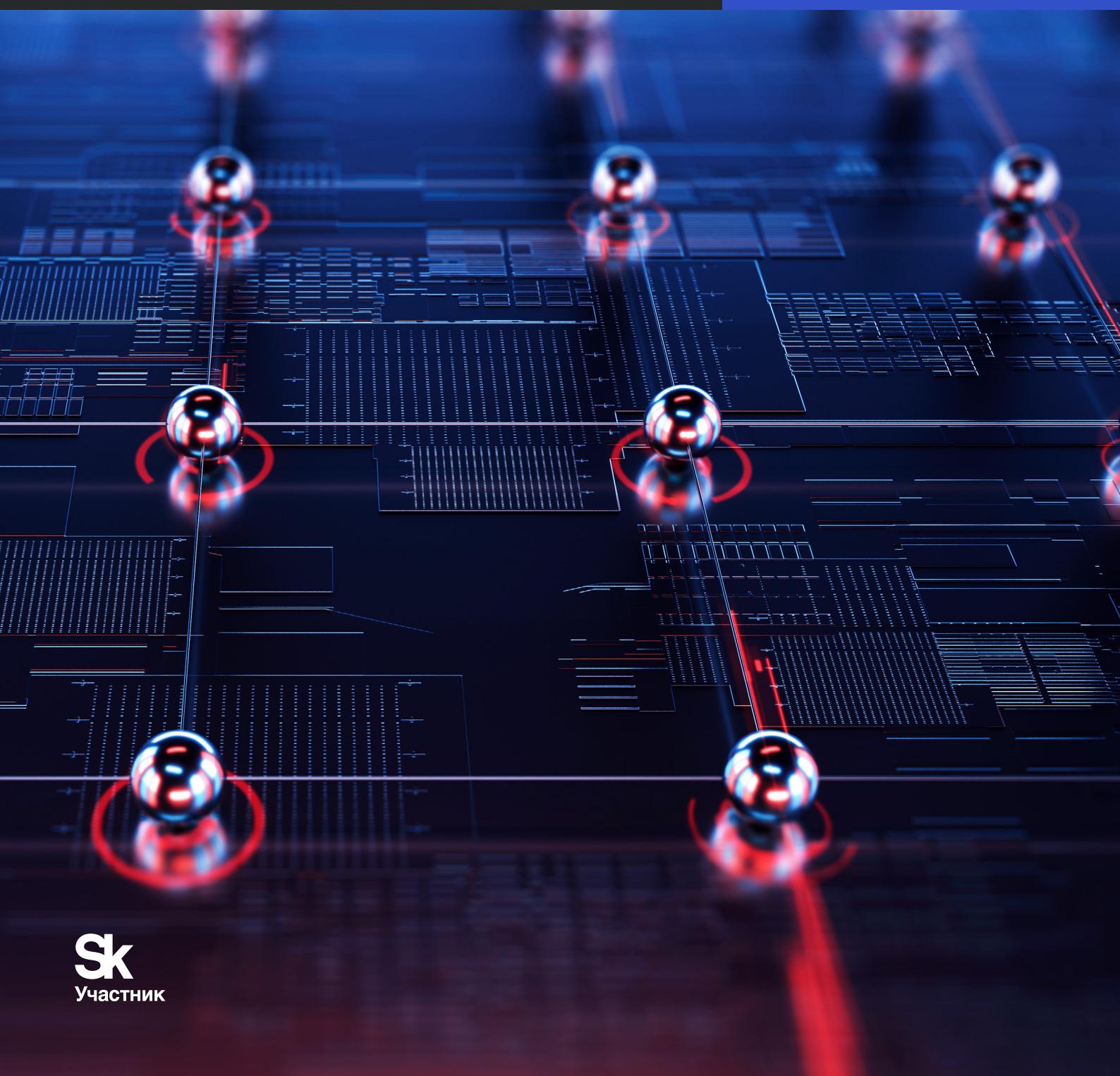


INFOWATCH ARMA INDUSTRIAL ENDPOINT

Защита
информации
рабочих станций
и серверов
АСУ ТП





InfoWatch ARMA Industrial Endpoint — программное обеспечение, которое защищает рабочие станции и серверы SCADA от киберугроз

	Блокирует запуск недоверенных программ
	Контролирует целостность файлов на рабочих станциях и серверах АСУ ТП
	Поставляет данные о событиях безопасности на всех рабочих местах для централизованного сбора и хранения в системе InfoWatch ARMA Management Console

