

PT ISIM

СИСТЕМА ДЛЯ ОБЕСПЕЧЕНИЯ
КИБЕРУСТОЙЧИВОСТИ
ПРОМЫШЛЕННОЙ
ИНФРАСТРУКТУРЫ

15.05.2026



СОДЕРЖАНИЕ

Киберустойчивость как элемент промышленной безопасности	→	1
PT ISIM — система для обеспечения киберустойчивости промышленной инфраструктуры	→	2
Масштабируемость	→	3
Промышленная экспертиза PT ISIM	→	3
Возможности PT ISIM	→	4
Выполнение мер приказа ФСТЭК России № 239	→	6
Как работает PT ISIM	→	7
Архитектура PT ISIM	→	8
Модели поставки PT ISIM	→	10
Программно-аппаратный комплекс PT ISIM	→	11
Конфигурация и технические характеристики	→	11

КИБЕРУСТОЙЧИВОСТЬ КАК ЭЛЕМЕНТ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ

1

Инциденты кибербезопасности остаются главным риском для компаний по всему миру, независимо от их размера*.

Для технологических инфраструктур угрозу представляет не только специфичное для АСУ ТП вредоносное ПО (**Industroyer**, **Duqu** или **BlackEnergy**), но и обычное, в том числе программы-шифровальщики.

83%

атак связаны с использованием ВПО**

Шифровальщики способны нарушить основную деятельность промышленного предприятия. Например, в результате **атаки на Colonial Pipeline (2021)** работа крупной сети нефтепроводов была приостановлена на несколько дней, а **инцидент в Norsk Hydro (2019)** нарушил производство алюминия на заводах компании по всему миру.

44%

успешных атак связаны с использованием программ-шифровальщиков**

Почти **50%** всех атак поначалу остаются незамеченными. Более **60%** компаний не проводят должный ретроспективный анализ после первого инцидента, из-за чего опасная ситуация повторяется снова.

200 дней

составляет среднее время скрытого присутствия хакера в инфраструктуре***

Статистика показывает, насколько важно обеспечивать защиту не только периметра, но и внутренней сети. Обезопасить промышленную инфраструктуру позволяют специализированные системы непрерывного мониторинга, такие как PT ISIM.

* Allianz Risk Barometer. Results appendix 2025.

** Positive Technologies: актуальные киберугрозы для российских промышленных предприятий.

*** По данным внутренних исследований Positive Technologies (результаты предоставляются по запросу)

PT ISIM — СИСТЕМА ДЛЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ПРОМЫШЛЕННОЙ ИНФРАСТРУКТУРЫ

2

Какие задачи позволяет решить PT ISIM

1

Выполнение требований регулятора по защите критической информационной инфраструктуры (приказы ФСТЭК России № 31 и 239).

2

Выявление уязвимостей, планирование и реализация мер по усилению защищенности промышленной инфраструктуры.

3

Проактивное обнаружение и устранение угроз информационной безопасности.

Система обеспечивает защиту технологических сетей, рабочих станций и серверов АСУ ТП, инженерных систем зданий и IIoT-устройств от киберугроз и действий нарушителей со стороны подрядных организаций.

Кому полезен PT ISIM. Специалистам по ИБ, ИТ, сетевым инженерам и сотрудникам службы эксплуатации АСУ ТП.

С чем помогает. Система собирает данные о технологической инфраструктуре с помощью инструментов мониторинга, а также использует встроенную промышленную экспертизу, обеспечивая:

- наблюдаемость технологической инфраструктуры и управление активами;
- выявление уязвимостей, слабых мест и нарушений в конфигурациях;
- контроль безопасности технологических сетей;
- мониторинг событий и аномалий;
- анализ угроз и разбор инцидентов;
- контроль технологических параметров и уставок;
- координацию реагирования в промышленном контуре.

