POSITIVE TECHNOLOGIES

Positive Technologies Industrial Security Incident Manager

PT ISIM

Описание продукта

Безопасность АСУ ТП. **Основные угрозы**

Автоматизированные системы управления технологическими процессами (АСУ ТП) сегодня применяются во множестве отраслей — в нефтегазовой промышленности, металлургии, энергетике, космонавтике, медицине. Традиционно при проектировании АСУ ТП исходят из предположения, что подобные системы — это часть замкнутой экосистемы, которая рассчитана на различные режимы работы, включая аварийные, что позволяет в определенной степени пренебрегать рисками информационной безопасности.

«58% уязвимостей, опубликованных в 2017 году, было обнаружено в компонентах АСУ ТП лидирующих производителей — Schneider Electric, Moxa, Siemens. Более половины найденных уязвимостей имеют критическую и высокую степень риска».

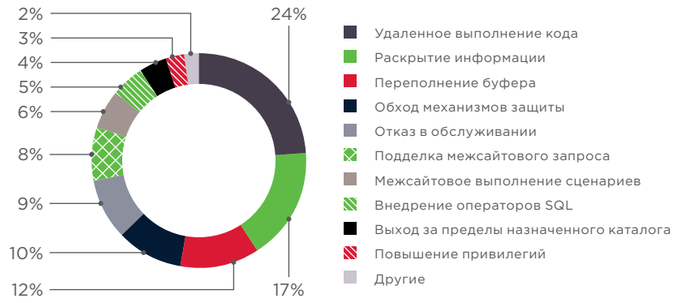
Ежегодное исследование
Positive Research, 2018

Существуют ли подобные условия в действительности? Многочисленные исследования кибербезопасности АСУ ТП доказывают, что нет. Миф об АСУ ТП, функционирующих внутри некой доверенной зоны, перестал существовать вместе с понятием «воздушный зазор» (физическая изоляция технологической сети). Как правило, именно воздушный зазор считался действенным средством против инцидентов информационной безопасности в промышленности.

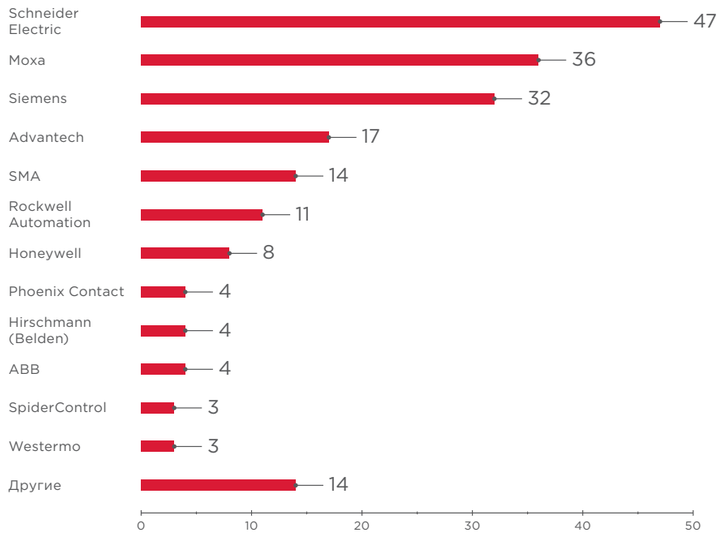
Для эффективного решения бизнес-задач промышленные компании, напротив, стремятся интегрировать корпоративные и производственные IT-инфраструктуры. Все чаще технологические сети намеренно или по ошибке подключают к публичным сетям, тем самым ставя под угрозу их безопасность. В начале 2018 года эксперты Positive Technologies выявили более 175 000 различных компонентов АСУ ТП, напрямую подключенных к сети Интернет.

Основной тренд — рост числа новых уязвимостей в промышленном сетевом оборудовании. Недостатки безопасности были выявлены в продукции Schneider Electric (47 уязвимостей), Moxa (36) и Siemens (32). Если в 2016 году в сетевых устройствах было разглашено в полтора раза меньше уязвимостей, чем в компонентах SCADA/ЧМИ/РСУ, то по итогам 2017 года разрыв сократился до минимума. К наиболее распространенным типами уязвимостей относятся «Раскрытие информации», «Удаленное выполнение кода» и «Переполнение буфера».

