

Стенд «Безопасная цифровая подстанция»

В городе Чебоксары в период с 23 по 26 апреля состоялась V Международная научно-практическая конференция «Релейная защита и автоматизация электроэнергетических систем России» и выставка «РЕЛАВЭКСПО-2019». Компания iGrids, как организатор и спонсор форума, уделила огромное внимание вопросам кибербезопасности в наглядной форме стендовых моделей, а также доступных материалов для проектировщиков, заказчиков и производителей.



Совместно с партнерами ООО «ИнфоТеКС» и АО «Лаборатория Касперского» для стенда электротехнического кластера ЧР «ИнТЭК» компания iGrids реализовала **модель «Безопасной цифровой подстанции»**.

На данной модели было продемонстрировано совместное применение актуальных решений в области ЦПС участников электротехнического кластера и Системы информационной безопасности. Представленная Система информационной безопасности состояла из решений Kaspersky Industrial CyberSecurity - специального промышленного антивируса и системы обнаружения вторжений (СОВ), и решений «ИнфоТеКС» для организации беспроводных крипто защищенных каналов связи – ПАК ViPNet.



iGrids

+7 (831) 280-97-89

info@igrids.ru

igrids.ru

На рисунке 1 представлена главная схема стэнда цифровой подстанции. На линии W4 и на трансформаторе T1 присутствует по комплекту защит от каждого производителя устройств РЗА, входящих в электротехнический кластер Чувашской Республики.

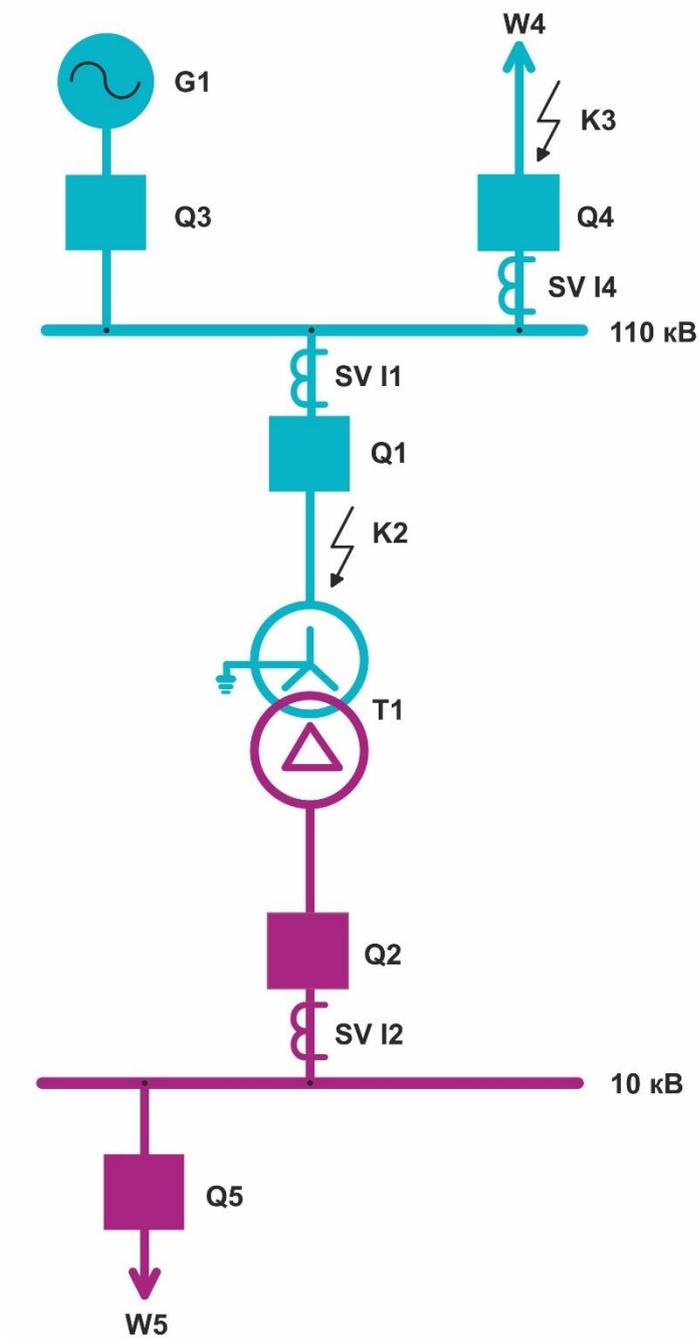


Рисунок 1 – Главная схема стэнда «Безопасная цифровая подстанция»

