INFOWATCH®

ARMA IF

INFOWATCH ARMA INDUSTRIAL FIREWALL

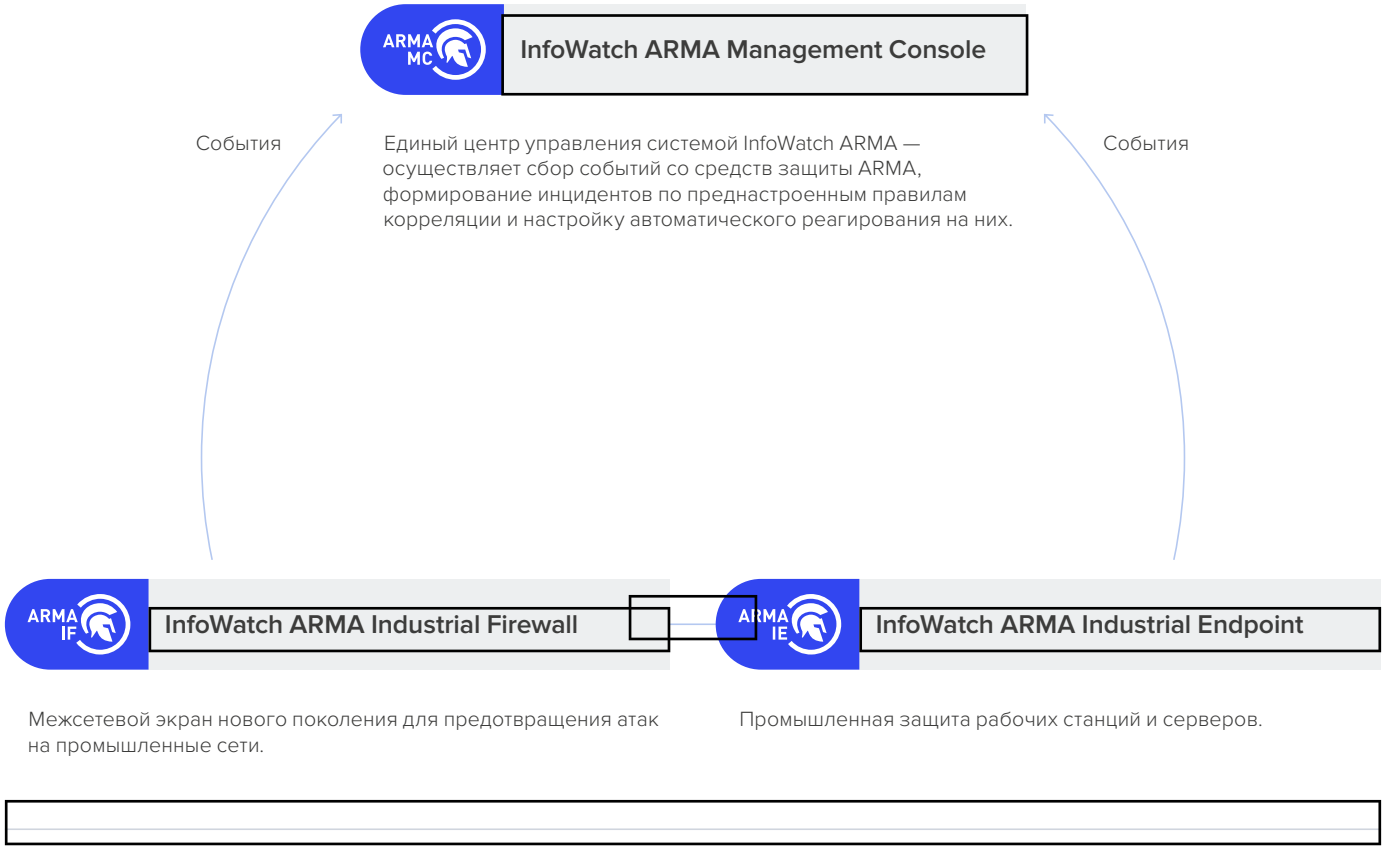
Промышленный межсетевой экран для защиты сетей АСУ ТП

Sk

Участник

Эшелонированная защита с межсетевым экраном InfoWatch ARMA

InfoWatch Industrial Firewall является частью единой системы InfoWatch ARMA. Использование единой системы уменьшает поверхность для атаки злоумышленника и позволяет выполнить до 90% технических требований ФСТЭК России (Приказ № 239).