При этом большинство уязвимостей могут быть проэксплуатированы удаленно злоумышленником низкой квалификации, а устранение уязвимостей зачастую попросту невозможно по различным объективным причинам. Таким образом, внешний нарушитель, проникнув в технологическую сеть через корпоративные или публичные сети, может сразу получить максимальные возможности по нарушению работы производственной системы.



Распространенные типы уязвимостей компонентов АСУ ТП



Количество опубликованных в 2017 году уязвимостей по основным производителям компонентов АСУ ТП

Кроме того, к инцидентам информационной безопасности приводят и действия персонала предприятия. Причина может быть в низкой квалификации, халатности, несоблюдении регламентов и правил доступа. Простые пароли, записанные на бумаге, несанкционированное подключение электронных носителей и устройств (USB-накопителей, смартфонов, GSM-модемов) к АРМ оператора, проникновение вредоносного ПО из корпоративной сети (например, через электронную почту) — это лишь малая часть событий, приводящих к инцидентам ИБ и нарушениям в работе технологических систем.

Отдельно стоит отметить угрозы, связанные с персоналом подрядчиков, принимающих участие в проектировании, построении и обслуживании АСУ ТП. Как правило, таким специалистам предоставляются максимальные системные привилегии, а также полный физический или удаленный доступ, при этом контролировать их действия по разным причинам затруднительно. Отсюда случаи некорректной настройки оборудования и злоумышленного изменения режимных параметров, заражения АРМ вредоносными программами в ходе регламентного и оперативного обслуживания.

Обеспечение защиты АСУ ТП от подобных угроз требует комплексного подхода, включающего физическую сегментацию сетей, защиту периметра, внедрение политик безопасности и постоянный мониторинг защищенности. Поскольку стандартные средства защиты узлов и периметра не дают полного представления о текущем состоянии защищенности, рекомендуется использовать специализированные комплексы для непрерывного анализа защищенности АСУ ТП и детектирования инцидентов в реальном времени.

Проведенные Positive Technologies в 2017 году работы по анализу защищенности АСУ ТП показали, что в большинстве случаев можно проникнуть в технологическую сеть из корпоративной инфраструктуры, а также из публичных сетей и получить полный контроль над промышленными системами.

82%

исследованных технологических сетей недостаточно защищены от проникновения из корпоративного сегмента.

Исследование Positive Technologies
«Промышленные компании:
векторы атак, 2018»

100%

промышленных компаний недостаточно строго следят за сложностью используемых паролей. В каждой компании встречаются пароли по умолчанию, пустые пароли или комбинация 123456.

Исследование Positive Technologies
«Промышленные компании:
векторы атак, 2018»

Области применения

Автоматизированные системы управления технологическими процессами промышленных предприятий

Системы управления городских инженерных инфраструктур

Автоматизированные системы управления объектов критической инфраструктуры

Системы управления инженерной инфраструктурой центров обработки данных, деловых и торговых центров

PT ISIM: ключевые возможности

Многолетний опыт анализа защищенности АСУ ТП и разработки прикладных систем позволил экспертам Positive Technologies создать эффективный инструмент непрерывного анализа защищенности промышленных предприятиях — PT Industrial Security Incident Manager (PT ISIM).

- **Безопасность технологического процесса.** Архитектура пассивного мониторинга PT ISIM исключает нежелательное воздействие на технологический процесс.
- **Инвентаризация и контроль целостности сети АСУ ТП.** PT ISIM автоматически инвентаризирует элементы сети, включая компоненты промышленной системы управления, и непрерывно контролирует целостность технологической сети.
- **Визуализация инцидентов.** За счет удобных средств графического отображения элементов сетевой топологии и технологического процесса (мнемосхем) можно визуализировать инциденты информационной безопасности, в том числе на уровне бизнес-логики.
- **Обнаружение сложных атак.** PT ISIM анализирует события информационной безопасности и связывает их в логические цепочки. Цепочка событий позволяет наглядно представить развитие инцидента во времени и в нужный момент принять меры по предотвращению угрозы. Таким образом PT ISIM эффективно выявляет и длительные многоэтапные атаки.
- **Оперативное реагирование на инциденты ИБ.** В случае возникновения инцидента PT ISIM предоставляет ответственным сотрудникам информацию, соответствующую их полномочиям. Оперативный персонал располагает минимальным набором инструментов, необходимых для поддержки административных регламентов, а служба ИБ получает полный доступ к информации об инцидентах для их расследования.
- **Учет специфики предприятия.** С помощью PT ISIM можно контролировать векторы атак, уникальные для промышленного объекта. Для настройки механизма контроля этих векторов используются данные, получаемые в результате анализа защищенности АСУ ТП предприятия.
- **Соответствие требованиям промышленной среды.** Физические условия эксплуатации в промышленности бывают крайне агрессивными. Промышленное исполнение компонентов PT ISIM подбирается с учетом специфики отрасли и защищаемого предприятия.

PT Industrial Security Threat Indicators

Для обнаружения фактов нарушения информационной безопасности PT ISIM использует собственную уникальную базу промышленных киберугроз — PT Industrial Security Threat Indicators (PT ISTI). Она позволяет PT ISIM на ранней стадии выявлять подготовку к кибератакам на ПО и оборудование АСУ ТП (сканирование узлов сети АСУ ТП, эксплуатацию уязвимостей), находить недостатки в настройке систем (слабые пароли, отключенное шифрование), обнаруживать применение потенциально небезопасных средств сетевого взаимодействия (например, устаревшие версии протоколов) и использование недокументированных (в том числе небезопасных) команд управления оборудованием АСУ ТП (ПЛК, промышленными коммутаторами и терминалами).

База угроз помогает PT ISIM превентивно выявлять уязвимости сети АСУ ТП, в том числе те, которые эксплуатируются вирусами-шифровальщиками (например, WannaCry, Petya) и другим вредоносным ПО (например, Trisis/Triton), а также идентифицировать в сети работу майнеров криптовалюты.

Эксперты Positive Technologies регулярно пополняют PT ISTI сигнатурами и правилами обнаружения атак на промышленное оборудование и программное обеспечение. База формируется на основе уязвимостей и типичных недостатков информационной безопасности АСУ ТП, найденных специалистами компании в ходе проектов по анализу защищенности, а также в рамках регулярных исследований новых угроз.

Доставка обновлений в PT ISIM может осуществляться автоматически и вручную. База содержит несколько сотен сигнатур и правил обнаружения различных атак на распространенные системы ABB, Emerson, Hirschman, Schneider Electric, Siemens, Yokogawa.

Построение системы: цели и задачи

Система PT ISIM предназначена для повышения уровня защищенности, доступности и поддержки непрерывности технологических процессов с помощью анализа сетевого трафика и превентивного обнаружения атак, направленных на АСУ ТП.

Цели построения системы

- Непрерывный анализ киберзащищенности АСУ ТП
- Контроль действий персонала и подрядчиков
- Обнаружение нарушений ИБ и кибератак на АСУ ТП
- Своевременное выявление инцидентов и информирование ответственных лиц
- Создание доверенного источника данных для эффективного проведения расследований нарушений ИБ
- Анализ инцидентов, включая определение причин возникновения, а также оценку последствий
- Помощь в планировании мер по устранению и предотвращению инцидентов
- Обеспечение соответствия требованиям регулирующих организаций (в том числе — выполнение приказов ФСТЭК № 31, 239, норм закона о КИИ № 187-ФЗ и выстраивание взаимодействия с центрами ГосСОПКА)

Задачи

- Непрерывная обработка копии трафика АСУ ТП, получаемого через однонаправленный шлюз (диод данных)
- Анализ событий на уровне различных коммуникационных протоколов, включая промышленные (Siemens S7, IEC104, DIGSI, GOOSE/MMS, Schneider Electric UMAS, CIP, Yokogawa, PROFINET DCP, SPA-Bus, EKRA, OPC, Modbus и другие)
- Автоматическая визуализация схемы сети АСУ ТП
- Выявление неавторизованных подключений к сети АСУ ТП
- Детектирование потенциальных угроз и прямых попыток эксплуатации известных уязвимостей
- Обнаружение неавторизованного изменения технологических параметров
- Контроль доступа к параметрам ПЛК по сети (чтение и изменение микропрограмм и проектов ПЛК)
- Обнаружение неавторизованного управления ПЛК по сети
- Выявление сложных, распределенных во времени атак на АСУ ТП (цепочки атак)
- Генерация инцидентов ИБ с учетом логики технологического процесса
- Визуализация мнемосхемы техпроцесса и индикация компонентов, работа которых нарушена в результате инцидентов ИБ
- Формирование и отправка отчетов об инцидентах и состоянии защищенности АСУ ТП во внешние системы (SIEM, ГосСОПКА)