Состав комплекта ступенчатых защит (КСЗ):

- МП РЗА БЕ2704 производства ООО НПП «ЭКРА»;
- МП РЗА TOP 300 производства ООО «Релематика»;
- МП РЗА БЭМП производства АО «ЧЭАЗ»;
- МП РЗА Бреслер-0107 производства ООО «НПП Бреслер».



iGrids

+7 (831) 280-97-89
info@igrids.ru
igrids.ru

Состав комплекта дифференциальной защиты трансформатора (ДЗТ):

- МП РЗА ТОР 300 производства ООО «Релематика»;
- МП РЗА БЕ2704 производства ООО НПП «ЭКРА»;
- МП РЗА Бреслер-0107 производства ООО «НПП Бреслер»;
- МП РЗА БЭМП производства АО «ЧЭАЗ».



iGrids

+7 (831) 280-97-89

info@igrids.ru

igrids.ru

На рисунке 2 представлена схема информационного обмена, которая включает шину процесса, шину станции, оборудование РЗА, а также систему информационной безопасности.

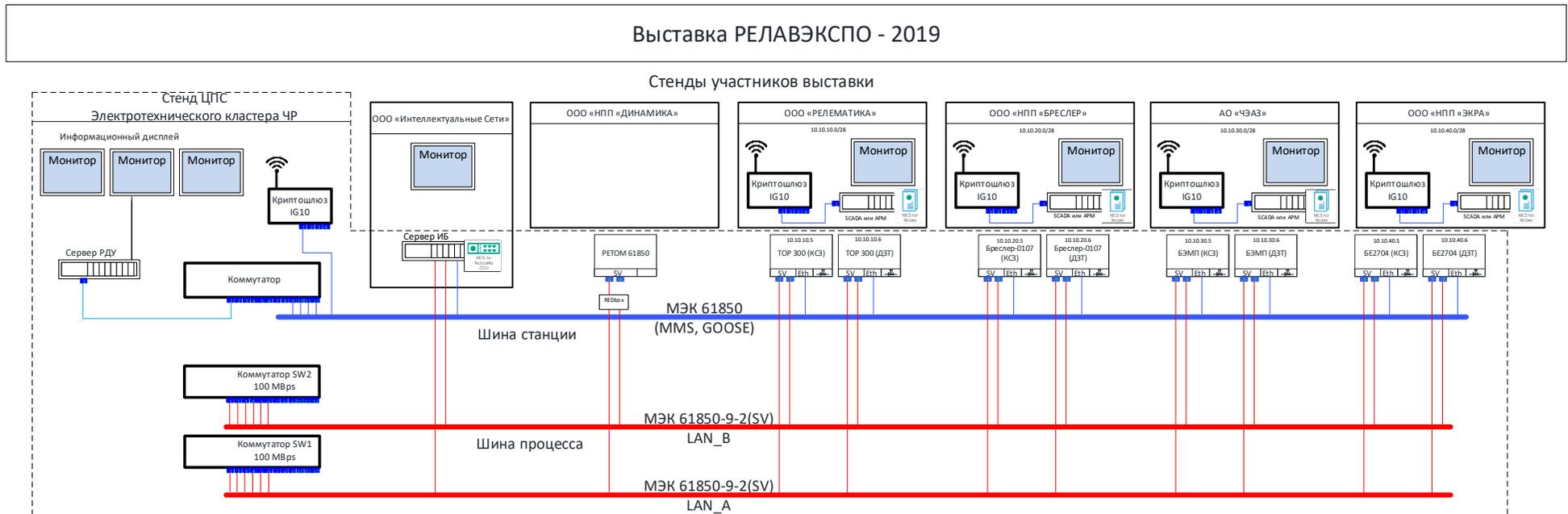


Рисунок 2 - Схема информационного обмена

Шина процесса представляет собой две независимые параллельные сети LAN A и LAN B, работающие по протоколу параллельного резервирования (PRP). Устройства, входящие в состав комплекта защит КСЗ и ДЗТ, поддерживают протокол PRP и подключаются в шину процесса напрямую. Устройства, не поддерживающие протокол PRP (например, РЕТОМ-61850), подключаются через специальное устройство Redundancy Box (RedBox).

Генерация потока измерений по протоколу МЭК 61850-9-2 выполняется при помощи устройства РЕТОМ-61850 производства НПП «Динамика». РЕТОМ-61850 работает в трех режимах:

1. Нормальный режим. В этом режиме РЕТОМ-61850 выдает номинальные значения тока и напряжения. Устройства РЗА принимают поток измерений (SV) по шине процесса и через шину станции выдают значения измерений на свой отдельный сервер SCADA, расположенный на стенде производителя.

