1 Задачи

Программное обеспечение «Диагностическая станция ПТК АСУТП» – это решение, комплектуемое из программных модулей «ds-logger» и «ds-click», предназначенное для создания программно-технических комплексов обработки и передачи информации. Применение программного обеспечения «Диагностическая станция ПТК АСУТП» позволяет в полном объеме реализовать функцию загрузки шаблонов безопасности и диагностики в формате XML из интерфейса командной строки в ПАК «ИК.ДС», а также обработки и отправки сообщений из ПАК «ИК.ДС» в формате Syslog RFC3164/RFC5424.

2 Функциональные характеристики

Программное обеспечение «Диагностическая станция ПТК АСУТП» может быть интегрировано с различными системами управления событиями и информации о безопасности.

Принцип обработки данных:

– Модуль «ds-click» загружает шаблоны безопасности и диагностики в формате XML в ПАК «ИК.ДС».

– ПАК «ИК.ДС» формирует сообщения об инцидентах в режиме реального времени в соответствии с загруженными шаблонами.

– Нормализация данных: сформированные сообщения нормализуются и приводятся к единому формату.

– Модуль «ds-logger» отправляет нормализованные данные в формате Syslog RFC3164/RFC5424 произвольному получателю данных (SIEM или иной получатель).

3 Характеристики передачи данных

Тип и формат передаваемых данных соответствует спецификациям используемого протокола Syslog RFC3164/RFC5424.

Максимальный объем – 64к.

Формат сообщений прикладного уровня следующий:

`{ALERT.SENDTO}` – ip-адрес удаленного сервера syslog-dest;

`{ALERT.SUBJECT}` – глобальный тег ZBX;

`{ALERT.MESSAGE}` – тело сообщения следующего формата:

`ID:{EVENT.ID};` – уникальный ID события;

`{EVENT.TAGS};` – теги события;

`Time:{EVENT.DATE}{EVENT.TIME};` – метка времени возникновения события в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС;

`IP:{HOST.IP};` – ip-адрес узла, на котором возникло событие;

`Host:{HOST.NAME};` – символьное имя узла, на котором возникло событие;

`Problem:{EVENT.NAME};` – событие (имя проблемы);

`Severity:{TRIGGER.SEVERITY};` – важность события.