Возможности масштабирования

Решение на базе PT ISIM гибко масштабируется в зависимости от конкретных требований и задач. Внедрение компонентов PT ISIM может происходить поэтапно, не требуя крупных единовременных инвестиций. Базовая версия сетевого сенсора — PT ISIM netView Sensor — требует минимальных усилий по установке и идеально подходит как для пилотного внедрения, так и для каждодневной эксплуатации. В дальнейшем опции лицензирования PT ISIM позволяют расширять функциональность системы без замены оборудования. Итоговое количество компонентов PT ISIM в составе системы не ограничено. На начальных этапах развертывания система может использоваться только на критически важных площадках с последующим полным покрытием всех процессов в промышленной сети.

PT ISIM netView Sensor не требует от пользователей специальных навыков и знаний ни при внедрении, ни в эксплуатации

1 час

занимает подключение PT ISIM netView Sensor к действующему сегменту АСУ ТП

80%

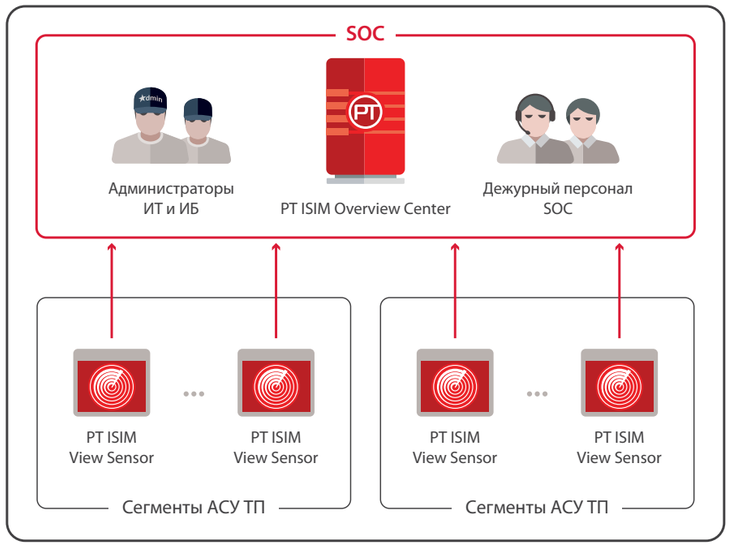
актуальных угроз АСУ ТП может быть обнаружено сенсором PT ISIM netView Sensor без кропотливой предварительной настройки, характерной для других решений

Комплексное решение на базе PT ISIM идеально подходит для организации корпоративного SOC и для оказания коммерческих услуг аутсорсинга ИБ.

Компоненты системы.
Назначение и технические особенности

PT ISIM — программно-аппаратный комплекс, включающий серверы анализа сетевого трафика (сенсоры), серверы бизнес-аналитики и управления уровня ситуационного центра (SOC), а также панельный компьютер, предназначенный для индикации и квитирования критически опасных инцидентов оперативным персоналом промышленных объектов.

- На уровне защищаемого сетевого сегмента АСУ ТП (в котором расположены АРМ операторов, серверы SCADA и ПЛК) применяются серверы сбора и анализа трафика — сенсоры, PT ISIM View Sensor. Они получают копию трафика с порта зеркалирования коммутатора (Mirror/SPAN) или TAP-устройства. При этом между сегментом АСУ ТП и сенсором устанавливается аппаратный однонаправленный шлюз данных (data diode) для исключения влияния PT ISIM на действующий технологический процесс.
- Для централизации процесса обработки инцидентов и организации ситуационного центра используется компонент PT ISIM Overview Center. Он предоставляет сводную информацию о зарегистрированных инцидентах и обеспечивает централизованную настройку и обновление компонентов на подключенных к нему сенсорах.
- Все компоненты PT ISIM работают под управлением ОС Debian. Взаимодействие между компонентами происходит по протоколу HTTPS. Для установки и первоначальной настройки может требоваться доступ по протоколу SSH.
- Для сенсоров PT ISIM View Sensor доступны три вида серверного шасси в зависимости от физических условий эксплуатации. Заказчик может выбрать любой из них. Допускается обновление ранее приобретенной лицензии PT ISIM View Sensor до более функциональной.
- Конечные пользователи и специалисты АСУ ТП работают со всеми компонентами PT ISIM через современный браузерный веб-интерфейс по защищенному соединению (HTTPS).