Сертификация ФСТЭК России

Межсетевой экран типа «Д» четвёртого класса защиты (ИТ.МЭ.Д4.ПЗ)

Система обнаружения вторжений уровня сети четвёртого класса защиты (ИТ.СОВ.С4.ПЗ)

Включён в единый реестр российского ПО Минкомсвязи РФ

№4429. Действителен до 27 июля 2026

Основные возможности для защиты промышленной сети с InfoWatch ARMA Industrial Firewall

Система обнаружения и предотвращения вторжений (СОВ), IPS / IDS

- Собственная база сигнатур постоянно пополняется командой экспертов InfoWatch ARMA — позволяет обнаруживать попытки эксплуатации как классических, так и специфических уязвимостей
- Возможно самостоятельно дополнять базу СОВ пользовательскими правилами для максимальной защиты компании

Глубокая инспекция промышленных протоколов
Modbus TCP
Modbus TCP x90 func. code (UMAS)
S7 Communication
S7 Communication plus
OPC DA
OPC UA
IEC 60870-5-104
IEC 61850-8-1 MMS
IEC 61850-8-1 GOOSE
KRUG
Profinet (без возможности фильтрации)

Глубина проработки, а также объём поддерживаемых функций и параметров приведены в техническом описании InfoWatch ARMA Industrial Firewall на сайте arma-firewall.infowatch.ru

Глубокий анализ промышленного трафика (DPI)

Качественное обнаружение и предотвращение вторжений в АСУ ТП невозможно без глубокого анализа промышленного трафика.

- Даёт возможность сократить информационные потоки только до регламентированных и уменьшить количество ложных срабатываний
- Позволяет работать с трафиком на уровне команд протоколов и настроить защиту под свои задачи. Благодаря детальному разбору трафика до уровня команд и их значений можно настроить автоматическую блокировку вредоносных пакетов в трафике от источника угрозы
- Обеспечивает высокую видимость сети: позволяет детально зафиксировать действия пользователей и работу систем и своевременно отреагировать на киберугрозы

Два основных сценария, которые используют наши клиенты

Контроль действий пользователей

Назначайте пользователям права, чтобы контролировать легитимность действий в сети. Например, ограничьте права оператора до функции чтения информации.

Контроль недопустимых операций с ПЛК

Установите запрет на изменения в системе — блокировку или оповещение при попытке загрузки программы управления или обновления операционной системы ПЛК.

Анализ трафика с помощью потокового антивируса

Проводит сканирование потока данных в промышленной и корпоративной сети, обнаруживает вредоносные объекты (вирусы, вредоносные скрипты, трояны и другие угрозы) и блокирует их на сетевом уровне. Антивирусные базы регулярно обновляются для обнаружения актуальных угроз.

Безопасное удалённое подключение по ГОСТ-VPN

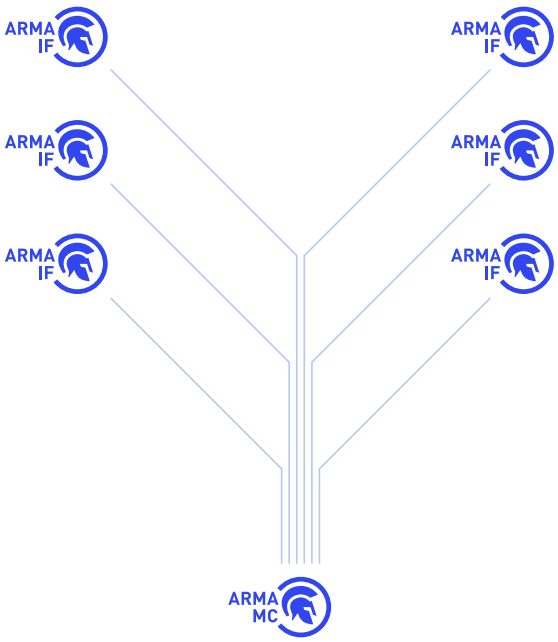
Обеспечивает безопасность передачи данных при объединении в единую сеть филиалов предприятия, удалённом подключении к производственной площадке или при работе технической поддержки.