2. Режим срабатывания КСЗ. При замыкании первого дискретного входа РЕТОМ-61850 происходит воспроизведение Comtrade-файла аварийного режима (K3 на рисунке 1), при котором происходит срабатывание устройств РЗА, расположенных на линии W4. Устройства РЗА передают сигнал о срабатывании в сервер SCADA, расположенный на стенде производителя, после чего сигнал от каждого сервера SCADA передается в сервер РДУ, который фиксирует срабатывание устройства РЗА каждого производителя. Индикация срабатывания защит КСЗ показана на рисунке 4 (сигнал «Срабатывание КСЗ»).

3. Режим срабатывания ДЗТ. При замыкании второго дискретного входа РЕТОМ-61850 происходит воспроизведение Comtrade-файла аварийного режима (K2 на рисунке 1), при котором происходит срабатывание устройств РЗА, расположенных на трансформаторе Т1. Устройства РЗА передают сигнал о срабатывании в сервер SCADA, расположенный на стенде производителя, после чего сигнал от каждого сервера SCADA передается в сервер РДУ, который фиксирует срабатывание устройства РЗА каждого производителя. Индикация срабатывания защит ДЗТ показана на рисунке 4 (сигнал «Срабатывание ДЗТ»).

В нормальном режиме устройства РЗА 1 (КСЗ) и РЗА 2 (ДЗТ) каждого производителя передают измерения токов и напряжений по шине станции по протоколу МЭК 61850 (MMS) в сервер SCADA, расположенный на стенде производителя устройств РЗА (рисунок 3). Связь с сервером SCADA осуществляется по защищённому (шифрование данных по ГОСТ) беспроводному (GSM /Wi-Fi) каналу связи.

При срабатывании КСЗ/ДЗТ происходит передача сигнала о срабатывании по защищённому беспроводному каналу в сервера SCADA, сигналы о срабатывании защит от серверов SCADA передаются в сервер РДУ, который фиксирует срабатывание защит КСЗ/ДЗТ от каждого производителя (рисунок 4).

