INFOWATCH® ARMA ARMA

КИБЕРУСТОЙЧИВОСТЬ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В ПОСТКОВИДНУЮ ЭРУ

Что изменилось в ИБ АСУ ТП и как соответствовать новой реальности

Дмитрий Аносов

Генеральный директор InfoWatch ARMA

INFOWATCH®

ИЗМЕНЕНИЯ В ИБ АСУ ТП, КОТОРЫЕ МЫ ВИДИМ В 2021

Современные вызовы кибербезопасности

INFOWATCH®

→ **«Размытие» периметра — кибератаки гигантского размера**

Цифровизация и гибридная архитектура: IT- и OT-сети управляются компонентами, которые взаимодействуют с физическими объектами (киберфизические системы)

→ **Ограниченная видимость сети**

Разновендорный парк без единого центра управления и расследования инцидентов: долгая реакция на инцидент, отсутствие полной картины происходящего в сети. Как вы защитите то, что не видите?

→ **Недостаток квалифицированных кадров**

Кадровый «голод», «профессиональное выгорание» существующего штата ИБ: высокая нагрузка, рассогласованность действий служб ИТ и ИБ

→ **Требования законодательства ужесточаются**

Что нового в постковидной эре?

- → 2020 показал: **киберпреступники могут получить неограниченный доступ** к любому устройству, работающему в сети — научились прокладывать путь от АСУ ТП к рабочим станциям и ПЛК
- → **Сегодня не только промышленные сети, но и рабочие станции АСУ ТП** уже имеют подключения к ИТ-сетям и доступ к цеху и ПЛК. Именно они часто становятся начальной точкой атаки.
- → Киберпионеры вслед за хакерами **обратили пристальное внимание на сетевые ресурсы и активы компаний, которые «торчат наружу».** Дело РЖД.

