Positive Technologies
Industrial Security
Incident Manager

# ОПИСАНИЕ ПРОДУКТА

POSITIVE TECHNOLOGIES

*«Более 75% уязвимостей, опубликованных в 2016 году, было обнаружено в компонентах АСУ ТП лидирующих производителей — Siemens, Advantech, Schneider Electric и Moxa. Более половины найденных уязвимостей имеют критическую и высокую степень риска».*

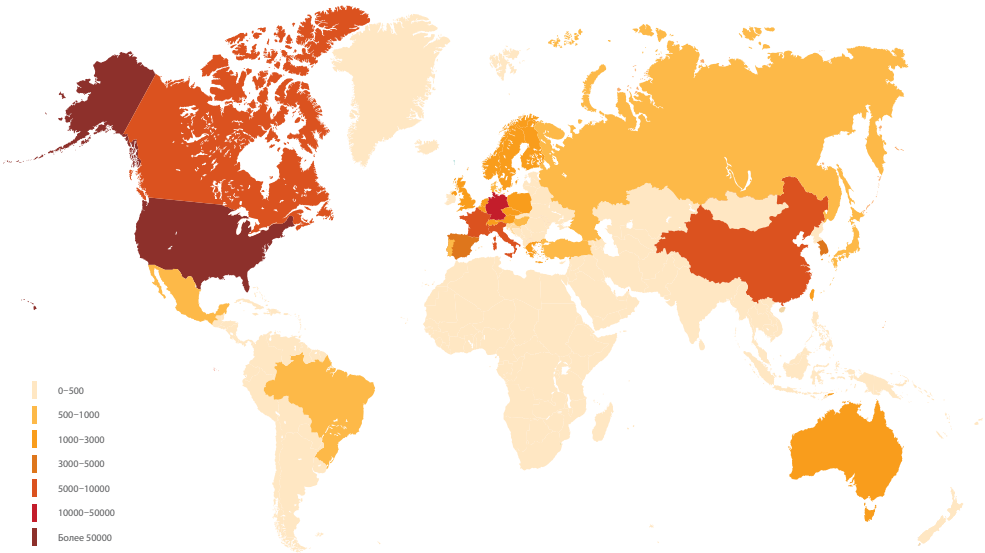
Ежегодное исследование Positive Research, 2017

# 1. 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.

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.

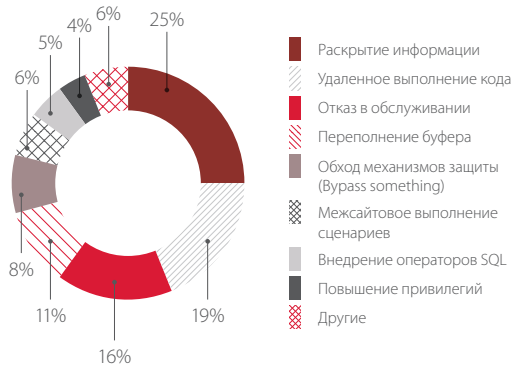
Для эффективного решения бизнес-задач промышленные компании, напротив, стремятся интегрировать корпоративные и производственные IT-инфраструктуры. Все чаще технологические сети намеренно или по ошибке подключают к публичным сетям, тем самым ставя под угрозу их безопасность. По состоянию на начало 2017 года эксперты Positive Technologies выявили более 160 000 различных компонентов АСУ ТП, напрямую подключенных к сети Интернет.



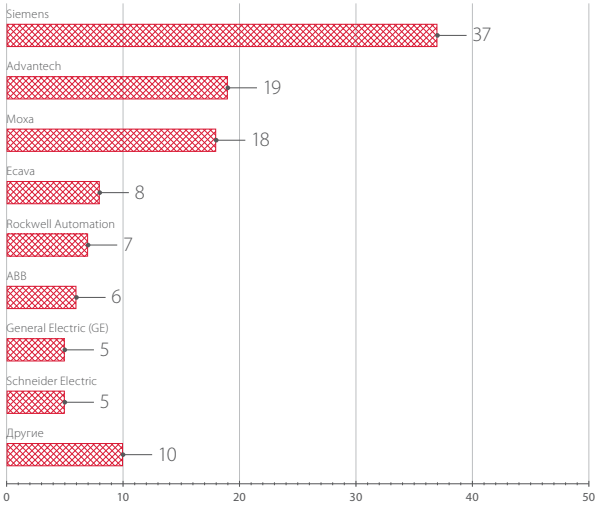

Количество компонентов АСУ ТП, доступных в сети Интернет (распределение по странам)

