Positive Technologies Industrial Security Incident Manager

Руководство оператора

POSITIVE TECHNOLOGIES

Содержание

1. Об этом документе

Руководство оператора безопасности содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies Industrial Security Incident Manager (далее также — PT ISIM) для защиты и управления информационными активами организации. В руководстве вы также найдете инструкции по настройке ключевых и дополнительных функции продукта для выполнения конкретных задач. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию PT ISIM .

Руководство адресовано руководителям и специалистам, ответственным за обеспечение информационной безопасности, контроль и расследование инцидентов.

Комплект документации PT ISIM включает в себя следующие документы:

- Этот документ.
- Руководство по установке — содержит инструкции по установке, первоначальной настройке, обновлению и удалению продукта.

В этом разделе

1.1. Условные обозначения

В этом документе могут встречаться условные обозначения (см. таблицу 1).

Таблица 1. Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети...	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты...	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
Нажмите кнопку **OK**.	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом

Пример текста с условным обозначением	Описание
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о продукте

Вы можете найти дополнительную информацию о "Позитив Текнолоджиз" на www.ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов ЗАО "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 10.).

2. О PT ISIM

Positive Technologies Industrial Security Incident Manager (PT ISIM) — это программно-аппаратный комплекс для обеспечения кибербезопасности автоматизированных систем управления технологическим процессом (АСУ ТП).

Основные функции PT ISIM:

- анализ трафика с целью обнаружения атак на промышленную сеть;
- снижение рисков возникновения таких угроз информационной безопасности, как несанкционированное подключение, атаки методом перебора пароля, неправомерные управляющие команды и подмена прошивки промышленного оборудования;
- расследование инцидентов, включая ретроспективный анализ на основе сохраненной копии трафика.

3. Принцип работы PT ISIM

Ниже приводится основная информация о принципе работы PT ISIM.

В этом разделе

3.1. Алгоритм обработки трафика

PT ISIM анализирует сетевой трафик и выявляет инциденты на основе правил корреляции и моделирования.

Обработка трафика в PT ISIM происходит в несколько этапов:

1. Сбор — захват трафика по протоколам FTP, HTTP, Telnet, ARP, MMS, МЭК 104, DIGSI, GOOSE, NTP, SNTP, а также по протоколам Bombardier (COS и FEU) с целью извлечения информации о каждом событии. Собранная информация передается на нормализацию, а исходная копия трафика сохраняется на жестком диске сервера в формате Pcap.
2. Нормализация — извлечение данных из атрибутов записей, которые могут иметь разный формат, и приведение их к единому формату нормализованных сообщений. Нормализованное сообщение имеет заданный набор полей, каждое из которых имеет определенные допустимые значения. Такой формат сообщения позволяет однозначно определить основные параметры события, отнести его к определенному узлу и устройству, а также провести дальнейший анализ события на основе значений отдельных полей.
3. Фильтрация — удаление сообщений, не представляющих интереса с точки зрения информационной безопасности.
4. Агрегация — группировка повторяющихся сообщений об однотипных событиях в единое сообщение согласно правилам агрегации. Правила агрегации определяют набор полей, совпадение по которым приводит к группировке нескольких сообщений в одно, а также период, на который распространяется агрегация.
5. Корреляция — проверка потока событий на соответствие определенному правилу. Результатом сработавшего правила корреляции является скоррелированное сообщение.
6. Моделирование — составление актуальной карты вычислительной сети, отражающей ее реальный состав и взаимодействие между узлами. На основе правил, учитывающих текущие данные модели, PT ISIM принимает решение о том, является ли событие или скоррелированное сообщение инцидентом.

Итогом обработки трафика является заведение записей о событиях и инцидентах в PT ISIM .

3.2. Безопасность хранения и передачи данных

Безопасность хранения и передачи данных при работе с PT ISIM имеет два аспекта:

- Исключается любое воздействие PT ISIM на технологические процессы предприятия, поскольку для сбора трафика PT ISIM подключается к SPAN-портам коммутаторов через диод данных. Подобное решение делает невозможным передачу данных от PT ISIM в сеть АСУ ТП как при нормальной работе продукта, так и в случае непредвиденного изменения настроек коммутатора или PT ISIM .
- Используются следующие инструменты обеспечения собственной безопасности PT ISIM:
  - Сценарий secure.sh. Его запуск реализует настраивает межсетевой экран таким образом, что запрещаются любые соединения с внешней сетью, кроме входящих TCP-соединений на порты 22, 80, 443 и входящих IMCP-соединений (эхо-запросов), а также ограничивает доступ к компонентам Redis и RabbitMQ, устанавливая пароли и разрешая соединения только в пределах сервера.
  - Защищенное соединение с веб-интерфейсом пользователя по HTTPS, а также перенаправление запросов, адресованных порту 80 (HTTP), на порт 443 (HTTPS).
  - Компонент Firewall, который предотвращает изменение настроек межсетевого экрана или его отключение.
  - Мониторинг состояния сетевого подключения PT ISIM к коммутаторам, с которых собирается трафик. Отсутствие подключения рассматривается как инцидент.
  - Мониторинг состояния компонентов Redis и RabbitMQ. Служба Watchdog периодически отправляет им запросы и принудительно перезапускает их, если они не отвечают на запросы в течение заданного времени или отвечают сообщением с ошибкой.

4. Вход в PT ISIM

Перед входом в PT ISIM обратитесь в техническую поддержку “Позитив Текнолоджиз” для получения адреса, имени для входа и пароля.