Для чего PT ISIM незаменим:

- Соблюдение требований регуляторов в области защиты объектов КИИ (приказы ФСТЭК России № 31 и 239, Постановление Правительства РФ № 1912, Федеральный закон № 187-ФЗ и т. п.).
- Обеспечение киберустойчивости технологической инфраструктуры:
 - Контроль параметров технологического процесса.
 - Антивирусная защита конечных узлов.
 - Обнаружение сложных целевых атак и внутренних злоупотреблений.

PT ISIM масштабируется от одного сегмента АСУ ТП до распределенной инфраструктуры с несколькими производственными площадками и холдинговой структурой управления. Продукт поддерживает распределенную архитектуру с использованием сетевых сенсоров, устанавливаемых в диспетчерских центрах, и коллекторов на удаленных площадках.

ПРОМЫШЛЕННАЯ ЭКСПЕРТИЗА PT ISIM

Эффективная защита технологической инфраструктуры невозможна без глубокого понимания специфики промышленных протоколов, SCADA-систем и логики работы АСУ ТП.

PT ISIM выявляет атаки на системы на базе Windows и Linux, стандартное сетевое оборудование, промышленные устройства и компоненты АСУ ТП.

В основе продукта — обширная промышленная экспертиза, включающая правила и индикаторы угроз. PT ISIM поддерживает анализ промышленных и общесетевых протоколов, что позволяет сформировать глубокое понимание специфики технологических сред и выявлять как типовые, так и таргетированные атаки.

Для мониторинга ключевых АСУ ТП реализованы готовые пакеты с преднастроенными правилами.

PT ISIM поддерживает распространенные российские и международные SCADA-системы, всевозможные промышленные протоколы и правила работы с популярными решениями для автоматизации.

16_k

правил и индикаторов
промышленных угроз

130+

поддерживаемых
промышленных
и общесетевых
протоколов

Готовые правила
мониторинга для

10+

АСУ ТП



Полный список протоколов



Анализ сетевого трафика

PT ISIM выполняет глубокий анализ технологического трафика и выявляет угрозы в режиме реального времени. Система поддерживает широкий спектр общесетевых и промышленных протоколов, обеспечивая:

- обнаружение вторжений, аномальных сетевых сессий и признаков компрометации инфраструктуры;
- выявление вредоносной активности и распространения вирусов;
- фиксацию подключений к внешним IP-адресам и нарушений периметра;
- обнаружение использования средств удаленного доступа и небезопасных протоколов;
- контроль сетевых взаимодействий между узлами технологической сети.



Контроль технологического процесса

PT ISIM контролирует параметры технологического процесса и действия, способные повлиять на безопасность и непрерывность производства. Система анализирует контекст событий и помогает выявлять попытки скрытого вмешательства:

- отслеживает отклонения технологических параметров и выход за критические уставки;
- выявляет передачу опасных технологических команд (перепрошивка ПЛК, форсирование переменных, очистку памяти);
- формирует логические цепочки событий для расследования инцидентов.



Инвентаризация активов

PT ISIM формирует актуальную карту технологической инфраструктуры и обеспечивает непрерывный контроль изменений. Система автоматически обнаруживает узлы и собирает данные об их программном и аппаратном обеспечении:

- выявляет новые устройства, рабочие станции, ПЛК и сетевое оборудование;
- контролирует изменения конфигураций оборудования и ПО;
- фиксирует учетные записи пользователей;
- собирает данные через пассивный анализ трафика, активный опрос или агенты PT ISIM Endpoint.



Управление уязвимостями

PT ISIM выявляет уязвимости в компонентах технологической инфраструктуры и помогает оценивать риски для производственной среды:

- обнаруживает уязвимости на Windows- и Linux-узлах, ПЛК и сетевом оборудовании;
- приоритизирует уязвимости по критичности для инфраструктуры;
- предоставляет рекомендации по устранению уязвимостей.