Еще одна проблема — уязвимости подсистем и компонентов АСУ ТП. Их количество уже давно остается стабильно высоким. Как показали наши исследования, большая часть уязвимостей, опубликованных в 2016 году, приходится на устройства, выполняющие функции диспетчеризации и мониторинга (ЧМИ/SCADA), а наиболее распространенные типы уязвимостей — «Удаленное выполнение кода», «Отказ в обслуживании» и «Раскрытие информации».

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




Уязвимости по основным производителям компонентов АСУ ТП

*Проведенные Positive Technologies в 2016 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.*

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 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 безопасности 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.

## 2. 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).

*«Это первый в мире практический опыт обеспечения киберзащищенности микропроцессорных систем управления движением поездов».*

Исполнительный директор ООО «Бомбардье Транспортейшн (Сигнал)» В. А. Гросс о проекте внедрения PT ISIM для защиты российских железных дорог от киберугроз

- **Безопасность технологического процесса.** Архитектура пассивного мониторинга PT ISIM исключает нежелательное воздействие на технологический процесс.
- **Контроль целостности сети.** 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 (мнемосхемы), 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 соответствующие 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 PT ISIM подбирается с учетом специфики отрасли и защищаемого предприятия.

# 3. 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.

## 3.1. 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 приказа ФСТЭК № 31, норм закона о КИИ и выстраивание взаимодействия с центрами системы ГосСОПКА)

## 3.2. Задачи

PT ISIM решает задачи:

- Непрерывная обработка копии трафика АСУ ТП, получаемого через однонаправленный шлюз (диод данных)
- Анализ событий на уровне различных коммуникационных протоколов, включая промышленные (S7, Modbus, IEC)
- 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 настройкам 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 информации об инцидентах и состоянии защищенности АСУ ТП во внешние системы (SIEM, ГосСОПКА)

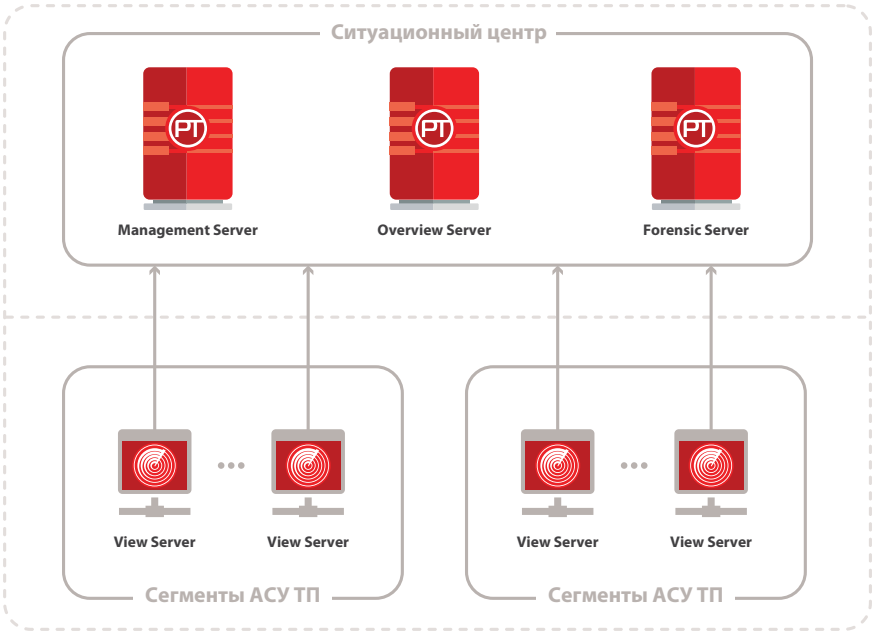
## Возможности масштабирования

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 Traffic View Server — 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 сети промышленных объектов.