Чтобы войти в PT ISIM:

1. В адресной строке браузера введите адрес PT ISIM.
2. В открывшейся странице входа (см. рисунок 1) введите имя пользователя и пароль.
3. Нажмите кнопку **Войти**.

Рисунок 1. Страница входа в PT ISIM

Если имя и пароль введены корректно, откроется главная страница PT ISIM — страница **События** (см. рисунок 2).

5. Интерфейс PT ISIM

Интерфейс PT ISIM состоит из трех основных страниц: **События**, **Зафиксированные инциденты** и **Топология**. Ниже приводится описание основных элементов управления на этих страницах.

В этом разделе

5.1. Страница События

Страница **События** является главной страницей PT ISIM и служит для работы с событиями. На рисунке 2 представлены основные элементы страницы **События**.

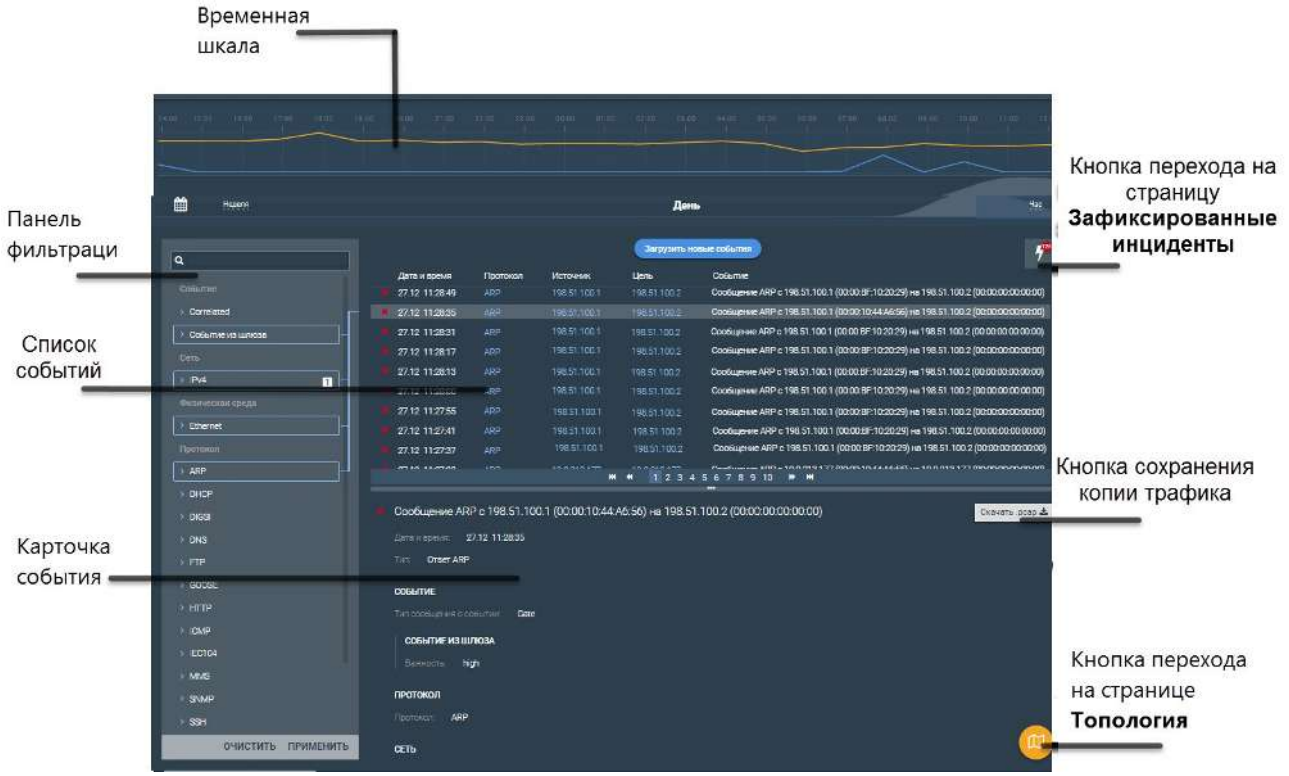


Рисунок 2. Страница **События**

На временной шкале количество событий отображается в виде графиков, каждый из которых соответствует уровню важности: синий график — информационный уровень, желтый — средний уровень, красный — высокий уровень. Инциденты обозначаются красной вертикальной линией.

5.2. Страница Зафиксированные инциденты

Страница **Зафиксированные инциденты** (см. рисунок 3) служит для работы с инцидентами, обнаруженными PT ISIM.