Защита конечных точек и реагирование

PT ISIM обеспечивает мониторинг событий безопасности на рабочих станциях и серверах АСУ ТП, выявляет угрозы и помогает оперативно реагировать на инциденты, выполняя:

- анализ событий безопасности на серверах и АРМ для выявления внешних и внутренних угроз;
- выявление несанкционированного доступа;
- обнаружение атак типа living off the land, связанных с использованием злоумышленниками легитимных инструментов системы;
- выявление специфичных для технологических сетей техник атак в поддерживаемых SCADA-системах: подмены проектов, подбора паролей, нелегитимного запуска инженерных утилит и других признаков компрометации



Антивирусная защита

PT ISIM обеспечивает антивирусную защиту рабочих станций и серверов технологического сегмента с учетом специфики технологической инфраструктуры, выполняя:

- выявление и блокировку вредоносного ПО;
- обнаружение программ-шифровальщиков и попыток их распространения;
- предотвращение запуска подозрительных файлов;
- безагентскую антивирусную защиту за счет интеграции с PT Sandbox.



Управление событиями информационной безопасности

PT ISIM объединяет события безопасности из различных источников инфраструктуры и обеспечивает централизованный мониторинг технологического сегмента. Встроенные возможности SIEM расширяют контроль событий безопасности за пределы сетевого трафика. Система:

- собирает события с сетевых устройств, серверов, рабочих станций и ПЛК;
- нормализует и коррелирует события из различных источников;
- выявляет сложные цепочки атак и признаки компрометации;
- проводит проактивный поиск угроз в технологической инфраструктуре;
- выполняет централизованный поиск и расследование инцидентов безопасности.

ВЫПОЛНЕНИЕ МЕР ПРИКАЗА ФСТЭК РОССИИ № 239

6

Помогает выполнять требования Приказа № 239 и 31 ФСТЭК России по защите объектов КИИ.

Сертифицирован во ФСТЭК России по ОУД-4 и по профилям защиты САВЗ (А, Б и В четвертого класса защиты), СОВ (уровня сети четвертого класса защиты), средствам обнаружения и реагирования на уровне узла (EDR, 4), требованиям к средствам выявления (контроля) уязвимостей.

Предотвращение вторжений, компьютерных атак (СОВ)

Покрывает

100%

технических мер

Реагирование на компьютерные инциденты (ИНЦ)

Покрывает

100%

технических мер

Антивирусная защита (АВЗ)

Покрывает

100%

технических мер

Аудит безопасности (АУД)

Покрывает

93%

технических мер

Идентификация и аутентификация (ИАФ)