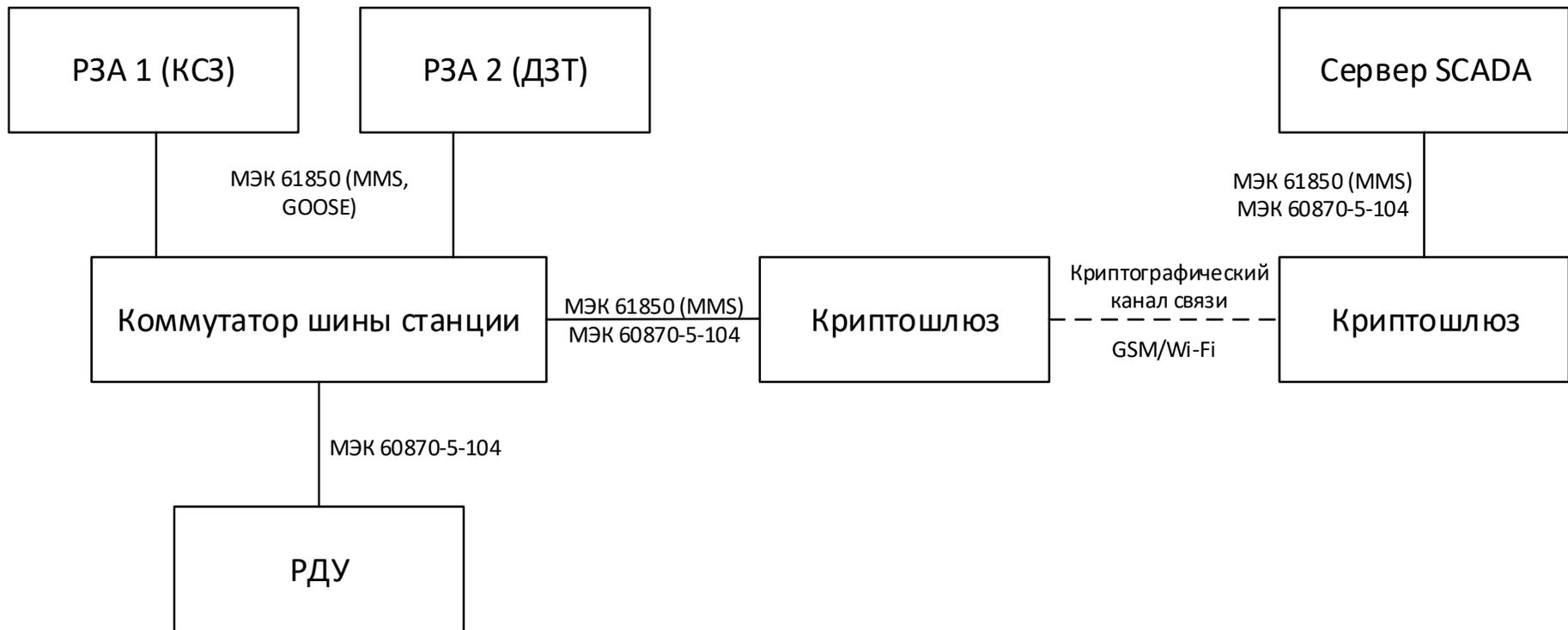
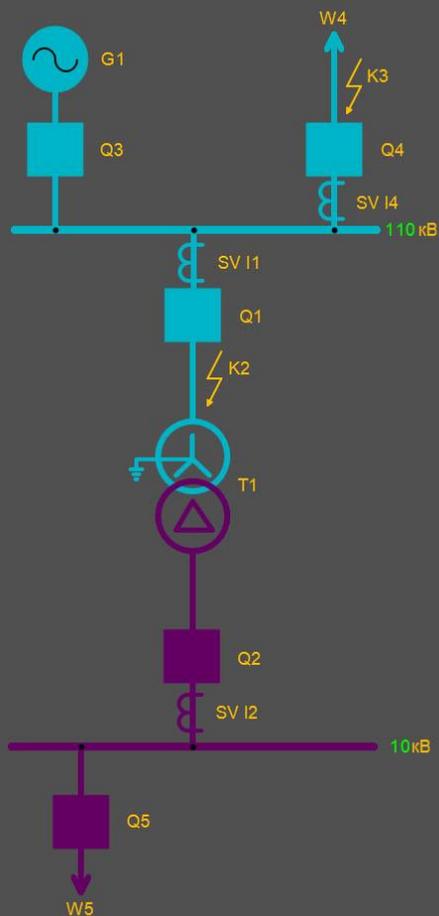


Рисунок 3 – Упрощенная схема информационного обмена



ООО НПП «ЭКРА»



Срабатывание
ДЗТ



Срабатывание
КСЗ

ООО «Релематика»



Срабатывание
ДЗТ



Срабатывание
КСЗ

АО «ЧЭАЗ»



Срабатывание
ДЗТ



Срабатывание
КСЗ

ООО «НПП Бреслер»



Срабатывание
ДЗТ



Срабатывание
КСЗ

Рисунок 4 – Мнемосхема 1 на мониторе РДУ

Система информационной безопасности

Система информационной безопасности стенда ЦПС состоит из программно-технических решений:

- Kaspersky Industrial CyberSecurity for Networks;
- Kaspersky Industrial CyberSecurity for Nodes;
- Программно-аппаратного комплекса ViPNet.