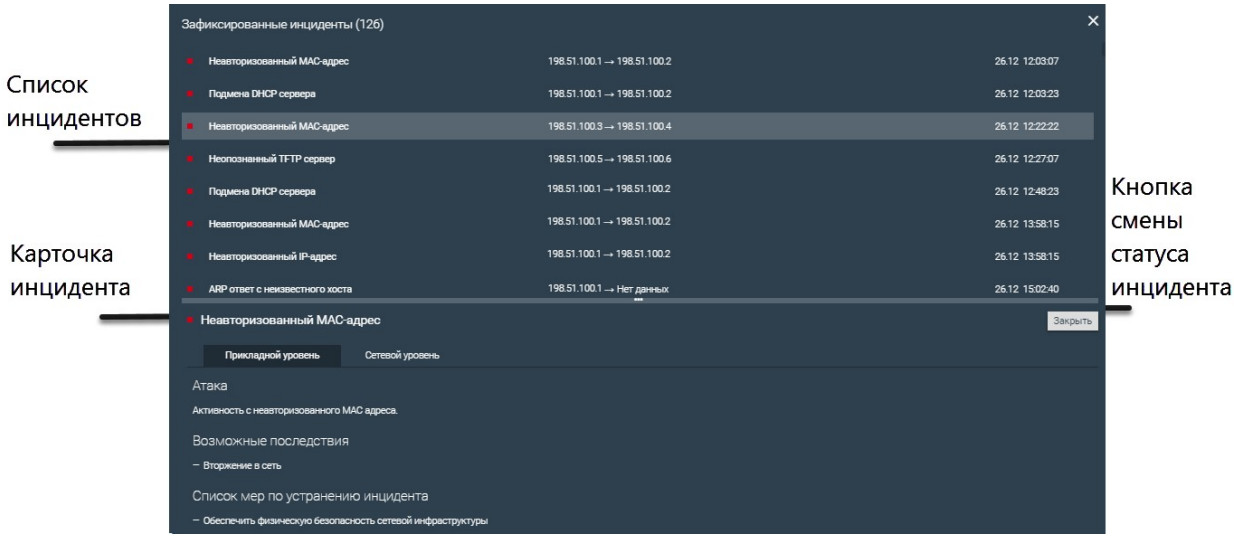


Рисунок 3. Страница Зафиксированные инциденты

Перейти на страницу **Зафиксированные инциденты** вы можете по кнопке на странице **События**. Данная кнопка указывает количество открытых инцидентов.

5.3. Страница Топология

Страница **Топология** (см. рисунок 4) представляет из себя карту вычислительной сети, состоящую из элементов (узлов) сети и связей между ними на сетевом уровне.

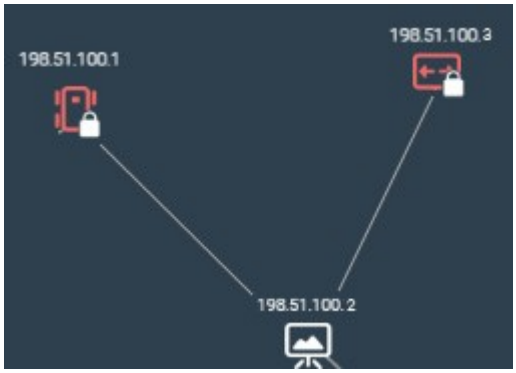


Рисунок 4. Страница Топология

Перейти на страницу **Топология** вы можете по кнопке на странице **События**.

6. Работа с событиями

Ниже приведена основная информация о событиях в PT ISIM, а также даны инструкции по работе с ними.

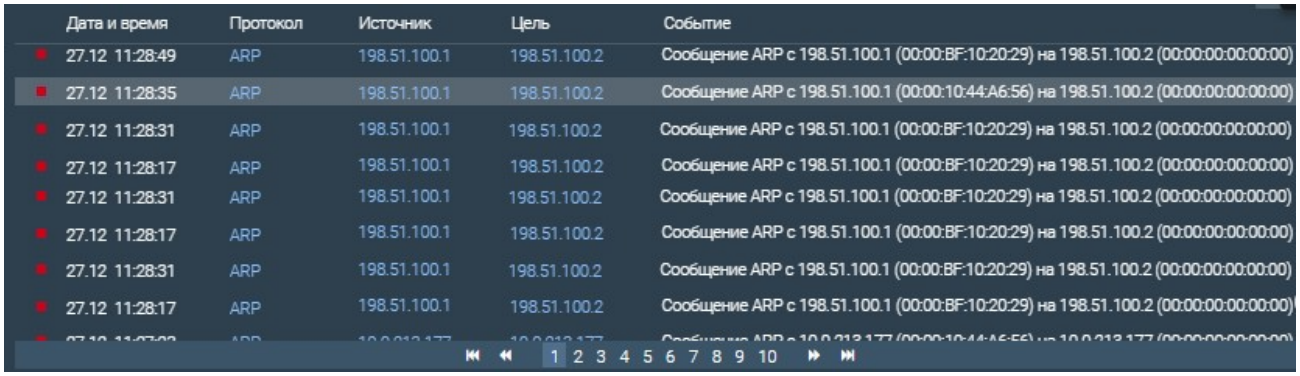
В этом разделе

- О событии (см. раздел 6.1)
- Просмотр подробной информации о событии (см. раздел 6.2)
- Переход между страницами списка событий (см. раздел 6.3)
- Настройка отображения списка событий (см. раздел 6.4)
- Обновление списка событий (см. раздел 6.5)

6.1. О событии

Событие — это запись об активности в сети, обнаруживаемой PT ISIM.

Список событий приводится на странице **События** (см. рисунок 5). Для каждого события в списке отображаются следующие атрибуты: **Важность**, **Дата и время**, **Протокол**, **Источник**, **Цель**, а также приводится его краткое описание.



	Дата и время	Протокол	Источник	Цель	Событие
🟥	27.12 11:28:49	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:35	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:10:44:A6:56) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:31	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:17	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:31	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:17	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:31	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)
🟥	27.12 11:28:17	ARP	198.51.100.1	198.51.100.2	Сообщение ARP с 198.51.100.1 (00:00:BF:10:20:29) на 198.51.100.2 (00:00:00:00:00:00)

Рисунок 5. Список событий

Важность событий бывает трех уровней:

1. Информационный. События такого уровня информируют о нормальной работе сети и не приводят к нарушению информационной безопасности предприятия. Например, запрос на получение файла по протоколу TFTP. События информационного уровня важности обозначаются синим цветом.
2. Средний. События такого уровня свидетельствуют о нарушении информационной безопасности и могут являться подготовительными действиями для проникновения в защищаемую сеть. Например, сканирование портов с неизвестного узла, несанкционированное получение конфигурации устройства. События среднего уровня важности обозначаются желтым цветом.