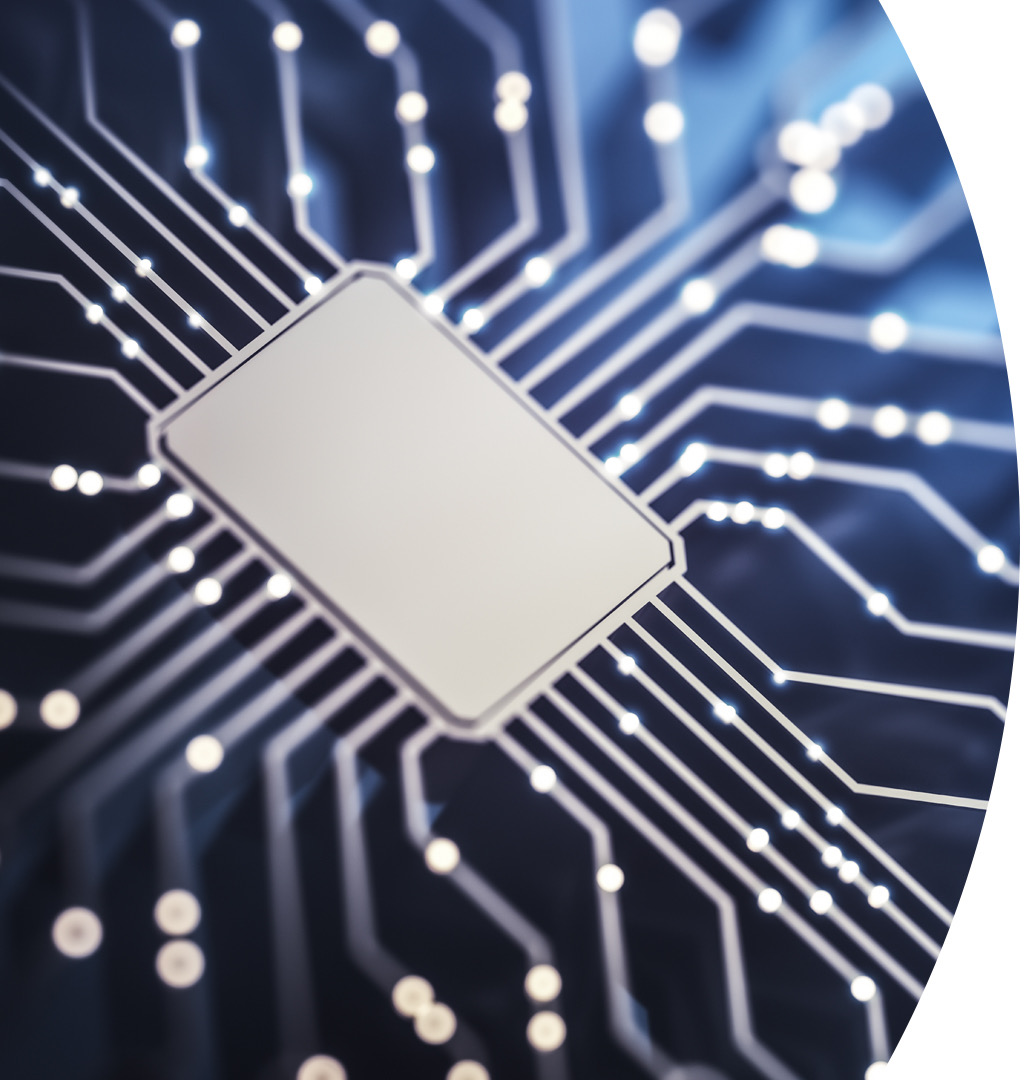
Подходы к атакам в 2021

- → Атаки на цепочку поставок (Supply Chain)
- → Атаки по сети (используя уязвимости ПАЗ, ПЛК, SCADA)
- → Атаки через сервисные каналы

«Времени на раскачку нет»

С января 2021 — госконтроль!

1. Прокуратурой
2. Профильными федеральными органами исполнительной власти
3. Органами госвласти субъектов РФ
4. Официальное взаимодействие напрямую



Неизменными остаются лишь задачи штата ИБ

- **Обеспечить защиту АСУ ТП** от компьютерных атак
- **Выполнить требования** регулятора
- **Автоматизировать работу** отдела ИБ

Кибербезопасность с InfoWatch ARMA в постковидной реальности

1. Эшелонированная защита

Чем больше эшелонов защиты, тем меньше шансов у хакера совершить атаку.

Эшелоны на макро- и микроуровне преодолевать долго, дорого, а атака может прерваться в любой момент — для киберпреступников «игра не стоит свеч».

Кибербезопасность с InfoWatch ARMA в постковидной реальности

2. Замкнутая программная среда

Позволяет сохранить непрерывность производственных процессов, даже если вирусу удалось проникнуть в систему.

Не вмешивается в промышленные операции и процессы. Не влияет на вычислительные ресурсы и мощность.

INFOWATCH®

Кибербезопасность с InfoWatch ARMA в постковидной реальности

3. Высокая прозрачность сети и событий в ней

Полнота данных о событиях в сети — залог быстрой реакции на инцидент и предотвращения последствий атаки.