Покрывает

57%

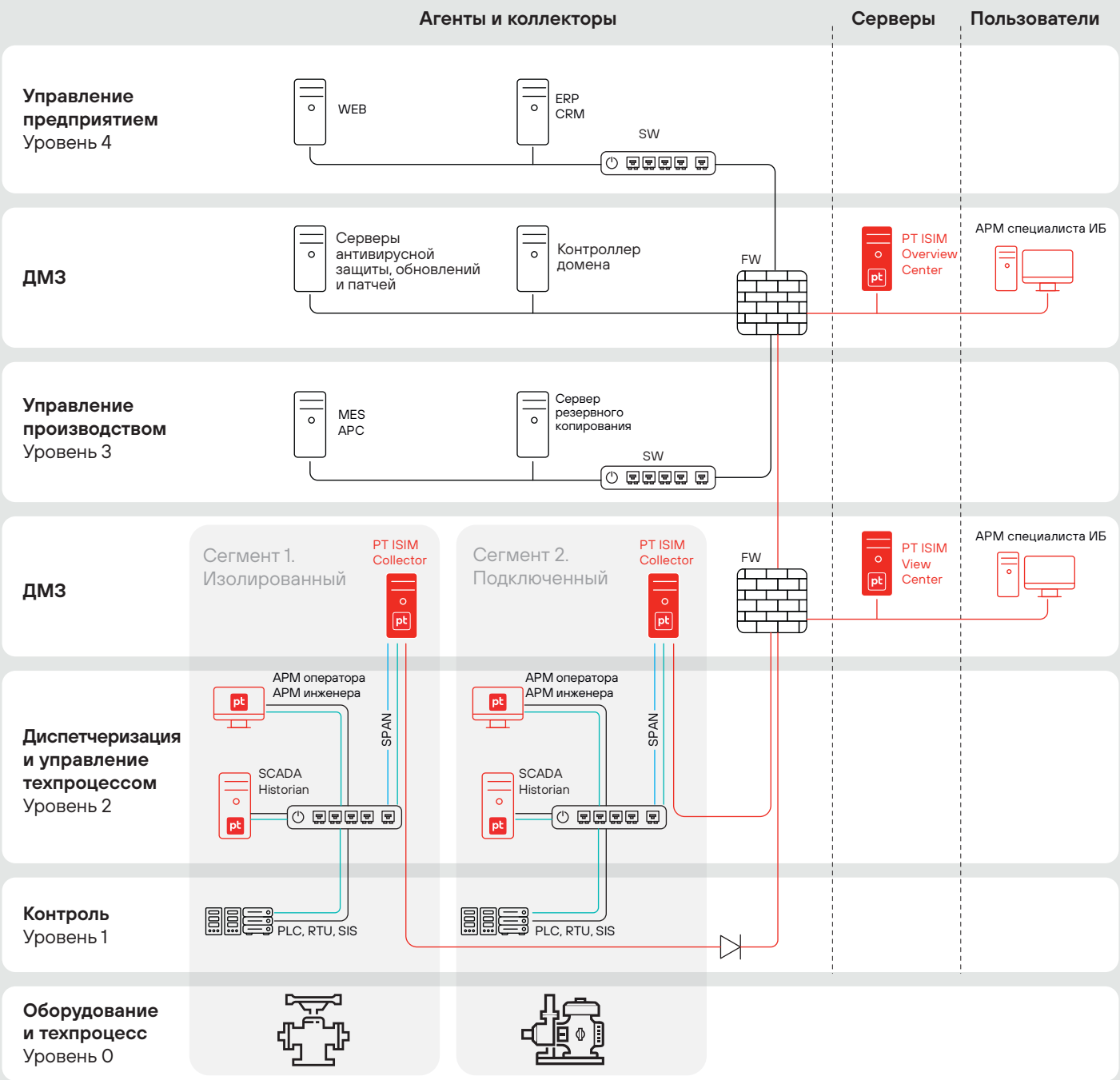
технических мер

Управление доступом (УПД)

Покрывает

64%

технических мер



- Трафик ОТ-сетей (ПЛК, SCADA, HMI, MES)
- Пассивное копирование трафика технологической сети (SPAN)
- Активные процессы (опрос, сканирование) и журналы
- PT ISIM data & management traffic
- ▷ UDG (data diode)
- pt PT ISIM Endpoint Agent

ОБЯЗАТЕЛЬНЫЙ КОМПОНЕНТ

Сенсор PT ISIM View Sensor

Анализирует и хранит сетевой трафик, получает события безопасности с агентов и управляет ими. Устанавливается на уровне сегмента сети АСУ ТП или всей производственной площадки.

Лицензирование — по количеству сенсоров

ОПЦИОНАЛЬНЫЕ ДОПОЛНИТЕЛЬНЫЕ КОМПОНЕНТЫ

Агенты PT ISIM Endpoint

Устанавливаются на SCADA-серверах и рабочих станциях операторов и инженеров. Собирают данные о конфигурации и установленном ПО, события безопасности операционных систем, системного и прикладного программного обеспечения АСУ ТП, обеспечивают антивирусную защиту и возможность реагирования.

Доступны в двух вариантах: только антивирус (EPP) или комплексная защита (EDR).

Лицензирование — по количеству агентов.

Сервер управления PT ISIM Overview Center

Собирает события с подключенных сенсоров, используется для их централизованной настройки и обновления. Устанавливается на уровне ситуационного центра (SOC).

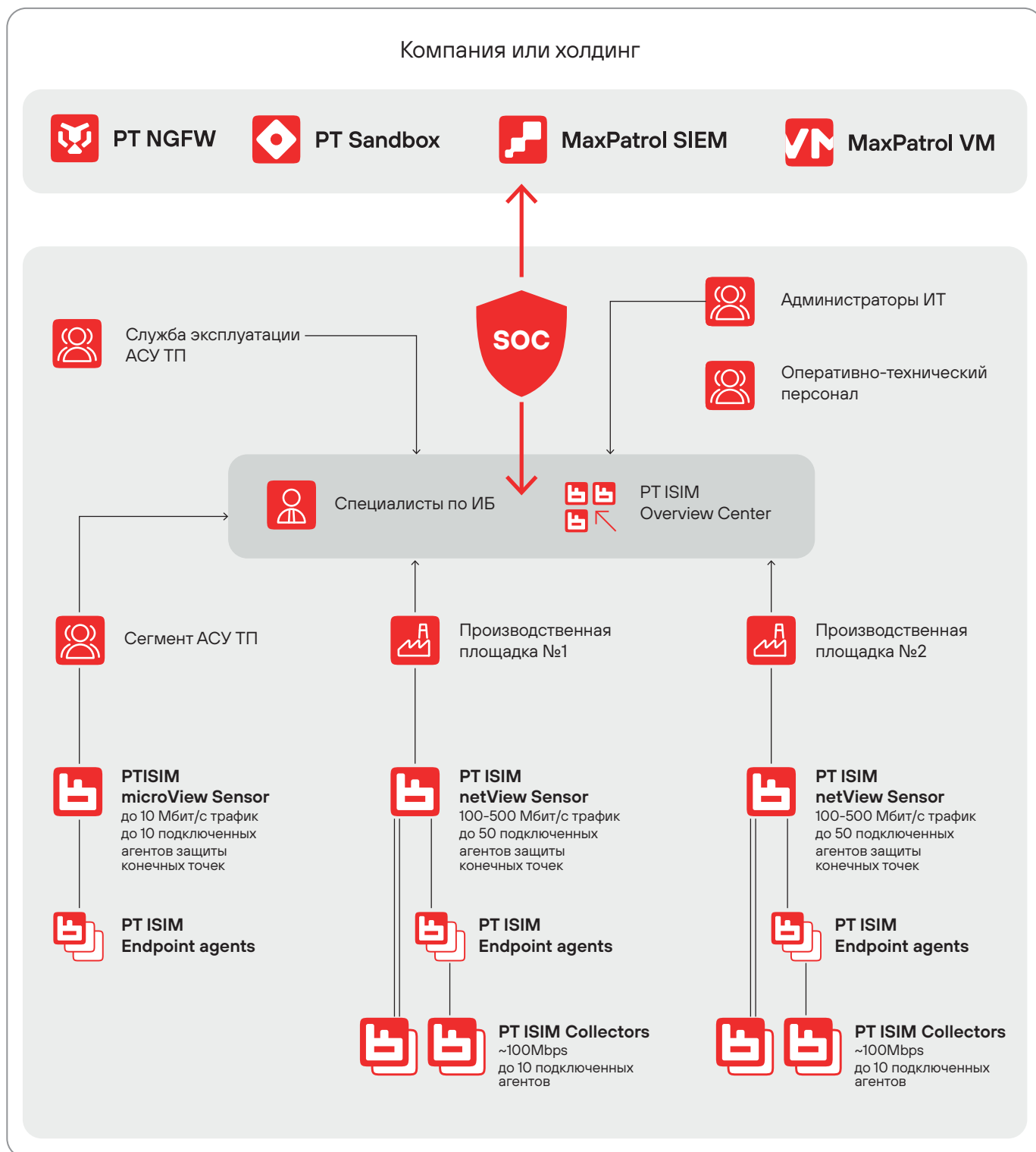
Лицензирование — по количеству серверов управления, без ограничений на количество подключенных сенсоров.

PT ISIM Collector

Коллектор без собственного интерфейса — для сбора и обработки SPAN-трафика в удаленных сегментах АСУ ТП (в том числе в расположенных за диодом данных), а также для его передачи в сенсор PT ISIM View Sensor с экономией в использовании канала связи для централизованного мониторинга безопасности.