3. Высокий. События такого уровня свидетельствуют о нарушении информационной безопасности и требуют особого внимания, так как могут привести к ошибкам в работе оборудования или даже вывести его из строя. Например, отправка по промышленному протоколу несанкционированной команды на управление устройством. События высокого уровня важности обозначаются красным цветом.

6.2. Просмотр подробной информации о событии

Чтобы просмотреть подробную информацию о событии, выберите событие в списке.

В нижней части страницы отобразится карточка события (см. рисунок 6), содержащая подробную информацию о событии.

Рисунок 6. Карточка события

6.3. Переход между страницами списка событий

Список событий разбит на страницы по 50 событий, расположенных в порядке их обнаружения, от последних к более ранним.

Чтобы перейти на страницу с более ранними событиями, выберите номер страницы или нажмите .

Чтобы перейти на страницу с более поздними событиями, выберите номер страницы или нажмите .

Чтобы просмотреть список 50 самых ранних событий, нажмите .

Чтобы просмотреть список 50 последних событий, нажмите .

6.4. Настройка отображения списка событий

PT ISIM позволяет фильтровать события, то есть настроить отображение только тех событий, которые соответствует определенному критерию. Ниже приводятся инструкции по использованию фильтрации.

В этом разделе

6.4.1. Фильтрация событий по атрибуту

Чтобы выполнить фильтрацию событий по атрибуту:

1. В панели фильтрации в левой части экрана выберите один или несколько атрибутов и их значения (см. рисунок 7).
2. Нажмите **Применить**.

В списке будут отображены только события, имеющие выбранное значение параметра.

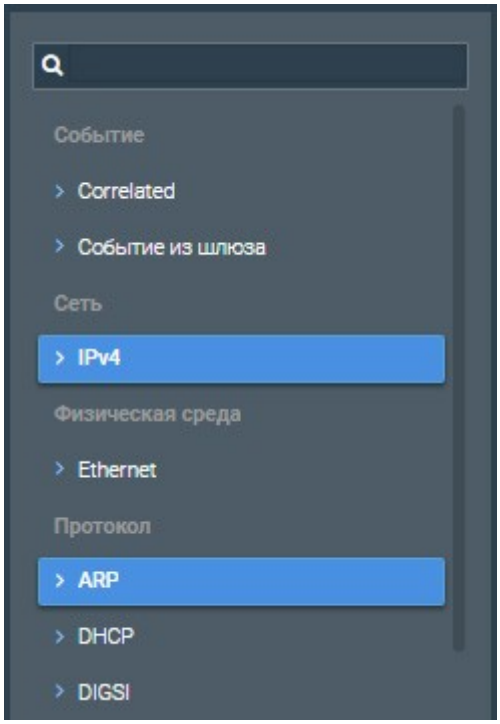


Рисунок 7. Фильтрация события по значению атрибутов

Если в списке выбрано событие, в панели фильтрации выделяются атрибуты, относящиеся к выбранному событию (см. рисунок 8).

Чтобы отобразить события, имеющие совпадения по одному или нескольким атрибутам с выделенным событием, выберите выделенные атрибуты в панели фильтрации.