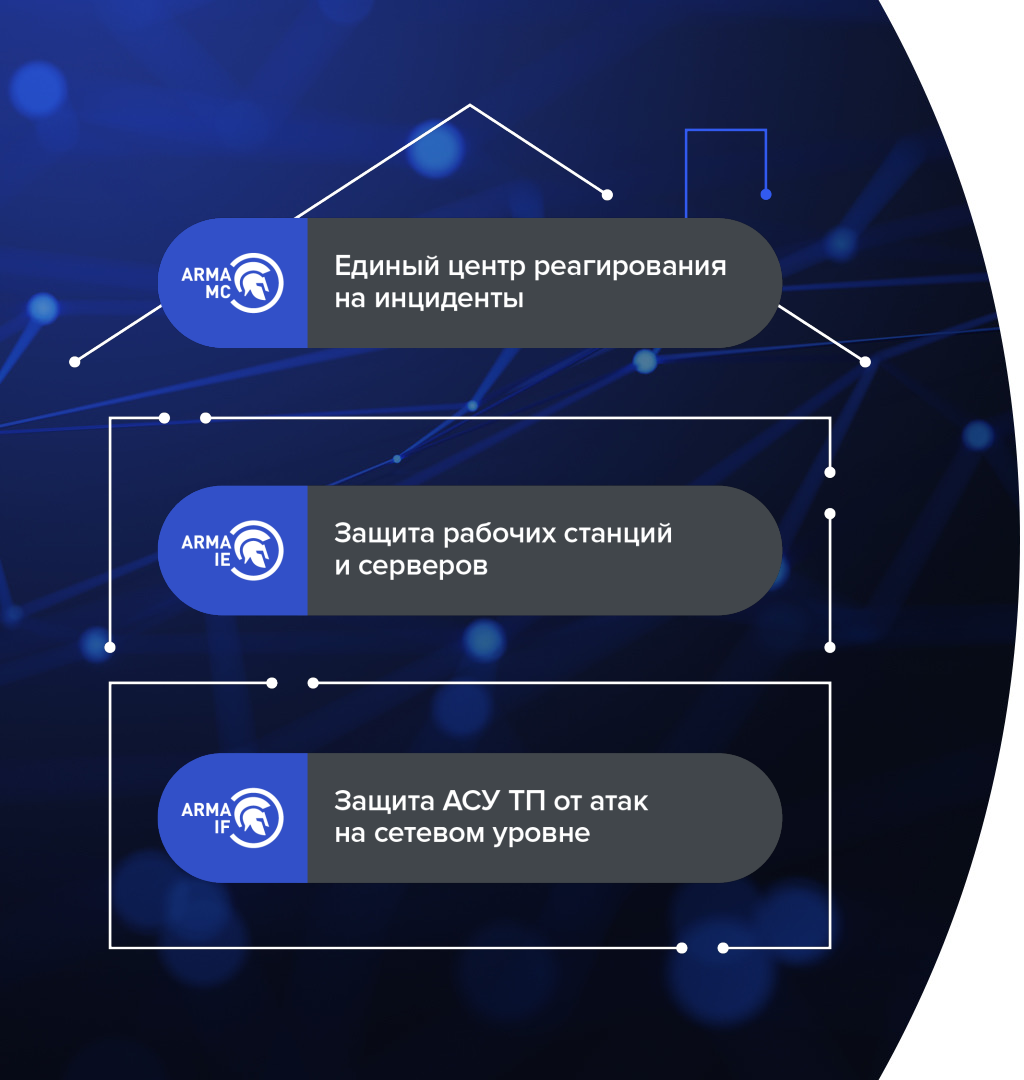
Полнота достигается глубоким анализом трафика и прозрачностью подключений активов к сети. В 2020 удалёнка принесла лавину «теневых» устройств и приложений. То, что вы пока не видите — блокируйте.

Кибербезопасность с InfoWatch ARMA в постковидной реальности

4. Автоматизация процессов защиты

Делегируйте системе работу с большими данных на георазпределенных объектах.

Кадровый «голод», «профессиональное выгорание» существующего штата ИБ из-за нагрузки. Штат ИБ нуждается в балансе нагрузки — оставить специалистам: стратегию защиты, расследование инцидентов, контроль.

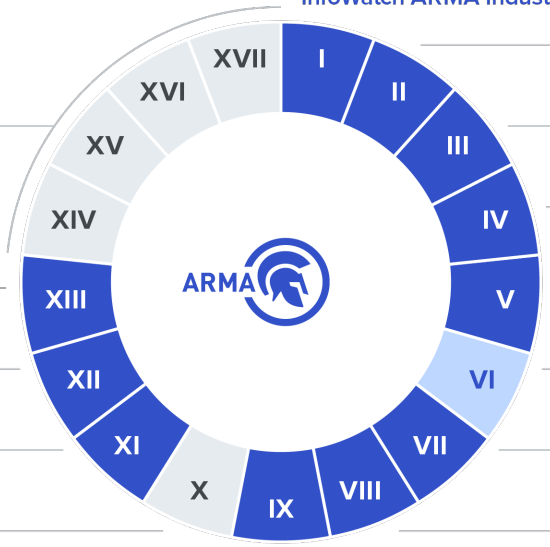


INFOWATCH®

InfoWatch ARMA — комплексная система для обеспечения кибербезопасности АСУ ТП

- Эшелонированная **защита с единым центром управления** системой защиты информации
- Выполнение до **90%** **технических требований** приказа ФСТЭК России № 239
- **Снижение стоимости владения** и ресурсов на сопровождение системы — интегрированность компонентов, моновендорность