Динамическая маршрутизация трафика

Предусмотрена поддержка протоколов динамической маршрутизации: OSPF, RIP, BGP.

Централизованное управление всеми межсетевыми экранами в сети с InfoWatch ARMA Management Console

Все межсетевые экраны InfoWatch ARMA Industrial Firewall подключаются к единому центру управления и автоматизации реагирования на инциденты InfoWatch ARMA Management Console. Для тех, у кого установлены десятки межсетевых экранов, централизованное администрирование позволяет экономить ресурсы специалистов ИБ благодаря нескольким возможностям:



InfoWatch ARMA Management Console

Централизованный сбор событий

События передаются в единый интерфейс и из них автоматически генерируются инциденты, основываясь на преднастроенных правилах корреляции в InfoWatch ARMA Management Console.

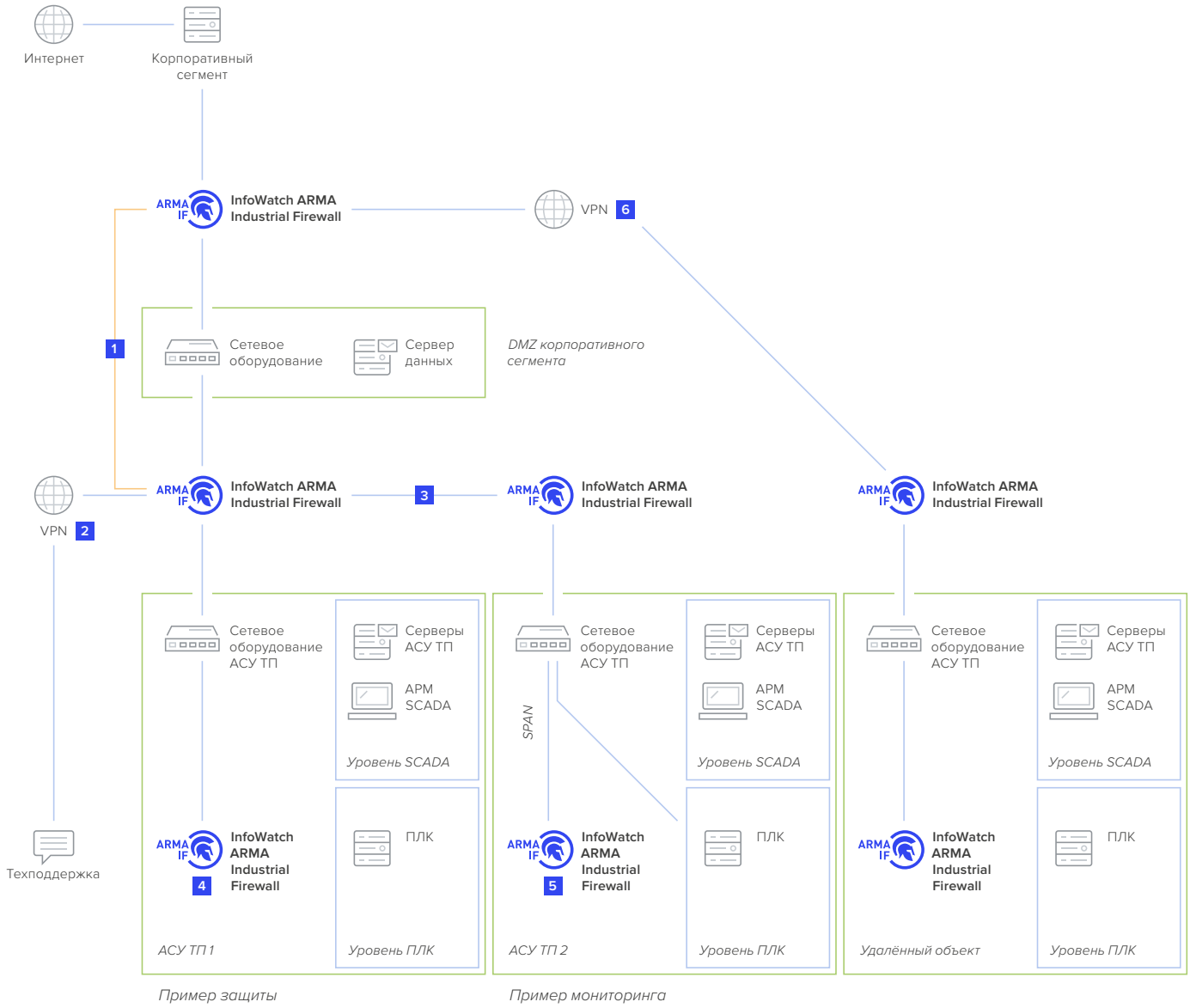
Автоматизация настройки политик

Достаточно настроить политики на одном межсетевом экране и тиражировать на остальные для экономии времени.

Централизованное обновление правил СОВ

Регулярная процедура — должна быть автоматизирована, чтобы не занимать время специалиста ИБ.

Примеры установки InfoWatch Industrial Firewall



1. Защита АСУ ТП на границе с корпоративным сегментом
2. Защита каналов технической поддержи
3. Защита обособленных и смежных АСУ ТП
4. Защита сети между SCADA и ПЛК
5. Защита внутри АСУ ТП
6. Защита удалённого подключения

Технические функции

Межсетевой экран

- Фильтрация по: адресу источника, адресу назначения, протоколам, портам, операционной системе
- Каждое правило может задавать свои настройки ограничения одновременных соединений
- Каждое правило может определять свои настройки журналирования трафика
- Нормализация пакетов
- Возможность включения режима чистого маршрутизатора
- Сбор и отображение статистики для всех правил межсетевого экрана
- Отображение автоматических правил межсетевого экрана в веб-интерфейсе

Организация политик

- Поддержка псевдонимов / Alias: для IP-адресов, диапазонов портов, доменных имён (полностью определённое доменное имя / FQDN)