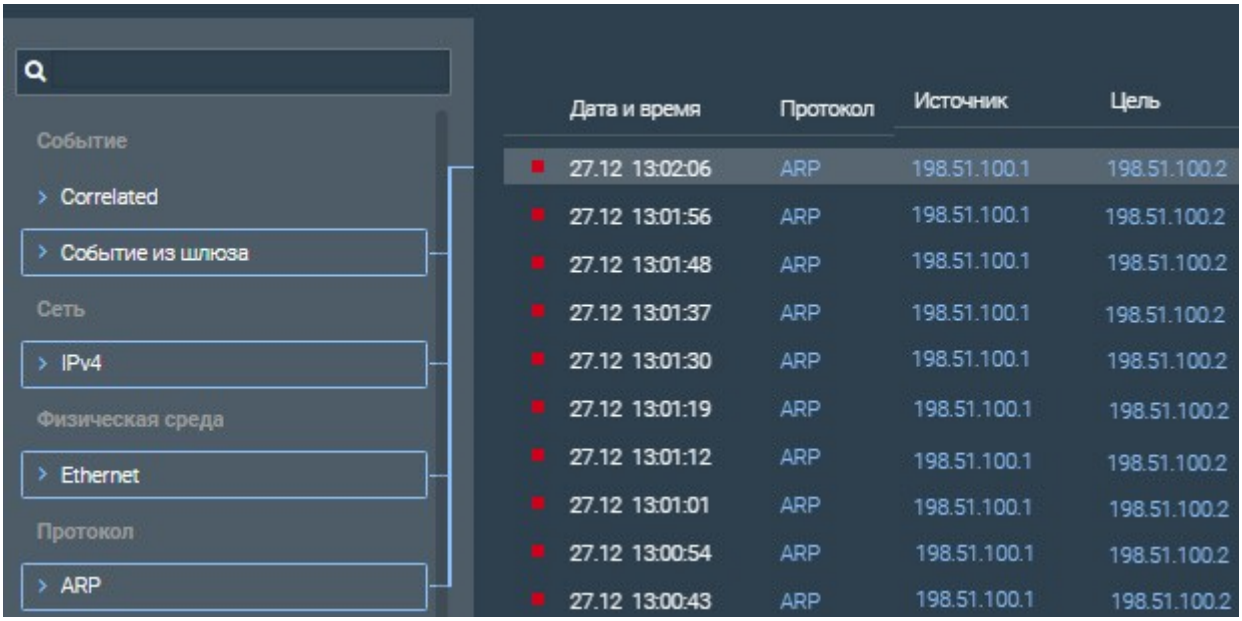


Рисунок 8. Выделение атрибутов события в панели фильтрации

Чтобы сбросить примененный фильтр, нажмите кнопку **Очистить** в нижней части панели фильтрации.

6.4.2. Фильтрация событий по времени

Чтобы выполнить фильтрацию событий в пределах последнего часа:

1. Выберите **Час** в нижней части временной шкалы.

   В списке будут отображены события за последние 60 минут. Цена деления шкалы составит пять минут.

2. Выделите интервал на временной шкале, удерживая левую кнопку мыши.

В списке будут отображены события за выбранный период.

Чтобы выполнить фильтрацию событий в пределах последних суток:

1. Выберите **День** в нижней части временной шкалы.

   В списке будут отображены события за последние 24 часа. Цена деления шкалы составит один час.

2. Выделите интервал на временной шкале, удерживая левую кнопку мыши.

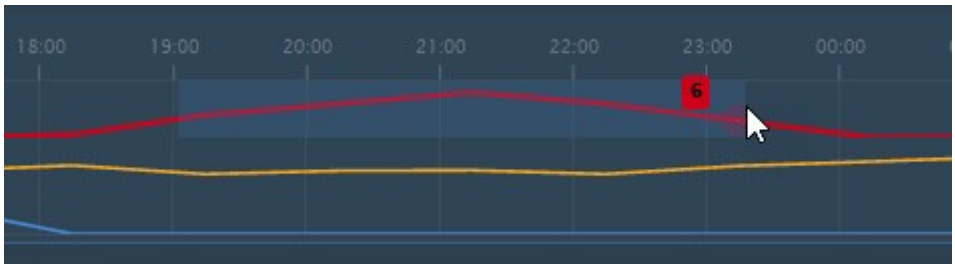


Рисунок 9. Выбор интервала на временной шкале

В списке будут отображены события за выбранный период.

Чтобы выполнить фильтрацию событий в пределах последней недели:

1. Выберите **Неделя** в нижней части временной шкалы.

   В списке будут отображены события за последние семь дней. Цена деления шкалы составит 12 часов.

2. Выделите интервал на временной шкале, удерживая левую кнопку мыши.

В списке будут отображены события за выбранный период.

Чтобы выполнить фильтрацию за определенные даты:

1. Нажмите в левой части экрана.
2. Выберите интервал в календаре или задайте его начало и конец в текстовых полях (см. рисунок 10).