Kaspersky Industrial CyberSecurity for Networks (KICS for Networks) – программа для защиты инфраструктуры промышленных предприятий от угроз информационной безопасности и для обеспечения непрерывности технологических процессов.

KICS for Networks анализирует трафик промышленной сети для обнаружения неизвестных программе узлов промышленной сети, неразрешенных системных команд, посылаемых на интеллектуальные электронные устройства, а также попыток установки недопустимых значений параметров технологического процесса.

Программа входит в состав решения Kaspersky Industrial CyberSecurity. KICS for Networks выполняет следующие функции:

- Проверяет взаимодействия между узлами промышленной сети на соответствие заданным правилам.
- Обнаруживает сетевые пакеты, отправленные с ранее неизвестных программе узлов промышленной сети. Обнаружение сетевых пакетов позволяет своевременно получать информацию об аномалиях в промышленной сети (например, о несанкционированном подключении нового устройства к промышленной сети).
- Извлекает из сетевых пакетов значения параметров технологического процесса, управляемого автоматизированной системой управления технологическим процессом, и проверяет допустимость этих значений.
- Анализирует трафик промышленной сети на наличие в сетевых пакетах системных команд, посылаемых на интеллектуальные электронные устройства для автоматизации технологического процесса на предприятии (далее «устройства»). Обнаруживает в трафике системные команды и ситуации, которые могут быть признаками нарушения безопасности промышленной сети.
- Анализирует трафик промышленной сети на наличие признаков атак, не оказывая влияния на промышленную сеть и не привлекая внимания потенциального нарушителя. Обнаруживает признаки атак с помощью заданных правил и встроенных алгоритмов проверки сетевых пакетов.
- Регистрирует события и передает сведения о них в сторонние системы, а также в Kaspersky Security Center.
- Предоставляет возможности управления работой программы и просмотра сведений через графический интерфейс пользователя. Обеспечивает удаленный доступ для подключения с использованием веб-интерфейса и интерфейса прикладного программирования.



**Kaspersky
Industrial CyberSecurity**
for Networks 2.8 Beta 2

- Мониторинг
- Устройства
- События
- Теги
- О программе

Начать обучение

kics

Устройства Добавить новое устройство

Таблица

40%

Карта сети

Статусы устройств
[Все статусы ^](#)

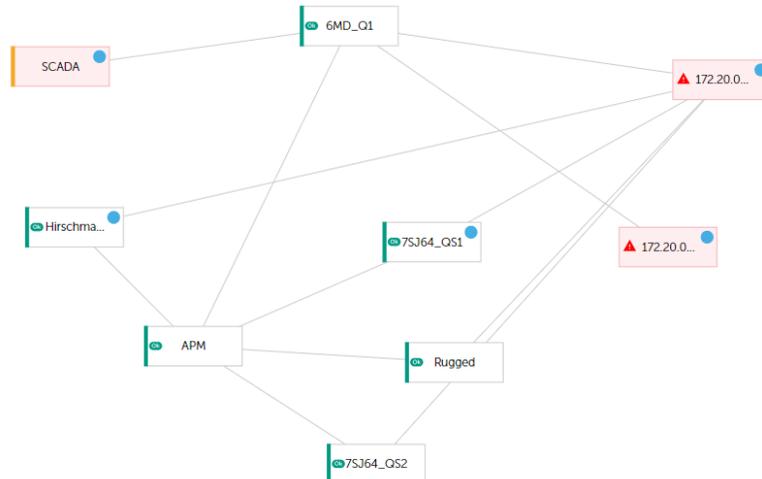
Важность соединений
[Все уровни важности ^](#)