Лицензирование — по количеству коллекторов





Два варианта поставки:

1

Программное обеспечение PT ISIM

Лицензируемое программное обеспечение для установки в виртуальной среде или на имеющихся серверах заказчика. Доступно в виде срочных или бессрочных лицензий.

2

Программно-аппаратный комплекс PT ISIM

Лицензированный программно-аппаратный комплекс:

- Аппаратная платформа с Astra Linux Special Edition. Интегрирована с программным обеспечением PT ISIM.
- Поставляется как единое готовое решение с технической поддержкой АО «Позитив Текнолоджиз».
- Серверы и ПАК находятся в реестре Минцифры и реестре РЭП Минпромторга, что соответствует требованиям Постановления Правительства РФ № 1912.

Варианты применения:

1

Комплаенс

соблюдение требований регуляторов и отраслевых стандартов

- COB для АСУ ТП

PT ISIM microView Sensor

2

Комплаенс

соблюдение требований регуляторов и отраслевых стандартов

- COB для АСУ ТП
- Антивирус для АСУ ТП

PT ISIM microView Sensor
PT ISIM Antivirus

3

Комплаенс

соблюдение требований регуляторов и отраслевых стандартов

Киберустойчивость промышленной инфраструктуры

- COB для АСУ ТП
- Антивирус для АСУ ТП
- Управление активами АСУ ТП
- Выявление уязвимостей в АСУ ТП
- EDR для АСУ ТП
- Контроль техпроцесса

PT ISIM proView Sensor
PT ISIM Endpoint

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС PT ISIM

11

Кросс-отраслевое решение

Широкая линейка конфигураций в сочетании с функциями контроля безопасности открытых и проприетарных технологий автоматизации для применения в различных ОТ-инфраструктурах

Кросс-функциональное решение

Набор инструментов экспертного уровня для решения задач, связанных с ИБ, ИТ и АСУ ТП, на промышленных предприятиях

Отечественное решение для критических инфраструктур

Отечественное ПО, ОС и ПАК — в реестре Минцифры.
Аппаратные платформы — в реестре РЭП Минпромторга.
Программное обеспечение сертифицировано ФСТЭК и протестировано на совместимость с АСУ ТП отечественных вендоров

КОНФИГУРАЦИЯ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ



Модель	NS-1050	NS-2010
Для каких компонентов подходит	PT ISIM microView Sensor PT ISIM Collector	PT ISIM netView Sensor PT ISIM proView Sensor PT ISIM Collector PT ISIM Overview Center
Процессор	1 × Intel Atom 16 ядер	1 × Intel Xeon Scalable Gen5 32 ядра
ОЗУ	64 ГБ DDR4 ECC DIMM	128 ГБ DDR5 ECC RDIMM
Дисковое пространство	480 ГБ SSD	4,8 ТБ SSD
Сетевой интерфейс RJ-45, 1 Гбит/с	2	4 (расширяется до 20)
Сетевой интерфейс SFP/RJ-45, 1 Гбит/с	4	До 16
Операционная система	Astra Linux Special Edition «Воронеж»	
ГИСП и реестр ПАК Минцифры	ПАК PT ISIM NS-1050 ЕВРГ.466539.002. Реестровая запись № 28964 от 28.07.2025	ПАК PT ISIM NS-2010 ЕВРГ.466539.002-01. Реестровая запись № 28967 от 28.07.2025

POSITIVE TECHNOLOGIES ОБЕСПЕЧИВАЕМ ПРАКТИЧЕСКУЮ КИБЕРБЕЗОПАСНОСТЬ

20_{лет}

опыта исследований
и разработок

26000+

сотрудников в компании:
инженеров по ИБ,
разработчиков, аналитиков
и других специалистов