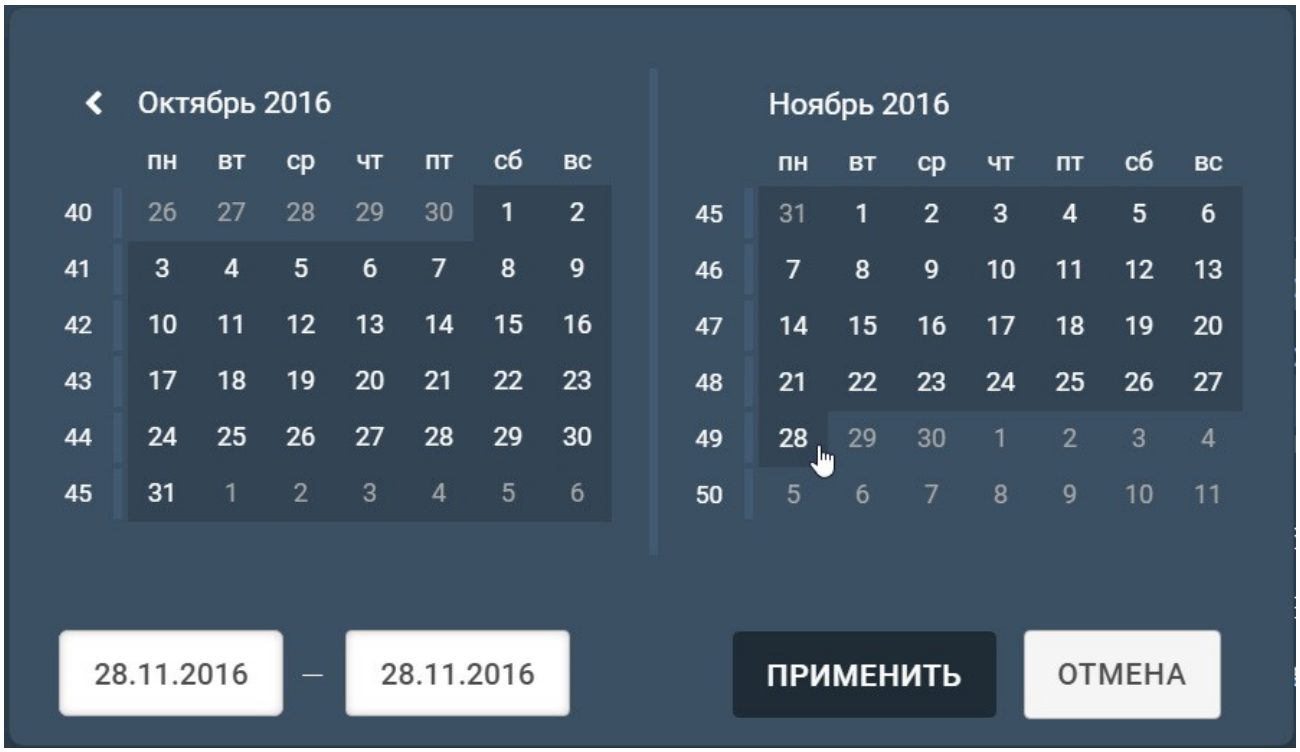


Рисунок 10. Выбор интервала на календаре

3. Нажмите кнопку **Применить**.

В списке будут отображены события за выбранные даты.

6.5. Обновление списка событий

Если во время работы на странице **События** PT ISIM обнаружил новые события, над списком появится кнопка **Загрузить новые события**.

Чтобы обновить список событий, нажмите кнопку **Загрузить новые события** над списком событий.

Если предварительно была применена фильтрация, появление кнопки и обновление списка происходят с учетом примененного фильтра.

7. Работа с инцидентами

Ниже приведена основная информация об инцидентах в PT ISIM, а также даны инструкции по работе с ними.

В этом разделе

7.1. Об инциденте

Инцидент — это событие или цепочка событий, результатом которой может стать нарушение целостности, конфиденциальности или доступности актива. PT ISIM обнаруживает инциденты на основе правил корреляции и моделирования системы.

Список инцидентов приводится на странице **Зафиксированные инциденты**. Для каждого инцидента в списке (см. рисунок 11) отображаются следующие атрибуты: уровень опасности, тип, IP-адрес источника, IP-адрес цели инцидента и время срабатывания правила корреляции.

Инцидент может быть открытым или закрытым. Открытые инциденты выделены в списке полужирным шрифтом, закрытые — зачеркнутым текстом. Вы можете менять статус инцидента по своему усмотрению в зависимости от последствий инцидента и принятых мер.

Рисунок 11. Список инцидентов

Уровень опасности инцидента может быть:

1. Средним — если инцидент имеет в составе хотя бы одно событие среднего уровня важности и ни одного события высокого уровня важности. Инцидент среднего уровня опасности обозначается желтым цветом.
2. Высоким — если инцидент имеет в составе хотя бы одно событие высокого уровня важности. Инцидент высокого уровня опасности обозначается красным цветом.

7.2. Просмотр подробной информации об инциденте

Чтобы просмотреть подробную информацию об инциденте, выберите инцидент в списке.

В нижней части страницы отобразится карточка инцидента (см. рисунок 12), содержащая следующую информацию:

- IP-адрес, MAC-адрес и тип сетевого узла источника инцидента;
- IP-адрес, MAC-адрес и тип сетевого узла цели инцидента;
- корреляция, с помощью которой был обнаружен инцидент;
- все события инцидента;
- описание прикладного смысла инцидента;
- описание возможных последствий инцидента.

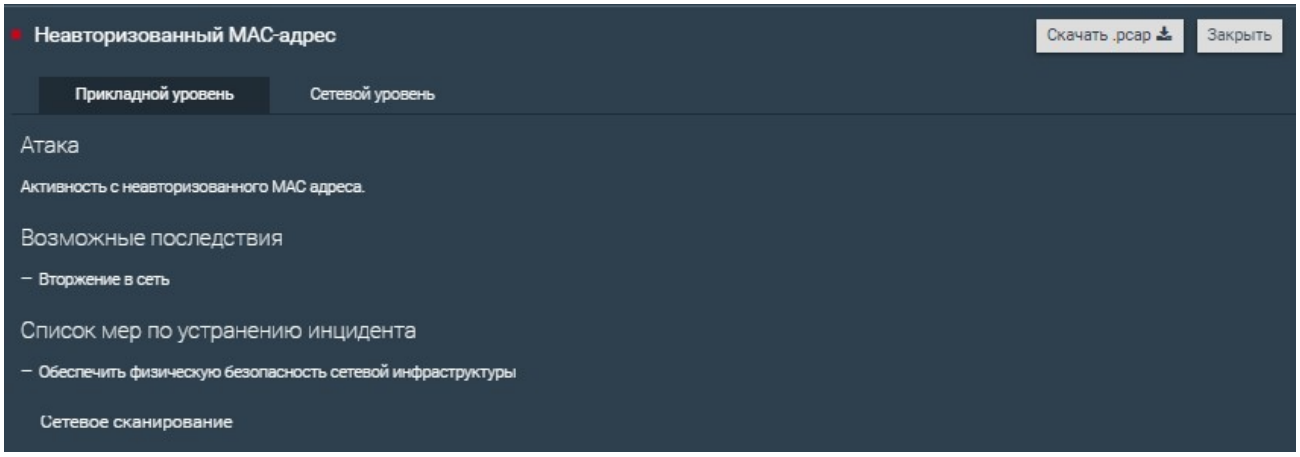


Рисунок 12. Карточка инцидента

7.3. Смена статуса инцидента

Чтобы закрыть открытый инцидент,

1. На странице **Зафиксированные инциденты** выберите необходимый инцидент.

   В нижней части окна откроется карточка выбранного инцидента.
2. Нажмите кнопку **Закрыть** в правой части карточки инцидента.