Компоненты системы.
Основные возможности

Компонент	Назначение и основные возможности
PT ISIM View Sensor 	▪ Анализ копии трафика сегмента АСУ ТП ▪ Обработка событий в реальном времени ▪ Поддержка промышленных и IT-протоколов (DPI) ▪ Автоматическая идентификация узлов сети АСУ ТП (инвентаризация) ▪ Визуализация топологии промышленной сети ▪ Интеллектуальное обнаружение нарушений (неавторизованного управления компонентами АСУ ТП и эксплуатации уязвимостей) ▪ Анализ событий с учетом бизнес-логики техпроцесса ▪ Мощный ретроспективный анализ событий
PT ISIM Overview Center 	▪ Агрегация данных об инцидентах, поступающих с нескольких сенсоров (View Sensor) ▪ Визуализация сводной информации о защищенности (бизнес-аналитика) ▪ Базовый анализ инцидентов и поддержка принятия оперативных решений ▪ Управление параметрами компонентов PT ISIM ▪ Централизованное обновление компонентов PT ISIM ▪ Комплексная диагностика
PT ISIM Industrial Tablet 	▪ Вывод информации о критически опасных инцидентах, требующих от оперативного персонала промышленного объекта немедленного реагирования в соответствии с регламентами ▪ Экспорт данных об инцидентах на внешний носитель

Дополнительные внешние компоненты

Для подключения PT ISIM View Sensor могут использоваться следующие дополнительные компоненты:

- аппаратный диод, обеспечивающий на физическом уровне однонаправленную передачу со SPAN-порта коммутатора на PT ISIM View Sensor[1];
- агрегирующее устройство, позволяющее уменьшить требуемое количество закупаемых PT ISIM View Servers за счет агрегации трафика с нескольких SPAN-портов коммутаторов[2];
- регенерирующее устройство, позволяющее реплицировать трафик с одного SPAN-порта на несколько других портов для устройств мониторинга[3];
- TAP-устройство для получения копии трафика при отсутствии SPAN-порта[4].

1 Например, AK AMT InfoDiode.
2 Например, Ixia iLink Aggregator.
3 Например, Ixia Copper Regen Tap.
4 Например, Ixia Copper Tap.

PT ISIM View Sensor. **Версии сенсора**

Сервер сбора и анализа сетевого трафика (сенсор, PT ISIM View Sensor) имеет две версии, отличающиеся набором функциональных возможностей. Для обновления необходимо приобрести соответствующую лицензию и активировать ее в системе.

Возможность	netView Sensor	proView Sensor
Безопасная и быстрая интеграция с сетью АСУ ТП	+	+
Автоматическое построение карты узлов сети АСУ ТП	+	+
Автоматическое построение карты сетевых коммуникаций АСУ ТП	+	+
Визуализация схемы сети АСУ ТП	+	+
Контроль подключений узлов к сети АСУ ТП в реальном времени	+	+
Поддержка промышленных протоколов (DPI)	+	+
Инструменты поиска и фильтрации событий	+	+
Обнаружение эксплуатации уязвимостей в ПО и оборудовании АСУ ТП	+	+
Контроль целостности сетевых соединений на уровне DPI	+	+
Визуализация инцидентов на схеме сети АСУ ТП	+	+
Автоматическое формирование белых списков сетевых соединений	+	+
Автоматическое формирование белых списков узлов сети	+	+
Управление белыми списками сетевых соединений	+	+
Управление белыми списками узлов сети АСУ ТП	+	+
Запись и хранение трафика сети АСУ ТП	+	+
Экспорт трафика и информации об инцидентах	+	+
Инвентаризация узлов сети АСУ ТП	+	+
Обнаружение сложных многоступенчатых атак	+	+
Ретроспективный анализ событий	+	+
Обнаружение сетевых аномалий	+	+
Режим автоматического обучения (моделирование техпроцесса)	–	+
Контроль технологических параметров	–	+
Интеллектуальная обработка событий с учетом логики техпроцесса	–	+
Визуализация инцидентов на мнемосхеме техпроцесса	–	+
Веб-интерфейс специалиста ИБ АСУ ТП	+	+
Веб-интерфейс оперативного персонала АСУ ТП	–	+
Набор форм стандартных отчетов	+	+
Уведомления по электронной почте об инцидентах ИБ АСУ ТП	+	+
Разграничение прав доступа к системе	+	+
Базовая система управления инцидентами ИБ АСУ ТП	+	+
Инструменты для создания и настройки собственных правил анализа	–	+
Инструменты создания графических мнемосхем	–	+
Расширенный набор форм отчетов	–	+
Передача данных об инцидентах во внешние системы (например, в SIEM-систему)	+	+
Интеграция с Microsoft Active Directory, LDAP	+	+
Обновление встроенной базы знаний промышленных угроз PT ISTI	+	+
Управление через PT ISIM Overview Center	+	+