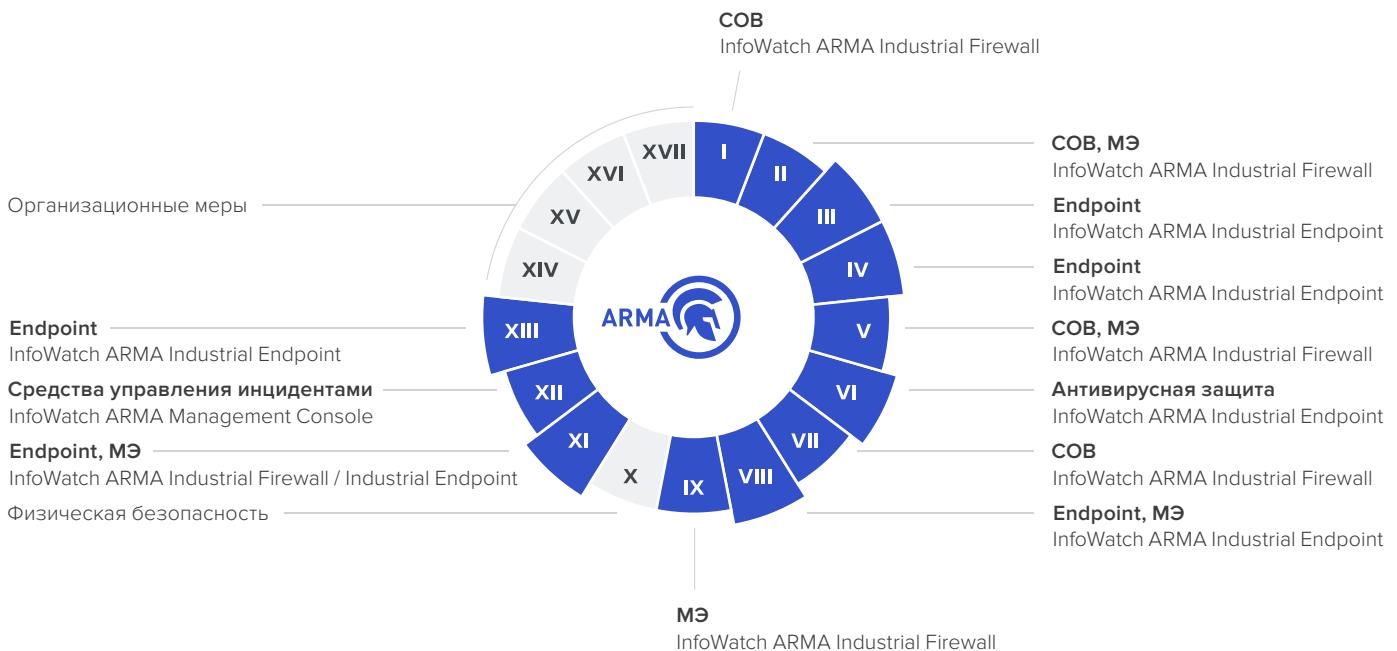
В каких случаях применяется

Если у вас возникали инциденты, связанные с проникновением вредоносного ПО в АСУ ТП через конечные точки IT-инфраструктуры — рабочие станции.

Это могут быть нелегитимно подключенные USB-носители. Или вредоносное ПО, распространяемое по сети от одного конечного устройства к другому.

Представьте ситуацию. Оператор АСУ ТП, чтобы не скучать в ночную смену, принёс USB-модем и подключил его к рабочей станции в изолированном сегменте. Сам того не подозревая, он только что создал канал для доставки вредоносного ПО в изолированный сегмент.

Какие группы технических мер Приказа №239 ФСТЭК России закрывает InfoWatch ARMA



Единая система защиты InfoWatch ARMA позволяет выполнить [до 90% технических мер](#) ФСТЭК России

Возможности для служб информационной безопасности

1 Контролирует подключение съёмных носителей

Позволяет разрешать или запрещать подключение съёмных носителей на уровне класса устройств — например, USB-носителей.

2 Позволяет создать замкнутую программную среду

- Контролирует запуск приложений по «белому списку», предоставляя доступ только к тем файлам, которые необходимы специалистам для работы. Такой «белый список» доверенных программ может формироваться как вручную, так и автоматически, если включить режим обучения
- Контролирует целостность файлов. Непрерывно следит за неизменностью среды рабочих станций и серверов АСУ ТП — файлов, папок, каталогов

3 Обнаруживает вредоносные программы и вирусы

Проводит антивирусное сканирование файлов сигнатурным методом и удаляет обнаруженные вирусы, информируя сотрудника ИБ АСУ ТП о каждом из них. База сигнатур не зависит от иностранных поставщиков и регулярно обновляется. Возможность централизованно обновлять эту базу через InfoWatch ARMA Management Console.