Статус инцидента сменится на закрытый, инцидент будет выделен зачеркнутым текстом и перенесен в конец списка инцидентов.

Чтобы открыть закрытый инцидент,

1. На странице **Зафиксированные инциденты** выберите необходимый закрытый инцидент (выделен зачеркнутым текстом).

   В нижней части окна откроется карточка выбранного инцидента.
2. Нажмите кнопку **Открыть** в правой части карточки инцидента.

Статус инцидента сменится на открытый, инцидент будет выделен обычным текстом.

8. Работа с топологией сети

Ниже приведена основная информация о топологии в PT ISIM, а также даны инструкции по работе с узлами сети.

В этом разделе

8.1. О топологии

Страница **Топология** представляет из себя карту вычислительной сети, состоящую из элементов (узлов) сети и связей между ними на сетевом уровне. Карта сети обновляется при изменении данных об узлах и соединениях.

Каждый узел может быть авторизованным или неавторизованным в зависимости от того, считаете ли вы взаимодействие с узлом разрешенным.

Красным цветом обозначаются узлы, которые имеют статус неавторизованный или хотя бы один открытый инцидент высокого уровня опасности. Если PT ISIM обнаруживает в сети новый узел, то считает его неавторизованным, при этом на странице **Зафиксированные инциденты** автоматически создается инцидент высокого уровня опасности.

Желтым цветом обозначаются узлы, которые имеют статус авторизованный и хотя бы один открытый инцидент среднего уровня опасности, но ни одного инцидента высокого уровня опасности.

Белым цветом обозначаются узлы, которые имеют статус авторизованный и не имеют ни одного открытого инцидента.

Узлы сети можно перемещать по карте для их более наглядного расположения.

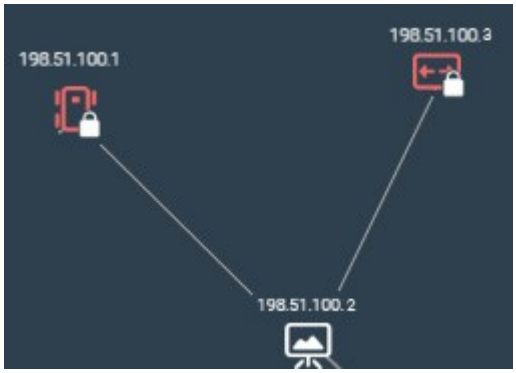


Рисунок 13. Страница Топология

Использование карты сети позволяет решать следующие задачи:

- Проверка состава сети. Карта сети наглядно отображает все узлы, входящие в сеть, и позволяет проверить, все ли необходимые элементы подключены к ней.
- Проверка связей между узлами. Возможны ситуации, когда определенные узлы сети не должны быть связаны друг с другом или же должны взаимодействовать только по определенному протоколу или порту. Карта позволяет увидеть лишние связи между ними, а также протоколы и порты, используемые для взаимодействия. Или наоборот, предполагается, что два узла должны взаимодействовать. В таком случае отсутствие связи между ними на карте может стать сигналом о необходимости перенастройки узлов.
- Контроль за соединениями с новыми узлами. Карта сети отображает новый узел и рассматривает первое соединение с таким узлом как инцидент высокого уровня опасности. Если соединение с данным узлом считается разрешенным, узлу присваивается статус авторизованный.
- Контроль за состоянием сети. Карта позволяет выявлять узлы сети, подверженные инцидентам, и связи с ними.

8.2. Просмотр информации об узле

Чтобы посмотреть информацию об узле сети, выберите узел на карте, выберите узел на карте.

Во всплывающем окне (см. рисунок 14) будет отображена следующая информация:

- **Название приложения** — имя, присваиваемое узлу для его идентификации;
- **IP** — IP-адрес узла;
- **MAC** — MAC-адрес узла;
- **тип** — тип узла (условные обозначения типов узлов приведены в приложении 1);
- **порты** — порты, по которым узел взаимодействует с другими узлами или взаимодействовал за последние 15 минут (если есть);
- **описание** — произвольное описание узла.

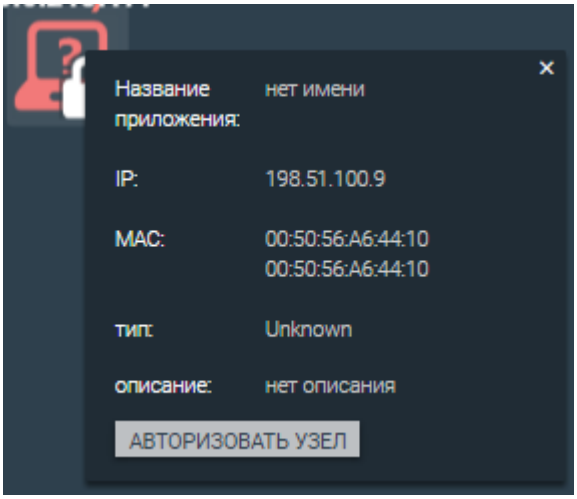


Рисунок 14. Подробная информация об узле

8.3. Просмотр информации о взаимодействии узлов

Чтобы посмотреть информацию о взаимодействии узлов, выберите соединяющую их линию.

Во всплывающем окне (см. рисунок 15) будет отображено количество событий, зафиксированных между двумя узлами, а также протоколы и порты, по которым происходит взаимодействие.