Протоколы
[Все протоколы ^](#)

Состояния устройств
[Все состояния ^](#)

Категории устройств
[Все категории ^](#)

Уровни модели OSI
[Все уровни ^](#)



04.04.19 10:24

Час



Сейчас

Рисунок 5 - Интерфейс KICS for Networks

Kaspersky Industrial CyberSecurity for Nodes (KICS for Nodes) – это средство комплексной защиты серверов и рабочих станций в промышленных системах управления от информационных угроз. Программа контролирует работу компьютеров индустриальной сети предприятия с помощью следующих компонентов, функций и технологий:

- Контроль запуска программ. Компонент отслеживает попытки запуска программ пользователями и регулирует запуск программ.

- Контроль устройств. Компонент позволяет контролировать регистрацию и использование запоминающих устройств и устройств чтения CD/DVD-дисков в целях защиты компьютера от угроз безопасности, которые могут возникнуть во время файлового обмена с подключаемым по USB флеш-накопителем или внешним устройством другого типа.

- Проверка целостности проектов ПЛК. Функция предназначена для проверки целостности проектов программируемых логических контроллеров (ПЛК), используемых в индустриальной сети.

Каждый тип угроз обрабатывается отдельным компонентом. Можно включать и выключать компоненты независимо друг от друга, а также настраивать параметры их работы. Программа проверяет и защищает компьютеры индустриальной сети с помощью следующих компонентов:

- Файловый Антивирус. Компонент позволяет избежать заражения файловой системы компьютера. Компонент запускается при старте KICS for Nodes, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые файлы на компьютере и на всех присоединенных дисках. Файловый Антивирус перехватывает каждое обращение к файлу и проверяет этот файл на присутствие вирусов и других программ, представляющих угрозу.

- Контроль Wi-Fi. Компонент отслеживает попытки подключения защищаемого компьютера к сетям Wi-Fi и блокирует или разрешает подключения к обнаруженным сетям.

- Управление сетевым экраном. Компонент обеспечивает управление брандмауэром Windows: он позволяет настраивать сетевой экран операционной системы, управлять политиками и блокировать любые возможности настройки брандмауэра извне.

- Защита от шифрования. Компонент позволяет обнаруживать активность вредоносного шифрования сетевых файловых ресурсов защищаемого компьютера со стороны удаленных компьютеров корпоративной сети.

- Мониторинг файловых операций. KICS for Nodes обнаруживает изменения в файлах из области мониторинга, указанной в параметрах задачи. Эти изменения указывают на нарушение безопасности на защищаемом компьютере.

- Анализ журналов. Компонент выполняет контроль целостности защищаемой среды на основе результатов анализа журналов событий Windows.

Передача информации о статусе защищенности узлов индустриальной сети от Kaspersky Security Center в SCADA-систему осуществляется посредством службы Kaspersky Security Gateway.

Эта информация выводится на экраны SCADA-системы, что позволяет оператору SCADA-системы оперативно реагировать на проблемы в защите индустриальной сети.

Kaspersky Security Gateway позволяет управлять следующими коммуникационными службами:

- IEC 60870-5-104. Унифицированный открытый протокол для систем автоматизации.
- OPC 2.0 DA. Спецификация для взаимодействия устройств в промышленных сетях.

Коммуникационные службы могут управляться как с помощью графического интерфейса Kaspersky Security Gateway, так и с помощью стандартных средств Microsoft Windows.