До 90% выполнения технических требований Приказа № 239 ФСТЭК России



СОВ
InfoWatch ARMA Industrial Firewall

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Endpoint
InfoWatch ARMA Industrial Endpoint

Endpoint
InfoWatch ARMA Industrial Endpoint

СОВ, МЭ
InfoWatch ARMA Industrial Firewall

Антивирусная защита
в разработке

СОВ
InfoWatch ARMA Industrial Firewall

Endpoint, МЭ
InfoWatch ARMA Industrial Endpoint

МЭ
InfoWatch ARMA Industrial Firewall

Физическая безопасность

Endpoint, МЭ
InfoWatch ARMA Industrial Firewall / Industrial Endpoint

Средства управления инцидентами
InfoWatch ARMA Management Console

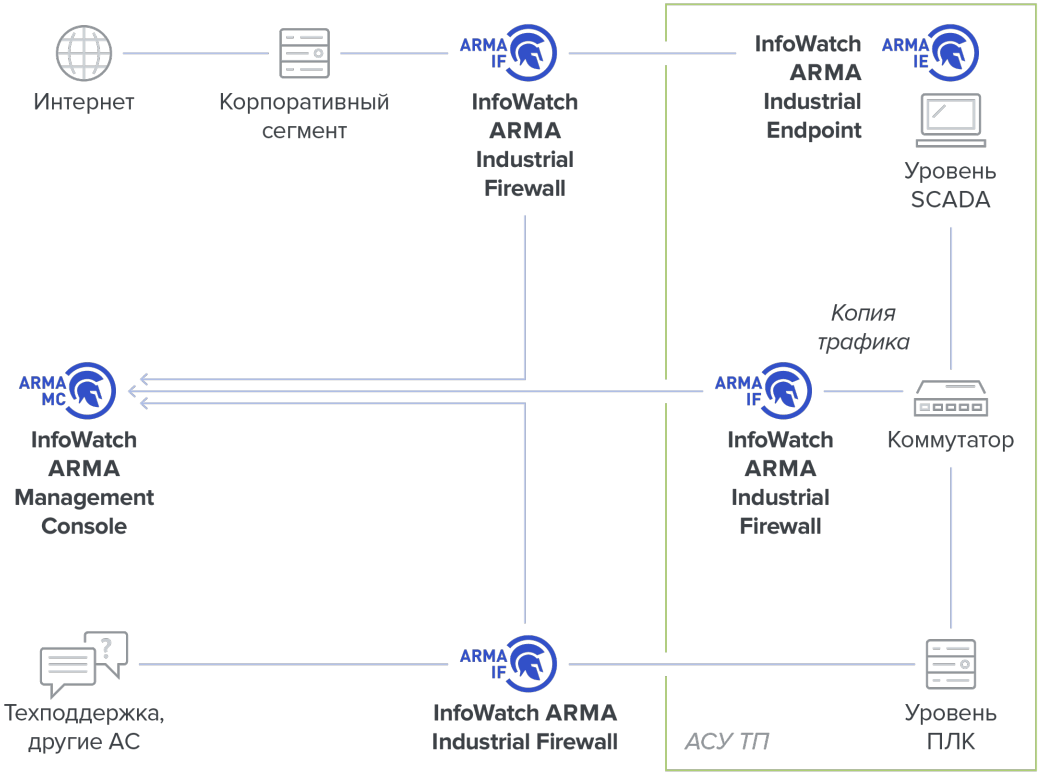
Endpoint
InfoWatch ARMA Industrial Endpoint

