INFOWATCH AUTOMATION SYSTEM ADVANCED PROTECTOR

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ЗАЩИТА ОТ АТАК НА ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ АСУ ТП

Программно-аппаратный комплекс для защиты АСУ ТП – это интеллектуальное решение для обнаружения и предотвращения атак, направленных на информационную инфраструктуру систем автоматического управления производственными и технологическими процессами (АСУ ТП).
Благодаря новому подходу и запатентованным технологиям защиты, решение имеет ряд преимуществ перед штатными средствами предотвращения вторжений, которые реализуются производителями оборудования.

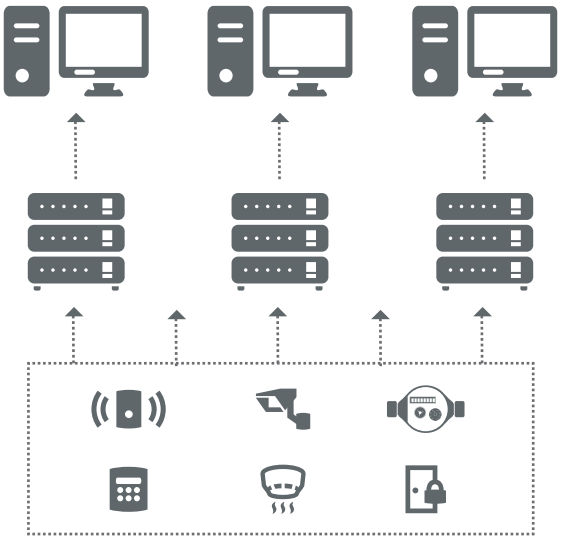
КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ ПРОДУКТА

- Обнаружение вторжений и защита от врезки в каналы передачи данных
- Межсетевое экранирование на уровне промышленных протоколов
- Контроль корректности технологического процесса
- Обеспечение целостности передаваемых данных в системе АСУ ТП
- Мониторинг уязвимостей АСУ ТП
- Поддержка проприетарных протоколов инженерных систем
- Соответствие руководящим документам ФСТЭК

Большинство существующих решений по защите АСУ ТП работают на верхнем уровне системы - уровне операторского контроля (SCADA-системы / HMI). В первую очередь, они включают различные методы защиты от вредоносного программного обеспечения, гарантируя антивирусную защиту систем управления.

В то же время специалисты по информационной безопасности единогласно считают исполнительные уровни системы - уровень программируемых логических контроллеров и конечных исполнительных устройств и механизмов - наиболее уязвимыми участками АСУ ТП. Более того, атаки именно на исполнительные устройства и механизмы потенциально могут привести (и приводят) к наиболее масштабным последствиям (человеческие жертвы, экологические и прочие техногенные катастрофы).

МНОГОУРОВНЕВЫЙ ПОДХОД К ЗАЩИТЕ АСУ ТП



MES/ERP

SCADA

ПЛК

Полевой уровень

- Защита от таргетированных атак
- Межсетевые экраны
- Однонаправленные шлюзы
- **SIEM**

INFOWATCH AUTOMATION SYSTEM ADVANCED PROTECTOR

INFOWATCH AUTOMATION SYSTEM ADVANCED PROTECTOR

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ПО ЗАЩИТЕ АСУ ТП СООТВЕТСТВУЕТ ДОКУМЕНТАМ ФСТЭК РОССИИ

- Руководящему Документу ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (РД по СВТ) – класс 5
- Руководящему Документу ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД по МЭ) – класс 3
- Методическому Документу ФСТЭК России «Профиль защиты систем обнаружения вторжений уровня сети пятого класса защиты ИТ.СОВ.С5.ПЗ» (РД по СОВ) – класс 5
- Руководящему Документу ФСТЭК России «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» - (РД по НДВ) – класс 3

ХАРАКТЕРНЫЕ АТАКИ НА АСУ ТП

Врезка в каналы передачи данных. Злоумышленник может произвести врезку в линию передачи данных и получить возможность считывать и подменять информацию, передаваемую по этим каналам.

Воздействие на оборудование автоматизации, установленное на удаленных объектах инфраструктуры. Взлом служебных помещений внешним нарушителем или несанкционированный доступ к оборудованию, полученный сотрудником предприятия, может привести к направленному вредоносному воздействию на оборудование автоматизации объекта.

Активация программных и аппаратных закладок, в том числе на микропрограммном уровне (прошивки контроллеров, датчиков и исполняемых устройств). Закладки могут быть активированы при наступлении определенного времени и события, и привести к выводу из строя оборудования.

ПОДХОД К ЗАЩИТЕ АСУ ТП

Внедрение комплекса защиты состоит из нескольких этапов:

1 этап: проводится комплексный аудит защищаемой технологической системы предприятия. Результатом этапа является максимально подробное описание инфраструктуры, используемого оборудования и протоколов, и детальная модель угроз

2 этап: проектирование системы защиты. Определяется конфигурация системы с учетом результатов аудита, производится проектирование и предварительная настройка системы защиты

3 этап: производится поэтапное развертывание системы в инфраструктуру АСУ ТП предприятия. Работа в режиме самообучения

4 этап: перевод системы защиты в активный режим работы

5 этап: сопровождение системы в режиме промышленной эксплуатации

ПРЕИМУЩЕСТВА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ ЗАЩИТЫ АСУ ТП

- Эшелонированная защита от атак на нижних уровнях, независимо от точки их возникновения
- Поддержка более 20 проприетарных протоколов, с учетом отраслевой специфики
- Методология аудита и построения модели угроз, обеспечивающая эффективную защиту
- Соответствие требованиям ФСТЭК в части обеспечения информационной безопасности
- Разработан при участии ведущих российских экспертов в области промышленной безопасности