- Возможность создания зон безопасности с помощью правил, ссылающихся на интерфейсные группы
- Категории правил
- Поддержка GeoIP (определение страны)

Гибкий контроль таблицы состояний

- Настраиваемый размер таблицы состояний
- Каждое правило может задавать свои настройки:
  - Ограничения одновременных подключений от клиента
  - Ограничения состояний для конкретного хоста
  - Ограничения на количество новых соединений в секунду
  - Таймаута для состояний соединения
  - Режима работы с соединениями
- Режимы работы с соединениями:
  - Keep (режим отслеживания состояния соединения)
  - Sloppy (менее строгий режим отслеживания состояния соединения)
  - Modulate (генерация высококачественных Initial Sequence Number)
  - Synproxy (режим защиты от атаки типа TCP YSN Flood)
  - None (режим работы без отслеживания состояния соединения)
  - Оптимизация работы с соединениями:
  - Normal (нормальный режим подходит для большинства сетей)
  - High latency (режим высокой задержки — подходит для спутниковых каналов связи)
  - Aggressive (агрессивный режим — соединения истекают быстрее, тратится меньше памяти)
  - Conservative (консервативный режим — соединения истекают медленнее, тратится больше памяти)

Аутентификация

- Удалённые серверы: LDAP, RADIUS
- Синхронизация пользователей с Active Directory
- Настройка прозрачной аутентификации (SSO)
- Локальный менеджер пользователей: ваучеры / карты

Авторизация

- Веб-интерфейс: локальный менеджер пользователей

Аккаунтинг

- Ваучеры / карты

Двухфакторная аутентификация

- Поддержка TOTP (одноразовых паролей с ограничением по времени)
- Поддержка 2FA-аутентификации в Captive Portal, веб-прокси, VPN, веб-интерфейсе, SSH / консоли

Сертификаты

- Удостоверяющий центр:
  - Создание или импортирование удостоверяющего центра
  - Создание или импортирование сертификатов

Поддержка 802.1Q VLAN

- Максимальное поддерживаемое число VLAN-сетей — 4096

Агрегирование каналов и переключение при сбое

- Переключение при сбое
- CARP
- Циклический алгоритм (Round Robin)
- Технология Ether Channel (FEC) от Cisco
- Протокол LACP из стандарта IEEE 802.3AD