Организационные меры

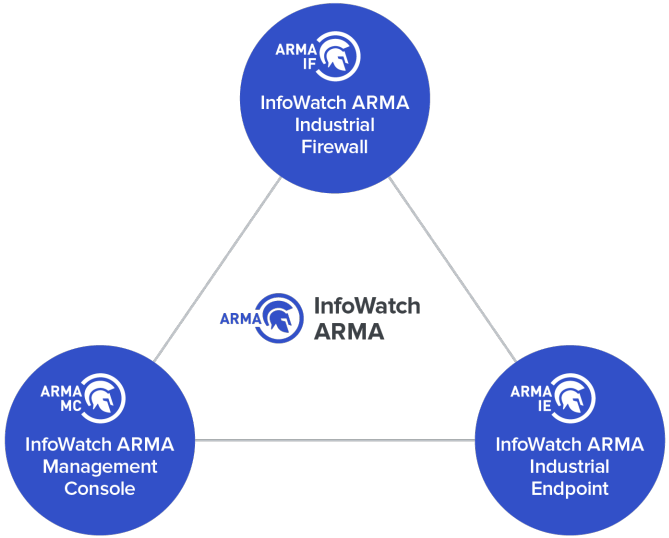
Получите карту соответствия InfoWatch ARMA группам мер ФСТЭК России

Оставьте запрос на сайте
arma.infowatch.ru

Комплексная система — эшелонированная защита и выгода при внедрении



Все продукты интегрированы между собой: могут эксплуатироваться как самостоятельные продукты, так и в комплексе.