4 Прост и удобен в управлении и обновлении

Графический интерфейс InfoWatch ARMA Industrial Endpoint позволяет совершать необходимые настройки, управлять и обновлять ПО. Синхронизация с единым центром управления InfoWatch ARMA Management Console помогает единовременно совершать эти действия:

- Управление контролем целостности файлов
- Управление контролем устройств
- Управление «белыми списками» программ
- Централизованное обновление ПО
- Настройки сигнатурного антивируса и централизованное обновление его баз

Чем поможет замкнутая программная среда

Задача замкнутой программной среды — сохранить непрерывность работы промышленных систем, даже если вирусу удалось проникнуть.

В отличие от классических антивирусов InfoWatch ARMA Industrial Endpoint не позволяет открыть недоверенное ПО на рабочих станциях. Система не проводит постоянного сканирования, поэтому не создаёт дополнительной нагрузки на рабочие станции и серверы АСУ ТП.

1 Минимизирует пространство для маневра злоумышленника

Запускаются только разрешённые и проверенные приложения и файлы. В таких условиях кибератаки проблематичны.

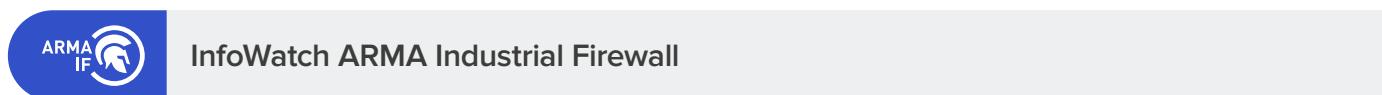
2 Минимизирует нагрузку на персонал

Тонкая настройка и отсутствие лишних возможностей кратко снижают лишние срабатывания. InfoWatch ARMA Industrial Endpoint самостоятельно составляет «белые списки» программ благодаря режиму обучения. Персонал занимается контролем, а не постоянным мониторингом.

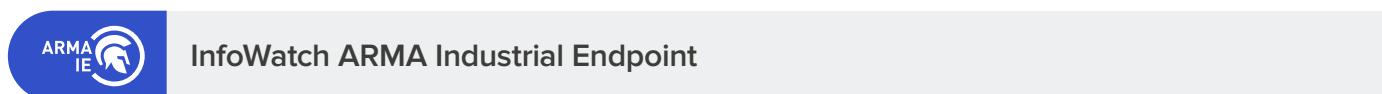
Больше возможностей с единой системой защиты

InfoWatch ARMA Industrial Endpoint является частью единой системы **InfoWatch ARMA**, которая создавалась специально для защиты промышленных сетей.

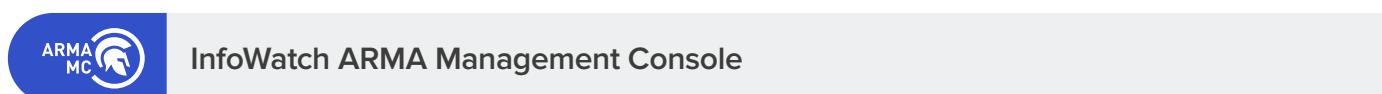
Внедрение каждого из компонентов защиты системы InfoWatch ARMA даёт расширенные возможности для обнаружения и оперативного реагирования на инциденты ИБ.



Сертифицированный промышленный межсетевой экран нового поколения — предотвращает атаки на сетевом уровне.



Промышленная защита рабочих станций и серверов.



Центр управления системами защиты — позволяет увидеть цепочки событий, собранные из разрозненных средств защиты, в едином веб-интерфейсе. С помощью правил корреляции из события создаёт инцидент и реагирует на него: предотвращает атаку и передаёт инструкции сотрудникам ИБ АСУ ТП.



С помощью **InfoWatch ARMA** можно реализовать принцип эшелонированной защиты технологической сети прямо «из коробки», минуя долгие и затратные интеграции.

Использование единой системы защиты InfoWatch ARMA уменьшает поверхность для атак злоумышленника и позволяет выполнить до 90% технических требований ФСТЭК России (Приказ №239).

Запросите персональное демо и узнайте все возможности системы **InfoWatch ARMA**

arma.infowatch.ru

sales@infowatch.ru

+7 495 22 900 22