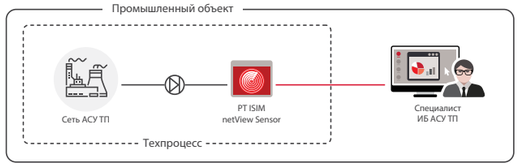
PT ISIM Overview Center. **Программные модули**

Сервер консолидации инцидентов и удаленного управления компонентами PT ISIM Overview Center имеет несколько программных модулей, лицензии на которые приобретаются отдельно.

Модуль PT ISIM Overview Center	Основные возможности
Business Intelligence	▪ Визуализация географической привязки сенсоров ▪ Дашборды ▪ Сводная аналитика по инцидентам ▪ Базовое управление инцидентами
Systems Management	▪ Централизованное управление сенсорами, обновление ПО и базы знаний угроз

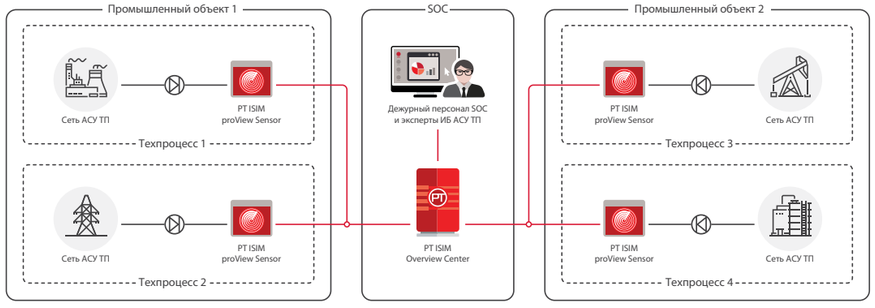
Примеры сценариев использования

Сценарий 1. **Автономное управление и минимальные затраты**



- На каждую из защищаемых площадок устанавливается минимальный набор компонентов (сенсор PT ISIM netView Sensor и при необходимости однонаправленный шлюз данных) для мониторинга информационной безопасности силами специалистов заказчика.
- Не требует глубокого предварительного обследования сети АСУ ТП и технологического процесса.
- Каждый сенсор управляется отдельно.
- Минимальные усилия по развертыванию, не требует специальных знаний.
- Подходит для защиты небольших инфраструктур, а также для поэтапного масштабирования решения на больших предприятиях с распределенной инфраструктурой.

Сценарий 2. **Максимальная эффективность и централизованное управление**



- Необходимо провести анализ защищенности технологических сегментов и компонентов АСУ ТП для достижения максимальной эффективности системы мониторинга.
- При использовании сенсоров PT ISIM proView Sensor векторы атак, найденные в ходе анализа защищенности, могут быть учтены в конфигурации системы мониторинга. Это дает возможность оперативно реагировать на сложные кибератаки, специфичные для конкретной АСУ ТП, включая эксплуатацию уязвимостей нулевого дня.
- Организуется общий ситуационный центр для обработки инцидентов.
- PT ISIM Overview Center централизованно управляет всеми компонентами PT ISIM.

Спецификация оборудования

	View Sensor		
	PTISIM-CHA24	**PTISIM-CH120-N1-H2**	**PTISIM-CH15-N3**
			
Исполнение	Промышленное	Стандартное	
Технические параметры			
Интерфейсы сбора трафика (SPAN/TAP), RJ-45	6 × 1 Гбит/с	3 × 1 Гбит/с	3 × 1 Гбит/с
Интерфейсы управления и вывода информации, RJ-45	2 × 1 Гбит/с	1 × 1 Гбит/с	1 × 1 Гбит/с
Процессор	1 × Intel Core i7	2 × Intel Xeon Silver 4108 1,8 ГГц 8C/16T	Intel Xeon E3-1230 v6 3,5 ГГц 4C/8T
Оперативная память	16 ГБ ОЗУ	32 ГБ ОЗУ	16 ГБ ОЗУ
Жесткие диски	2 × 1 ТБ SATA	4 × 1,2 ТБ 10K SAS; RAID 1 + RAID 1	2 × 1 ТБ 7,2K SATA; RAID 1
Блоки питания	AC/DC 100—240 В 1 × 22 Вт	Двойные блоки питания, Hot-plug (1+1), 550 Вт	Одинарный блок питания, 250 Вт
Тепловыделение	75 BTU/час	2559 BTU/час	1039 BTU/час
Сертификаты	CE, FCC, CCC, Electricity IV level for China, IEC-61850-3, IEEE-1613, UL, CB, LVD	CE, FCC	CE, FCC
Физические параметры			
Монтаж (крепление)	2U (стойка 19″)	1U (стойка 19″)	1U (стойка 19″)
Размер (Ш × Д × В)	440 × 280 × 88 мм	482 × 692,6 × 42,8 мм	482,4 × 493,9 × 42,8 мм
Масса	6,0 кг	17,5 кг	9,5 кг
Степень защиты IP	40	20	20
Охлаждение	Пассивное, без вентиляторов	Активное, вентиляторное	Активное, вентиляторное
Условия эксплуатации			
Температура	–25…+70 °C	10–35 °C	10–35 °C
Влажность	20%–95%	20%–80%	20%–80%
Вибрация	2 G_{rms}	0,26 G_{rms}	0,26 G_{rms}

	12,1″ XGA LCD Panel PC	Overview Center	
	PTISIM-CHT12	**PTISIM-CH15**	**PTISIM-CH120-H2**
			
Исполнение	Промышленное	Стандартное	
Технические параметры			
Интерфейсы сбора трафика (SPAN/TAP), RJ-45	–	–	–
Интерфейсы управления и вывода информации, RJ-45	2 × 1 Гбит/с	2 × 1 Гбит/с	2 × 1 Гбит/с
Процессор	1 × Intel Celeron	Intel Xeon E3-1230 v6 3,5 ГГц 4C/8T	2x Intel Xeon Silver 4108 1,8 ГГц 8C/16T
Оперативная память	4 ГБ ОЗУ	16 ГБ ОЗУ	32 ГБ ОЗУ
Жесткие диски	128 ГБ SSD mSATA	2 × 1 ТБ 7,2K SATA; RAID 1	4 × 1,2 ТБ 10K SAS; RAID 1 + RAID1
Блоки питания	AC 100—240 В DC 12—24 В, 1 × 90 Вт	Одинарный блок питания, 250 Вт	Двойные блоки питания, Hot-plug (1+1), 550 Вт
Тепловыделение	310 BTU/час	1039 BTU/час	2559 BTU/час
Сертификаты	CE, FCC	CE, FCC	CE, FCC
Физические параметры			
Монтаж (крепление)	Настенное, настольное	1U (стойка 19″)	1U (стойка 19″)
Размер (Ш × Д × В)	317 × 246 × 49 мм	482,4 × 493,9 × 42,8 мм	482 × 692,6 × 42,8 мм
Масса	2,1 кг	9,5 кг	17,5 кг
Степень защиты IP	65	20	20
Охлаждение	Пассивное, без вентиляторов	Активное, вентиляторное	Активное, вентиляторное
Условия эксплуатации			
Температура	0–50 °C	10–35 °C	10–35 °C
Влажность	10%–95%	20%–80%	20%–80%
Вибрация	2 G_{rms}	0,26 G_{rms}	0,26 G_{rms}

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

PT-ISIM_DS_A4.RUS.0013.18.JUN.28.2018