Автоматизация процессов кибербезопасности

INFOWATCH®

Промышленный межсетевой экран нового поколения

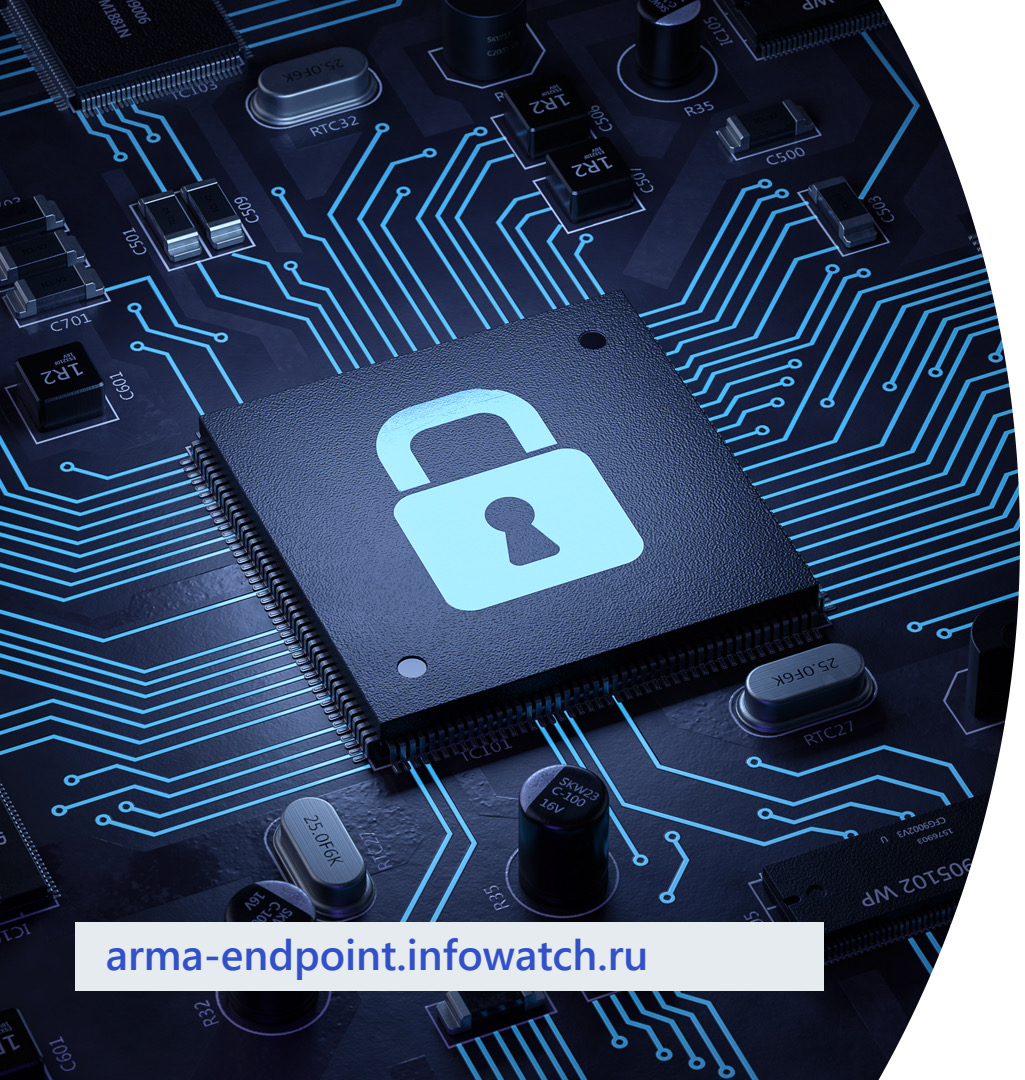
ARMA IF

InfoWatch ARMA Industrial Firewall

Защита КИИ промышленных объектов от сетевых атак

- Проходит сертификацию по 4 классу защиты тип «Д»
- Включён в единый реестр российского ПО Минкомсвязи РФ