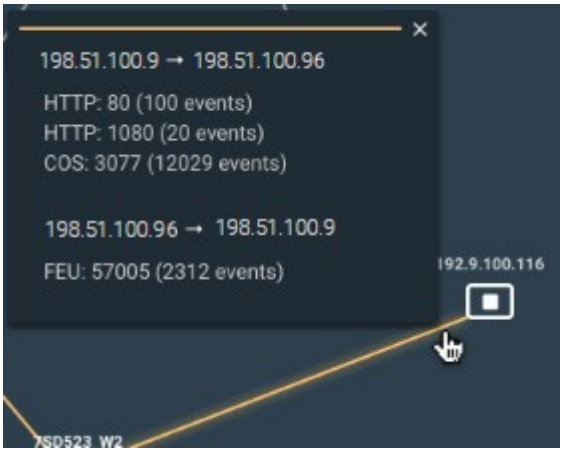


Рисунок 15. Подробная информация о взаимодействии узлов

8.4. Смена статуса узла

Чтобы изменить статус узла с авторизованный на неавторизованный, выберите узел и нажмите кнопку **Деавторизовать узел**.

Чтобы изменить статус узла с неавторизованный на авторизованный, выберите узел и нажмите кнопку **Авторизовать узел**.

9. Сохранение копии трафика в формате Pcap

PT ISIM позволяет сохранять копию перехваченного трафика в виде Pcap-файлов, например для их дальнейшего анализа сторонними программами.

Чтобы сохранить копию трафика, относящегося к событию:

1. Откройте страницу **События**.
2. В списке событий выберите событие.

   В нижней части страницы отобразится карточка события.
3. Нажмите **Скачать .pcap**.

Чтобы сохранить копию трафика за определенный период:

1. Откройте страницу **События**.
2. На временной шкале выделите период.

   На временной шкале появится кнопка **Скачать .pcap файл**
3. Нажмите **Скачать .pcap файл**.

Чтобы сохранить копию трафика, относящегося к инциденту:

1. На странице **События** нажмите .

   Откроется страница **Зафиксированные инциденты**.
2. В списке инцидентов выберите инцидент.

   В нижней части страницы отобразится карточка инцидента.
3. Нажмите **Скачать .pcap**.

10. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Заявки на портале являются основным каналом обработки обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

10.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать заявки на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов ЗАО "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

10.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 203 769 3606.

- США +1 857 208 7273.
- Италия +39 0 697631532.
- Швеция +46 8 121 111 86
- Южная Корея +82 264 108 582.
- Россия +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданной заявке.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте заявку на портале support.ptsecurity.com. Заявка на портале, созданная и обновляемая по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

10.3. Время работы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся заявкам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

10.4. Как служба технической поддержки работает с заявками

При получении вашей заявки специалист службы технической поддержки классифицирует инцидент, указанный в заявке (присваивает инциденту тип и уровень значимости) и выполняет дальнейшие шаги по разрешению инцидента.

В этом разделе

10.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста ЗАО "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

ЗАО "Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть заявку.

10.4.2. Типы инцидентов

Специалист технической поддержки относит инцидент в вашей заявке к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист ЗАО "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). ЗАО "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

ЗАО "Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт. ЗАО "Позитив Текнолоджиз" не несет ответственности за инциденты, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, ЗАО "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

10.4.3. Время реакции на обращение и приоритизация инцидентов

Время реакции на ваше обращение рассчитывается как время с момента получения от вас информации по обращению до ответа специалиста технической поддержки с описанием дальнейших шагов по разрешению инцидента. Время реакции зависит от указанного вами уровня значимости инцидента (см. таблицу ниже). Специалист технической поддержки может переопределять уровень значимости инцидента по приведенным ниже критериям. Значения сроков являются целевыми и подразумевают стремление и разумные усилия специалистов ЗАО "Позитив Текнолоджиз" для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 2. Время реакции технической поддержки на обращение

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 2 часов
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 4 часов
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительное влияние на бизнес	До 8 часов

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 16 часов

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки обращений).

10.4.4. Выполнение работ по заявке

По мере выполнения работ по вашей заявке специалист технической поддержки сообщает вам:

- о диагностике инцидента и ее результатах,
- поиске решения или возможности обойти причины возникновения инцидента,
- планировании и выпуске обновления продукта (если требуется для разрешения инцидента).

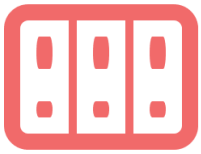
Если по итогам решения инцидента необходимо внести изменения в продукт, ЗАО "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по заявке считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- инцидент диагностирован как дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- инцидент идентифицирован как вызванный программными продуктами или оборудованием сторонних производителей и не подпадающий под гарантийные обязательства по продукту;
- инцидент классифицирован как неподдерживаемый.

11. Приложение А. Типы узлов

Таблица 3. Типы узлов

Изображение узла на странице Топология	Тип узла
	Неизвестный
	Автоматизированное рабочее место
	Операторская панель (HMI)
	Центральный процессор
	Концентратор связи
	IPU-шлюз связи с внешними системами
	Промышленный медиаконвертер
	Сервер SCADA

Изображение узла на странице Топология	Тип узла
	Релейная защита и автоматика
	Программируемый логический контроллер
	GPS-сервер времени
	Источник бесперебойного питания
	Сетевое устройство
	Датчик
	Коммутатор
	Модем
	Принтер

Изображение узла на странице Топология	Тип узла
	Рабочая станция
	База данных телеметрии
OPC	OPC-сервер
SPU	Оперативное процессорное устройство