250+

экспертов в нашем
исследовательском центре
безопасности

200+

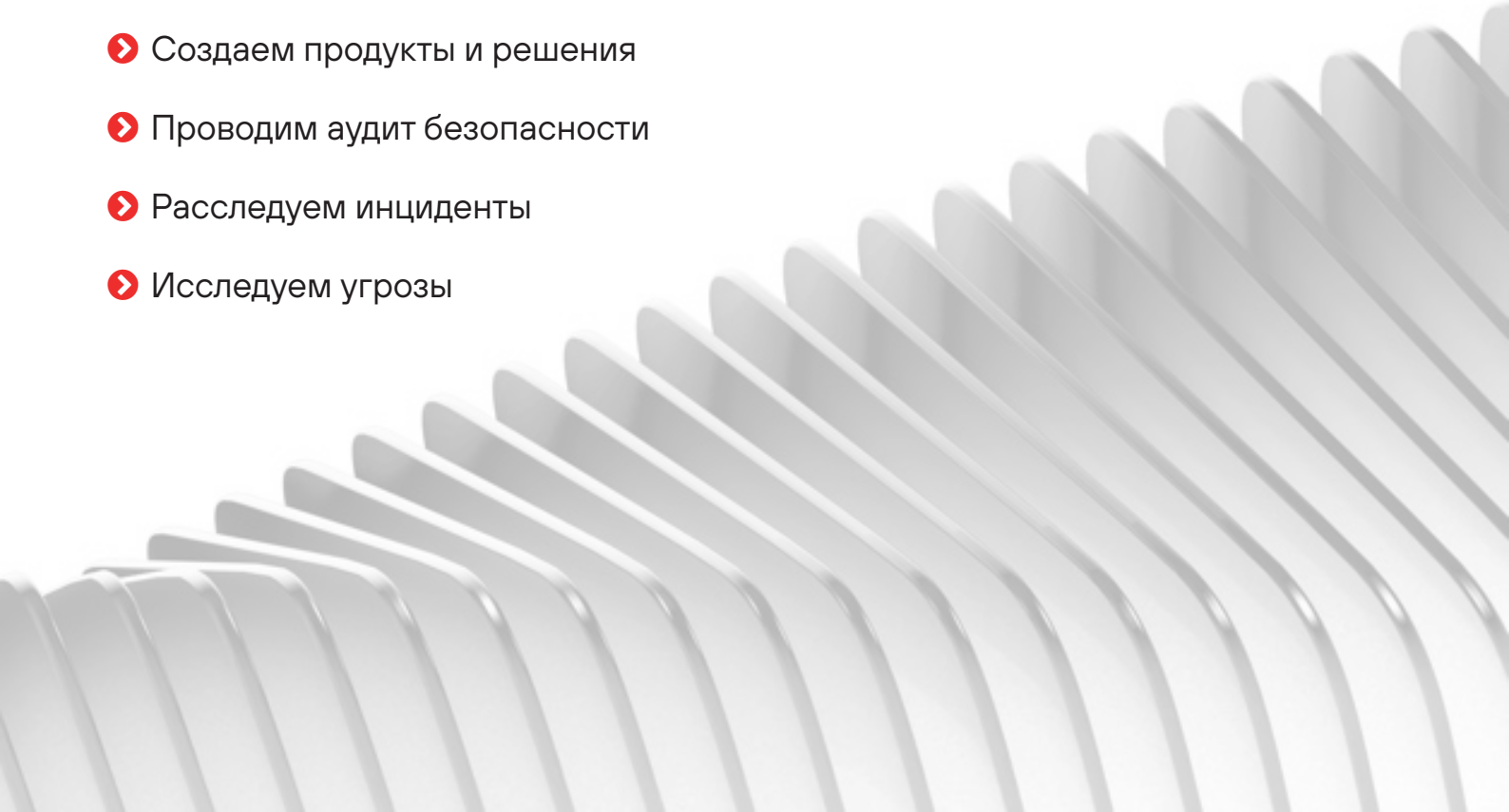
обнаруженных уязвимостей
нулевого дня в год

250+

аудитов безопасности
корпоративных систем
проводим ежегодно

50%

всех уязвимостей
в промышленности и телекоме
обнаружили наши эксперты

- Создаем продукты и решения
 - Проводим аудит безопасности
 - Расследуем инциденты
 - Исследуем угрозы
- 



Запросить тест-драйв



Новости PT ISIM