arma-firewall.infowatch.ru



INFOWATCH®

Защита рабочих станций и серверов АСУ ТП

ARMA IE

InfoWatch ARMA Industrial Endpoint

Создание замкнутой защищённой среды

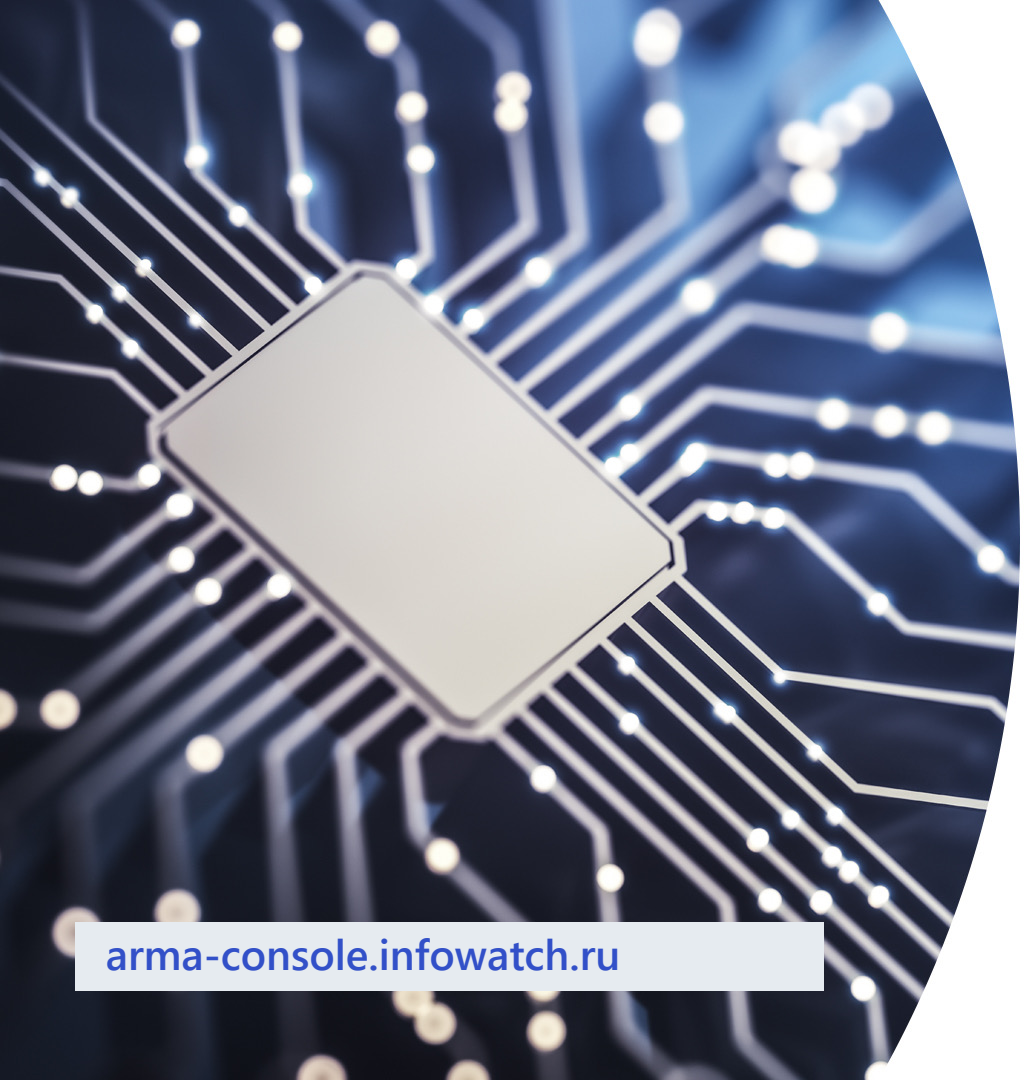
arma-endpoint.infowatch.ru

NEW Новый продукт

arma-endpoint.infowatch.ru

Защита рабочих станций и серверов АСУ ТП

- **Контроль целостности файлов** рабочих станций и серверов АСУ ТП
- **Позволяет ограничивать** главный канал распространения угроз — **USB и другие съёмные носители**
- **Блокировка** любого недоверенного **ПО**



INFOWATCH®

Единый центр управления системой защиты InfoWatch ARMA

InfoWatch ARMA Management Console

Централизованное обновление и управление конфигурациями

arma-console.infowatch.ru

NEW Новый продукт

Единый центр управления системой защиты InfoWatch ARMA

- **Централизованное управление** продуктами InfoWatch ARMA
- **Управление инцидентами ИБ** и их расследование
- **Сбор событий ИБ** и предоставление инцидентов в SOC- и SIEM-системы
- **Автоматическая реакция** на инциденты
- **Визуализация сети**

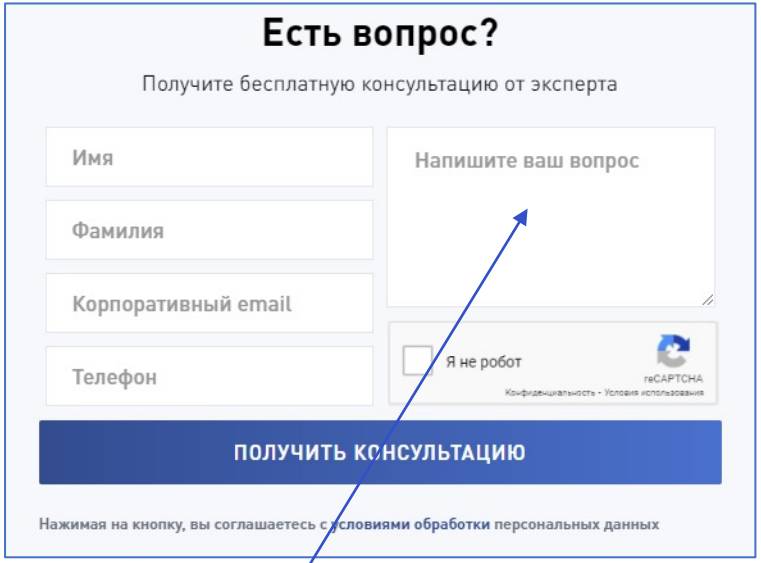
БЕСПЛАТНЫЙ ВОРКШОП

Решение ваших задач ИБ с системой InfoWatch ARMA

Индивидуально проводит
Игорь Душа, технический директор InfoWatch ARMA

/InfoWatchOut /InfoWatch /infowatchnews

Заполните форму здесь:
arma.infowatch.ru



В поле «вопрос» укажите
«воркшоп ARMA»