## 4. КОМПОНЕНТЫ СИСТЕМЫ. НАЗНАЧЕНИЕ И ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ

Система PT ISIM представляет из себя 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, View Servers. 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 организации ситуационного центра используются компоненты Overview Server (сводная информация о зарегистрированных инцидентах), Forensic Server (расследование инцидентов) и Management Server (централизованная настройка и обновление компонентов системы).
- Все компоненты работают под управлением ОС Debian. Взаимодействие между всеми компонентами PT ISIM производится по протоколу HTTPS. Для установки и первоначальной настройки может требоваться доступ по протоколу SSH.
- Для серверов-сенсоров (View Servers) доступны четыре вида шасси в зависимости от физических условий эксплуатации. Заказчик может выбрать любой из них. Допускается обновление ранее приобретенной лицензии PT ISIM View Server до более функциональной (при этом не требуется замена аппаратного шасси).
- Конечные пользователи (инженеры по кибербезопасности) работают со всеми компонентами PT ISIM через современный браузерный веб-интерфейс по защищенному соединению (HTTPS).



# 5. КОМПОНЕНТЫ СИСТЕМЫ. ОСНОВНЫЕ ВОЗМОЖНОСТИ

| Компоненты | Назначение и основные возможности |
|---|---|
| **PT ISIM View Server** | + Анализ копии трафика сегмента АСУ ТП<br>+ Обработка событий в реальном времени<br>+ Поддержка промышленных и IT-протоколов (DPI)<br>+ Автоматическая идентификация узлов<br>+ Визуализация топологии промышленной сети<br>+ Интеллектуальное обнаружение нарушений ИБ<br>+ Анализ событий с учетом бизнес-логики техпроцесса<br>+ Мощный ретроспективный анализ событий |
| **PT ISIM Overview Server** | + Агрегация данных об инцидентах, поступающих с нескольких сенсоров (View Servers)<br>+ Визуализация сводной информации о защищенности (бизнес-аналитика)<br>+ Базовый анализ инцидентов и поддержка принятия оперативных решений |
| **PT ISIM Forensic Server** | + Агрегация полного объема данных для расследования инцидентов, включая необходимые копии трафика с сенсоров<br>+ Управление инцидентами (жизненный цикл)<br>+ Моделирование инцидентов с учетом актуальной на тот момент конфигурации системы<br>+ Импортирование данных об инцидентах с внешнего носителя |
| **PT ISIM Management Server** | + Управление параметрами компонентов PT ISIM<br>+ Обновление компонентов PT ISIM<br>+ Комплексная диагностика |
| **PT ISIM Industrial Tablet** | + Вывод информации о критически опасных инцидентах, требующих от оперативного персонала промышленного объекта немедленного реагирования в соответствии с регламентами<br>+ Экспорт данных об инцидентах на внешний носитель |

## ДОПОЛНИТЕЛЬНЫЕ ВНЕШНИЕ КОМПОНЕНТЫ

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

+ аппаратный диод, обеспечивающий на физическом уровне однонаправленную передачу со SPAN-порта коммутатора на PT ISIM View Server[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 SERVER. ВЕРСИИ СЕНСОРА

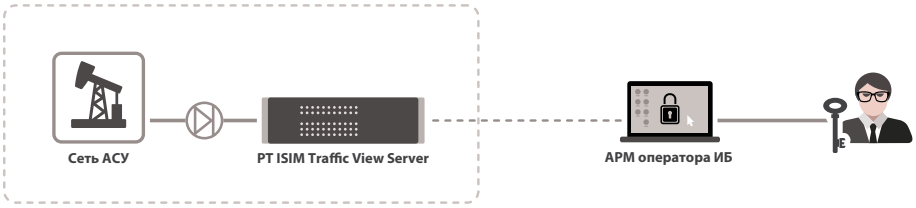
Сервер сбора и анализа сетевого трафика (сенсор, PT ISIM View Server) имеет три версии, отличающиеся набором функциональных возможностей. Для обновления необходимо приобрести соответствующую лицензию и активировать ее в системе.

