

PT ISIM

Система для обеспечения
киберустойчивости технологической
инфраструктуры



Полная видимость
технологической среды



Контроль
поверхности атаки



Выявление угроз и аномалий

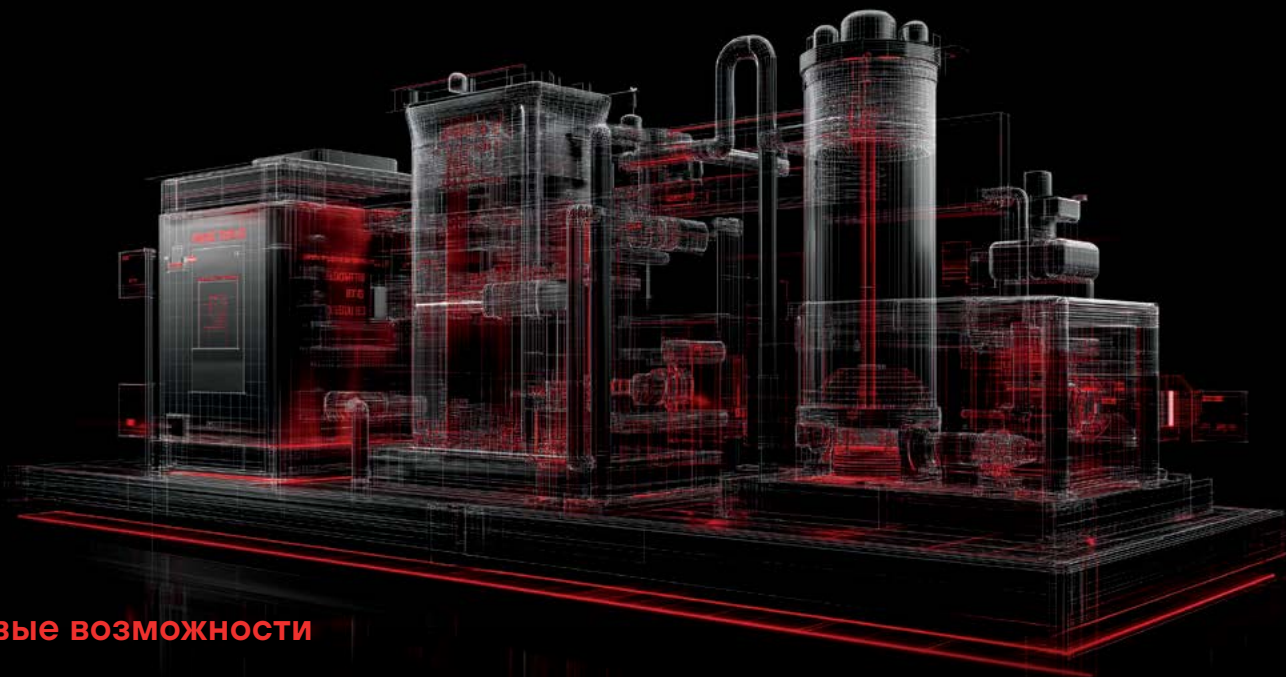


Защита конечных узлов



PT ISIM

PT ISIM помогает видеть технологическую среду, контролировать защищенность и своевременно выявлять угрозы, снижая риск инцидентов и обеспечивая непрерывность технологических процессов



Ключевые возможности



Инвентаризация сети и выявление уязвимостей

Формирует актуальную картину технологической инфраструктуры: определяет активы, выявляет уязвимости и помогает оценить текущее состояние защищенности



Контроль целостности сети

Помогает отслеживать изменения в сетевой инфраструктуре АСУ ТП, выявлять нарушения сегментации сети, доступы в корпоративную сеть и соединения с публичными адресами



Обнаружение аномалий трафика и угроз

В режиме реального времени выявляет отклонения в сетевой активности, признаки компрометации и потенциально опасные действия в технологической сети



Защита конечных узлов

Обеспечивает антивирусную защиту рабочих станций и серверов АСУ ТП от массовых и целевых атак



Защита SCADA-систем

Обнаруживает атаки на распространенные российские и зарубежные SCADA-системы, а также позволяет выявлять неправомерные действия персонала



Контроль параметров технологического процесса

Контролирует параметры, влияющие на безопасность и стабильность технологических процессов, помогает обнаруживать критические отклонения и попытки скрытого вмешательства

Почему PT ISIM



Промышленная экспертиза

Содержит **более 16 000** правил обнаружения и индикаторов промышленных угроз

Поддерживает **более 130** промышленных и общесетевых протоколов

Регистрирует события безопасности в **10+** популярных российских и иностранных SCADA-системах



Выполнение требований регуляторов

Помогает закрывать требования Приказа № 239 ФСТЭК России по защите объектов КИИ, обеспечивая антивирусную защиту, аудит безопасности, реагирование на инциденты и предотвращение компьютерных атак



Масштабируемость

Позволяет выстраивать защиту как одиночной АСУ ТП, так и распределенной, сегментированной или изолированной инфраструктуры производственного комплекса или холдинга



Программно-аппаратный комплекс

Поставляется в виде ПО для установки на собственных физических или виртуальных серверах либо в форме доверенных ПАК, соответствующих требованиям постановления Правительства от 14.11.2023 № 1912. Оборудование внедряется и поддерживается командой Positive Technologies



Кому полезен PT ISIM



Службам ИБ

Для выявления угроз и уязвимостей, а также для контроля защищенности технологического контура



Сетевым и ИТ-инженерам

Для инвентаризации инфраструктуры и контроля изменений



Службам эксплуатации АСУ ТП

Для повышения прозрачности технологической среды и снижения риска инцидентов



Руководителям, отвечающим за устойчивость производственных процессов

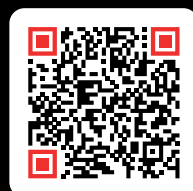
Для повышения управляемости и снижения риска простоев



[Запросить тест-драйв](#)



Новости
PT ISIM



Справочный
портал PT ISIM