Kaspersky Security Gateway передает в SCADA-систему следующую информацию:

- Статус доступности Сервера администрирования Kaspersky Security Center:
 - 1. Означает, что подключение Kaspersky Security Gateway к Серверу администрирования Kaspersky Security Center выполнено успешно.
 - 0. Означает, что подключение Kaspersky Security Gateway к Серверу администрирования Kaspersky Security Center не может быть выполнено.
 - 2. Означает, что KICS for Nodes не активирован или срок действия лицензии истек, и подключение Kaspersky Security Gateway к Серверу администрирования Kaspersky Security Center не может быть выполнено.
- Статус доступности всех защищаемых узлов сети:
 - 0. Означает, что, по крайней мере, один узел сети, находящийся под управлением Сервера администрирования Kaspersky Security Center и выбранный для мониторинга в параметрах Kaspersky Security Gateway, недоступен в момент вычисления статуса.
 - 1. Означает, что все узлы сети, находящиеся под управлением Сервера администрирования Kaspersky Security Center и выбранные для мониторинга в параметрах Kaspersky Security Gateway, доступны в момент вычисления статуса.
- Статус защищенности каждого узла сети в Kaspersky Security Center:
 - 0. Означает, что на узле сети, находящемся под управлением Сервера администрирования Kaspersky Security Center и выбранном для мониторинга в параметрах Kaspersky Security Gateway, нет критических или требующих обработки инцидентов.
 - 1. Означает, что на узле сети, находящемся под управлением Сервера администрирования Kaspersky Security Center и

выбранном для мониторинга в параметрах Kaspersky Security Gateway, произошел хотя бы один критический инцидент.

- 2. Означает, что на узле сети, находящемся под управлением Сервера администрирования Kaspersky Security Center и выбранном для мониторинга в параметрах Kaspersky Security Gateway, произошел хотя бы один инцидент, требующий обработки.

Статусы определяются в соответствии с параметрами Kaspersky Security Center для управляемых компьютеров / групп администрирования.

Программа передает информацию о статусах только тех узлов сети, которые выбраны для отображения в SCADA-системе в параметрах Kaspersky Security Gateway.

– Статус защищенности сети:

- 0. Означает, что все узлы сети имеют статус 0 в Kaspersky Security Center.
- 1. Означает, что хотя бы один узел сети имеет статус 1 в Kaspersky Security Center.
- 2. Означает, что хотя бы один компьютер в сети имеет статус 2 в Kaspersky Security Center.

На рисунке 6 показана мнемосхема РДУ с информацией, приходящей от Kaspersky Security Gateway.



Узлы доступны	<input type="radio"/>
Сервер КСЗ доступен	<input type="radio"/>
Защищенность узлов	<input type="radio"/>



Серверы SCADA	
ООО НПП «ЭКРА»	<input type="radio"/>
ООО «Релематика»	<input type="radio"/>
АО «ЧЭАЗ»	<input type="radio"/>
ООО «НПП Бреслер»	<input type="radio"/>

- — Нормальный режим работы
- — Предупреждение
- — Критический инцидент

ООО НПП «ЭКРА»



Срабатывание
ДЗТ



Срабатывание
КСЗ

ООО «Релематика»



Срабатывание
ДЗТ



Срабатывание
КСЗ

АО «ЧЭАЗ»



Срабатывание
ДЗТ



Срабатывание
КСЗ

ООО «НПП Бреслер»



Срабатывание
ДЗТ



Срабатывание
КСЗ

Рисунок 6 - Мнемосхема 2 на мониторе РДУ

ПАК ViPNet

Программно-аппаратный комплекс (ПАК) ViPNet Coordinator IG10 – сетевой шлюз безопасности в промышленном исполнении, предназначенный для защиты каналов связи в промышленных системах и сегментирования их на защищенные объекты. ViPNet Coordinator IG предназначен для обеспечения эффективной защиты от сетевых атак и несанкционированного доступа к информации путем создания защищенных каналов связи до 10 Мбит/с на основе технологии ViPNet и фильтрации IP-трафика в соответствии с установленными правилами.

Благодаря поддержке каналов Ethernet, 3G, Wi-Fi, RS-232/RS485 ViPNet Coordinator IG10 позволяет реализовать большое количество сценариев, в том числе удовлетворяющих требованиям серии стандартов ГОСТ Р МЭК 62443. ПАК ViPNet Coordinator IG10 имеет безвентиляторный дизайн и крепление на DIN-рейку.



Рисунок 7 - ПАК ViPNet