| Возможности | Traffic View Server | Basic View Server | Full View Server |
|---|---|---|---|
| Безопасная интеграция с сетью АСУ ТП | + | + | + |
| Запись, анализ и хранение трафика сети | + | + | + |
| Автоматическая инвентаризация узлов сети | + | + | + |
| Визуализация сетевой топологии | + | + | + |
| Контроль целостности сети в реальном времени | + | + | + |
| Поддержка промышленных протоколов (DPI) | + | + | + |
| Обнаружение эксплуатации уязвимостей | + | + | + |
| Поддержка правил популярных IDS (SNORT/Suricata) | – | + | + |
| Обнаружение аномалий на уровне DPI | + | + | + |
| Обнаружение многоступенчатых атак | + | + | + |
| Ретроспективный анализ событий | + | + | + |
| Визуализация инцидентов на сетевой топологии | + | + | + |
| Система управления инцидентами | – | + | + |
| Экспорт инцидентов для внешнего анализа | + | + | + |
| Веб-интерфейс | + | + | + |
| Система отчетов | – | + | + |
| Ролевая модель доступа | – | До 3 пользователей | До 10 пользователей |
| Интеграция с AD/LDAP | – | + | + |
| Диспетчерский интерфейс[1] | – | + | + |
| Контроль технологических параметров | – | + | + |
| Детектирование сетевых аномалий | – | + | + |
| Интеллектуальная обработка событий с учетом бизнес-логики[1] | – | – | + |
| Визуализация инцидентов на мнемосхеме техпроцесса[1] | – | – | + |
| Интеграция с внешними системами[1] | + | + | + |
| Интеграция с Management & Overview & Forensic Server | + | + | + |

1 Требуются дополнительные работы по конфигурированию решения.

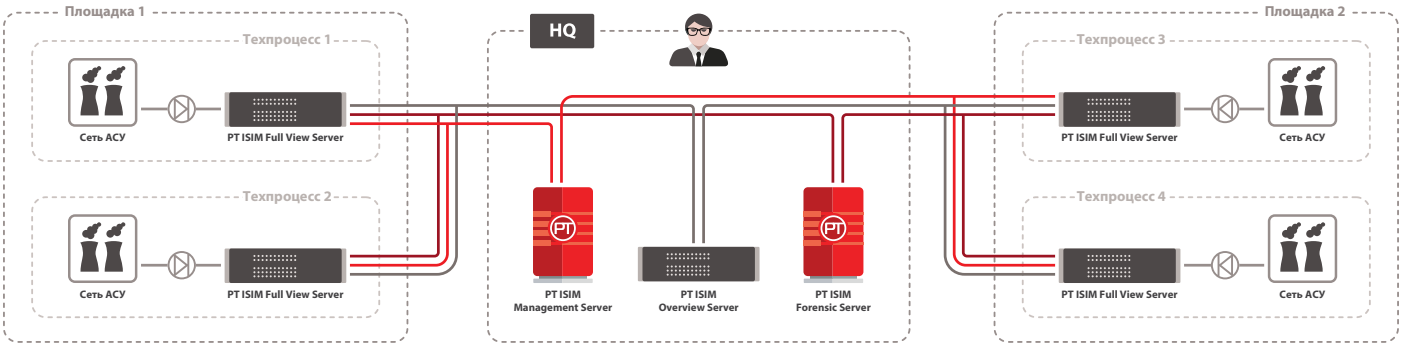
# 6. СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

## Сценарий 1. Автономное управление и минимальные затраты




- На каждую из защищаемых площадок устанавливается минимальный набор компонентов (сенсор PT ISIM Traffic View Server и при необходимости однонаправленный шлюз данных) для мониторинга сетевого трафика силами ИБ-специалистов заказчика.
- Предварительное обследование технологического процесса не требуется.
- Каждый PT ISIM Traffic View Server управляется отдельно.
- Минимальные усилия по развертыванию.
- Подходит как для пилотного тестирования, так и для защиты небольших инфраструктур.

## 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 Full View Servers и PT ISIM Basic View Servers 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.
- Организуется общий ситуационный центр для обработки инцидентов со множества площадок и сенсоров.
- PT ISIM Management Server централизованно управляет всеми компонентами PT ISIM.
- Для централизованного сбора информации и расследования инцидентов сотрудниками ситуационного центра используется PT ISIM Forensic Server.

