОСЖЕЛДОР ПРОЕКТ
Газпром авиа
SPSR express

Промышленность

ОБЪЕДИНЕННАЯ ДВИГАТЕЛЕСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ
ОБОРОНПРОМ
lira
Московский вертолетный завод им. М.Л. Миля

Страхование

ВСК СТРАХОВОЙ ДОМ
СОГАЗ СТРАХОВАЯ ГРУППА

Торговля

МИР КНИГИ .RU
МАГНИТ
magnum cash & carry
KUPIVIP.RU
FIX price
дикси

Телекоммуникации

МегаФон Точикистон
МТС
ВГТРК
Билайн

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

06 СЕНТЯБРЯ
2018
ВЛАДИВОСТОК

#CODEIB

Самойленко Никита

Менеджер по работе с клиентами
И партнерами в ДФО

ТЕЛЕФОН: +7 (962) 227-42-45

INFOWATCH®

EMAIL: **Nikita.Samoylenko@infowatch.com**