Поддержка других типов интерфейсов

- Мостовые интерфейсы

Трансляция сетевых адресов (NAT)

- Перенаправление портов
- Поддержка NAT Reflection (обращение к серверам из внутренней сети по публичным IP-адресам)
- Логирование правил NAT
- Исходящий NAT

Шейпер трафика (Traffic Shaping)

- Ограничение пропускной способности
- Разделение пропускной способности
- Приоритезация трафика
- Критерии совпадения правил: протокол, адрес источника, адрес назначения, порт, направление

Dynamic DNS

- Выбор сервиса Dynamic DNS из списка
- Произвольно настраиваемый сервис

DNS-форвардер

- Переопределения для хостов и доменов

DNS-сервер

- Переопределения для хостов — ресурсных записей типов A и MX
- Списки доступа
- Поддержка DNSSEC

DNS-фильтрация

- Поддержка OpenDNS

DHCP-сервер

- Поддержка IPv4 и IPv6
- Поддержка режима ретрансляции
- Поддержка BOOTP-опций

MultiWAN

- Балансировка нагрузки
- Переключение на запасной канал при сбое основного канала
- Псевдонимы / Alias

Network Time Server

- Поддержка Pulse Per Second источника
- Поддержка GPS-источника
- Задание и синхронизация времени по протоколу NTP

Система обнаружения / предотвращения вторжений

- Работа в режиме inline (устройство, выполняющее функцию, находится на пути трафика, а не в стороне)
- Предопределённые правила
- Блокировка сайтов по цифровым отпечаткам SSL-сертификатов
- Автообновление правил с помощью планировщика Cron
- Экспорт / импорт баз решающих правил локально и по протоколам FTP или SMB

Application Control (контроль приложений)

- Создание правил блокировки / разрешения использования приложений

Layer 7 — фильтрация

- Системо-независимый API для userland-приложений, которые используют низкоуровневые механизмы захвата пакетов (libpcap)
- Блокировка трафика, распознанного с помощью DPI и запрещённого в настройках
- Правила для отчёта и блокировки приложений по отдельным подсетям
- Каждое правило может работать в режиме только отчёта или режиме блокировки

Captive Portal

- Сценарии использования:
  - Гостевая сеть

- BYOD (мобильное рабочее место)
- Wi-Fi-доступ в отелях и кемпингах
- Управление шаблонами
- Поддержка нескольких зон

- Аутентификаторы (работает со всеми поддерживаемыми в системе аутентификаторами)
- Менеджер ваучеров:
  - Поддержка нескольких баз данных ваучеров
  - Экспортирование ваучеров в формат CSV
  - Таймауты и распознавание зарегистрированных пользователей
- Управление пропускной способностью с помощью шейпера
- Обход портала по белым спискам IP- и MAC-адресов
- Отчёты в реальном времени:
  - Топ-лист по IP-адресам с наибольшим использованием пропускной способности канала
  - Активные сессии
  - Оставшееся время
  - Интерфейс программирования REST

Виртуальные частные сети

- IPsec / OpenVPN / OpenVPN-ГОСТ: в режиме «сеть — сеть» и в режиме «узел — сеть» (подключение удалённых сотрудников)
- Экспорт конфигурации для лёгкой настройки клиента
- OpenVPN client export API для автоматизации процесса выдачи клиентских сертификатов для OpenVPN

Высокая доступность

- Переключение на запасной узел в кластере высокой доступности
- Loop Protection. Технологии STP и RSTP
- Синхронизация таблицы состояния соединений между узлами кластера
- Синхронизация настроек между узлами кластера

Кеширующий прокси

- Поддержка нескольких интерфейсов
- Режим прозрачного проксирования
- Создание списка разрешённых сайтов для варианта «запрещено всё» в режиме прозрачного проксирования
- Списки контроля доступа, чёрные списки ресурсов
- Управление трафиком
- Поддержка скачиваемых чёрных списков
- ICAP (поддержка внешних антивирусов)
- Запись логов в БД, гибкая отчётность по доменам, URL, пользователям, IP-адресам и т. д.
- Логирование трафика пользователей OpenVPN с привязкой к пользователю
- Гибкая настройка правил пользователей и групп (приоритеты, чёрные / белые списки, правила ICAP, маршрутизация на разные интернет-каналы)
- Возможность формирования списка исключений для доступа к сайтам, имеющим собственные (самоподписанные) SSL-сертификаты. Список сайтов (доменов) устанавливается администратором вручную при настройке универсального шлюза безопасности
- Возможность принудительного ограничения пропускной способности прокси-сервера для отдельных пользователей

Настройка реверс-прокси (Nginx)

Антивирусная проверка

- Поддержка интеграции с внешними антивирусами с помощью ICAP
- ClamAV (встроенный антивирус, работает со Squid через плагин C-ICAP)
- Резервное копирование и восстановление
- История изменений настроек

Резервное копирование файлов

- Сохранение резервных копий конфигурации на выделенный FTP-сервер

SNMP

- Мониторинг и ловушки

Диагностика

- Статус перезагрузки фильтров
- Информация по сетевому экрану
- Топ по активным пользователям
- Таблицы сетевого экрана:
  - Псевдонимы / Alias
  - Bogon-сети (немаршрутизируемые в интернете адреса)
- Текущие открытые сокеты
- Просмотр состояний всех соединений
- Сброс таблицы состояний
- Общие данные по состояниям соединений
- Технология Wake on LAN (пробуждение компьютера при получении пакета по сети)
- ARP-таблица (кэш протокола преобразования адресов)
- Просмотр данных в DNS
- NDP-таблица (кэш протокола обнаружения соседей)
- Утилита PING
- Захват пакетов
- Сканирование портов
- Трассировка маршрутов

Мониторинг

- Monit — проактивный мониторинг системы

Усовершенствованная система отчётов

- Анализатор потоков Insight:
  - Полностью интегрирован в решение
  - Детальная агрегация данных
  - Графическая репрезентация данных
  - Поддержка поиска и кликабельность
  - Экспорт в формат CSV
- Здоровье системы:
  - Работа с собираемыми данными по циклическому алгоритму
  - Возможность выбора и масштабирования
  - Возможность экспорта
- Графики трафика (мониторинг трафика в реальном времени)
- Hardware widget — предоставление сведений об аппаратной платформе

Мониторинг сети

- NetFlow Exporter версий 5 и 9 (поставляет данные в Insight)

Интерфейс программирования REST

- Поддержка списков контроля доступа (ACL)
- API-правила
- Получение логов в форматах Syslog и CEF

ARMA Management Console

- Централизованная панель управления несколькими узлами на головном узле

Поддержка протоколов динамической маршрутизации

- RIPv.1, RIPv.2, OSPFv2 и OSPFv3, BGP

Поддерживаемые промышленные протоколы

- Возможность фильтрации:
  - OPC UA
  - OPC DA
  - S7 Communication
  - S7 Communication plus
  - Modbus TCP
  - Modbus TCP x90 func. code (UMAS)
  - IEC 60870-5-104
  - IEC 61850-8-1 MMS
  - IEC 61850-8-1 GOOSE
  - Profinet (без глубокой фильтрации)
  - KRUG

Дополнительные возможности

- Интеграция с DLP InfoWatch Traffic Monitor
- Интеграция с песочницами по ICAP

Онлайн-документация

- В свободном доступе на русском языке, с поддержкой поиска

Запросите персональное демо
и узнайте все возможности
системы InfoWatch ARMA

arma.infowatch.ru

sales@infowatch.ru
+7 495 22 900 22

INFOWATCH®

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

ИНФОРМ Ростех

ГАЗПРОМ ВНИИГАЗ

Райффайзен БАНК

HOME CREDIT BANK

МТС БАНК

СОГАЗ СТРАХОВАЯ ГРУППА

e·on

МОСКОВСКИЙ ВЕРТОЛЕТНЫЙ ЗАВОД ИМ. М.Л. МИЛЯ

СУХОЙ

ОДК

О'КЕЙ

SPSR express

STADA

НИАРМЕДИК Сеть семейных клиник

МАГНИТ