## 7. СПЕЦИФИКАЦИЯ ОБОРУДОВАНИЯ

| | 12,1" XGA LCD Panel PC | View & Forward Servers | | | |
|---|---|---|---|---|---|
| | PT-CHT12-IS | PT-CHA11-IS | PT-CHA21-IS | PT-CHA22-IS | PT-CH10-N3-IS |
| Исполнение | Промышленное | | | | Стандартное |
| **Технические параметры** | | | | | |
| Интерфейсы сбора трафика (SPAN/TAP) | | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) |
| Интерфейсы управления и вывода информации | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) |
| Процессор | 1 × Intel Celeron | 1 × Intel Core i7 | 1 × Intel Core i7 | 1 × Intel Core i7 | 1 × Intel Xeon E3 |
| Оперативная память | 4 ГБ ОЗУ | 16 ГБ ОЗУ | 16 ГБ ОЗУ | 16 ГБ ОЗУ | 16 ГБ ОЗУ |
| Жесткие диски | 128 ГБ SSD mSATA | 2 × 1 ТБ SATA | 2 × 1 ТБ SATA | 2 × 1 ТБ SATA | 2 × 1 ТБ SATA |
| Блоки питания | AC 100–240V DC 12–24V, 1 × 90W | AC 100–240V 1 × 350W | AC/DC 100–240V 1 × 22W | AC/DC 100–240V 1 × 22W | AC 100–240V 1 × 250W |
| Тепловыделение | 310 BTU/час | 1195 BTU/час | 75 BTU/час | 75 BTU/час | 1039 BTU/час |
| Сертификаты | CE, FCC | CE, FCC | CE, FCC, IEC-61850-3 | CE, FCC, IEC-61850-3 | CE, FCC |
| **Физические параметры** | | | | | |
| Монтаж (крепление) | Настенное, настольное | 1U (стойка 19") | 2U (стойка 19") | 2U (стойка 19") | 1U (стойка 19") |
| Размер (Ш × Д × В) | 317 × 246 × 49 мм | 480 × 497 × 44 мм | 440 × 280 × 88 мм | 440 × 280 × 88 мм | 482 × 497 × 43 мм |
| Масса | 2,1 кг | 8,0 кг | 6,0 кг | 6,0 кг | 7,5 кг |
| Степень защиты IP | 65 | 20 | 40 | 40 | 20 |
| Охлаждение | Пассивное, без вентиляторов | Активное, вентиляторное | Пассивное, без вентиляторов | Пассивное, без вентиляторов | Активное, вентиляторное |
| **Условия эксплуатации** | | | | | |
| Температура | 0–50 °C | 0–40 °C | 0–40 °C | –25 … +70 °C | 10–35 °C |
| Влажность | 10%–95% | 10%–80% | 20%–95% | 20%–95% | 20%–80% |
| Вибрация | 2 $G_{rms}$ | 0,5 $G_{rms}$ | 0,5 $G_{rms}$ | 2 $G_{rms}$ | 0,26 $G_{rms}$ |

| | Management Server | Overview Server | Forensic Server |
|---|---|---|---|
| | PT-CH10-IS | PT-CH210-IS | PT-CH210-M2-H3-IS |
| Исполнение | Стандартное | | |
| **Технические параметры** | | | |
| Интерфейсы управления и вывода информации | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) | 2 × 1 Гбит/с (1000BASE-T) |
| Процессор | 1 × Intel Xeon E3 | 2 × Intel Xeon E5 | 2 × Intel Xeon E5 |
| Оперативная память | 16 ГБ ОЗУ | 64 ГБ ОЗУ | 128 ГБ ОЗУ |
| Жесткие диски | 2 × 1 ТБ SATA | 2 × 1,2 ТБ SAS | 4 × 1,2 ТБ SAS + 4 × 4 ТБ SATA |
| Блоки питания | AC 100–240V 1 x 250W | AC 100–240V 2 x 750W | AC 100–240V 2 x 750W |
| Тепловыделение | 1039 BTU/час | 2891 BTU/час | 2891 BTU/час |
| Сертификаты | CE, FCC | CE, FCC | CE, FCC |
| **Физические параметры** | | | |
| Монтаж (крепление) | 1U (стойка 19″) | 2U (стойка 19″) | 2U (стойка 19″) |
| Размер (Ш × Д × В) | 482 × 497 × 43 мм | 482 × 613 × 87 мм | 482 × 613 × 87 мм |
| Масса | 7,5 кг | 21,5 кг | 23,5 кг |
| Степень защиты IP | 20 | 20 | 20 |
| Охлаждение | Активное, вентиляторное | Активное, вентиляторное | Активное, вентиляторное |
| **Условия эксплуатации** | | | |
| Температура | 10–35 °C | 10–35 °C | 10–35 °C |
| Влажность | 20%–80% | 10%–80% | 10%–80% |
| Вибрация | 0,26 $G_{rms}$ | 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. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays