Кибербезопасность электроэнергетической инфраструктуры

kaspersky

www.kaspersky.ru

Оглавление

Кибербезопасность электроэнергетической инфраструктуры

Современная энергетическая система — сложнейший технический объект, уникальный по своим масштабам и своей значимости для обеспечения человеческой жизнедеятельности. Ввиду физических особенностей электроэнергии и скоротечности электрических процессов управление работой и безопасная эксплуатация такого объекта является сложной организационно-технической задачей. По этой причине устройства, предназначенные для защиты электроэнергетического оборудования от аварийных режимов работы, а также для автоматизации процессов управления появились практически одновременно с началом промышленного использования электроэнергии. Требования, предъявляемые к ним, их конструкция и функциональные возможности усложнялись и развивались вместе с энергосистемой в ответ на растущие запросы потребителей и эксплуатации

Сегодня автоматические и автоматизированные системы защиты и управления (АСЗУ) — это сложный, взаимосвязанный информационный комплекс, охватывающий все грани эксплуатации объектов электроэнергетики и являющийся неотъемлемой частью электроэнергетической инфраструктуры. Бурное развитие вычислительной техники и коммуникационных технологий, их проникновение во все области техники, в том числе и в сферу автоматизации объектов электроэнергетики, привело к изменению не только технических средств систем защиты управления компонентами энергосистемы, но и к изменению принципов построения электросетевого комплекса с учетом новых возможностей по управляемости и наблюдаемости.

Именно задача повышения качества управления является одной из основных при обсуждении вопросов перспективного развития электроэнергетики и перехода в будущем к интеллектуальной энергосистеме с активно-адаптивной сетью (ИЭС ААС). Таким образом, роль управляющих систем в процессе производства, транспортировки и распределения электроэнергии, обеспечения безопасной эксплуатации и бесперебойного снабжения потребителей в настоящий момент времени является ключевой и в дальнейшем эта роль будет только возрастать.

В настоящее время вычислительные системы АСЗУ имеют высокую степень интегрированности и широко используют цифровые коммуникации на основе открытых международных стандартов, таких как МЭК 60870, МЭК 61850, МЭК 61970. Повышение связанности и информированности отдельных подсистем дало возможность существенно увеличить возможности систем защиты и управления, сделать их более интеллектуальными и эффективными в использовании, а использование стандартизованных подходов и средств позволило значительно снизить стоимость интеграции и обеспечить более высокую степень функциональной надежности.

Современный комплекс защиты и управления энергообъектом объединяет практически все виды технологических информационных подсистем, такие как например:

- Программно-аппаратные комплексы автоматизированного диспетчерского управления
- Автоматика регулирования и поддержания режимов работы энергосистемы
- Системы релейной защиты и автоматики.
- Системы противоаварийного автоматического управления
- Автоматизированные системы управления технологическим процессом
- Автоматизированные системы учета электроэнергии
- Системы контроля качества электроэнергии
- САУ управляемого силового оборудования
- Вспомогательные информационные системы

Уязвимость АСЗУ объектов электроэнергетики перед угрозами информационной безопасности

Высокий уровень открытости и интегрированности систем электроэнергетики наряду с широким развитием и проникновением информационных и интернет технологий во все сферы жизни человечества привели к появлению новых вызовов для отрасли. Автоматизированные системы защиты и управления объектов электроэнергетики нашего времени представляют собой интегрированную распределенную вычислительную систему, коммуницирующую по открытым, хорошо документированным протоколам, которые были разработаны прежде всего с фокусом на обеспечение функциональных технологических преимуществ и удобство эксплуатации. Вопросам обеспечения информационной безопасности таких систем не уделялось большого внимания в связи с низким приоритетом этого вопроса и ожидаемой неясностью внутреннего устройства АСЗУ для непосвящённых.

Такой подход был частично оправдан, когда системы управления электроснабжением строились как локальные аналоговые подсистемы на основе релейной логики или, позднее, как изолированные решения с использованием закрытых протоколов. Для нынешних открытых, глобально интегрированных и взаимосвязанных, в том числе и с нетехнологическими корпоративными сервисами, систем такой подход является опрометчивым и недальновидным.

Стандарт МЭК 62351 «Управление электроэнергетическими системами и сопутствующий информационный обмен. Безопасность данных и коммуникаций» выделяет следующие проблемы информационной безопасности на объектах электроэнергетики и их причины:

Открытые коммуникации

Открытые и незащищённые каналы связи между компонентами систем защиты и управления, а также между объектами силовой инфраструктуры:

- **Отсутствие проверки подлинности**
  Слабая или отсутствующая аутентификация взаимодействующих агентов. В результате, например, команда управления может быть отдана произвольным устройством, находящимся в технологической сети, устройство телемеханики может быть подменено, а система верхнего уровня может получить подложную информацию, провоцируя диспетчера на неверные действия.

- **Открытые стандарты и открытая передача данных**
  Используемые протоколы передачи данных построены на базе открытых для изучения стандартов и подробно и качественно документированы. В открытом доступе присутствуют средства анализа и эмуляции, а также свободные реализации данных протоков в виде исходных кодов. Данное обстоятельство значительно облегчает задачу злоумышленнику. Данные передаются открыто и доступны для прослушивания, повторения и искажения.

- **Высокая детализация сетевых коммуникаций**
  Особенности реализации протоколов МЭК 60807-5-10x и МЭК 61850 MMS позволяют легко выводить из строя устройства АСЗУ (например, SCADA диспетчерского центра или терминал РЗА) путем массированной бомбардировки неверными пакетами данных.

- **Связь с открытыми сетями**
  Корпоративная и технологическая сети современного объекта имеют множество пересечений почти на всех уровнях иерархии управления, что повышает риск внешнего неавторизованного доступа к оборудованию АСЗУ.

Отсутствие у обслуживающего персонала знаний в области ИБ

Ограниченное число специалистов обслуживает довольно большой парк устройств, зачастую распределенный по значительной территории на объектах, не имеющих постоянного персонала. Причем у данного персонала, зачастую, отсутствуют даже элементарные знания в области информационной безопасности:

- **Привилегированный удаленный доступ из недоверенной сети**
  В целях повышения удобства обслуживания организуются каналы удаленного доступа, позволяющие получить полный привилегированный доступ к оборудованию удаленного объекта. Зачастую такой доступ не является частью какого-либо проекта и организуется стихийно небезопасным способом, например, с корпоративных АРМ, имеющих выход в интернет.

- **Отсутствие политик парольной защиты и управления пользователями**
  Большое количество устройств, обслуживаемое ограниченным количеством персонала, затрудняет управление политиками доступа к устройствам, включая парольные политики и политики управления пользователями. Поэтому устройства годами эксплуатируются с паролями по умолчанию, что существенно облегчает неавторизованный доступ.

- **Устаревшее ПО**
  Программное обеспечение вычислительных средств, используемых в составе АСЗУ, практически не обновляется в течение срока службы. Выявленные ошибки ПО не устраняются, кроме случаев, когда эти ошибки непосредственно влияют на технологический процесс.

- **Обслуживание с небезопасных рабочих станций**
  В процессе обслуживания используются переносные АРМ (ноутбуки), которые в то же время используются как корпоративные рабочие станции, а также как «испытательные лаборатории» для ПО и просто для личных целей.

- **Отсутствие регулярного контроля конфигураций и ПО**
  Верификация конфигураций и программного обеспечения устройств производится вручную и крайне редко (не чаще раза в год).

Отсутствие следования требованиям ИБ при проектировании решений

Устройства, программное обеспечение и системы на их основе разрабатываются и создаются без учета проблематики информационной безопасности.

- **Слабая устойчивость к взлому**
  Слабая устойчивость к информационному взлому устройств АСЗУ, так как разработчики просто не учитывают возможность целенаправленного неправомерного воздействия на устройство.

- **Некорректные или недостаточные настройки безопасности ЛВС**
  Некорректные настройки технологической локальной вычислительной сети. Например, выполнение сегментации сети и управление доступом между сегментами ЛВС. Системной проблемой является отсутствие в проектах на создание АСЗУ конкретных решений по организации ЛВС. Поэтому качество исполнения работ по настройке устройств ЛВС зависит от квалификации персонала наладочной организации.

- **Отсутствие защиты данных, передаваемых по открытым каналам**
  Отсутствие средств защиты трафика, предаваемого по открытым каналам связи.

- **Отсутствие ролевого разграничения прав доступа**
  Некорректное разграничение прав доступа персонала к устройствам, допускающее доступ не в соответствии с должностными обязанностями.

- **Отсутствие решений по контролю запуска приложений**
  Отсутствие проектных решений по обеспечению защиты вычислительных средств с загружаемым ПО от несанкционированного запуска программ. Применяемые вне проекта средства, зачатую являются малоэффективными (несовместимость с технологическим ПО, недостаточность ресурсов ВС для совместной работы и др.)

- **Отсутствие или недостаточность средств регистрации событий ИБ**
  В составе систем управления отсутствуют или являются недостаточно функциональными специализированные средства мониторинга и регистрации событий информационной безопасности, позволяющие верно интерпретировать картину произошедшего.

Сложности разграничения и управления доступом подрядных организаций

Распространённой практикой является проведение отдельных видов обслуживания силами подрядных организаций. В связи с этим вопрос обеспечения временного доступа к ограниченному количеству оборудования без возможности влияния на остальные части системы, а также отмены такого доступа по окончании работ является крайне актуальным.

В силу вышеизложенного, очевидно, существует системная проблема, заключающаяся в следующем:

- Современные системы защиты и управления оборудованием энергосистемы не являются ни изолированными от внешнего мира, ни системами с закрытой реализацией.
- АСЗУ не имеют достаточных встроенных средств обеспечения информационной безопасности.
- Обнаружение нелегитимного информационного воздействия, активного или прошедшего, при текущем состоянии дел организационно и технически крайне затруднительно.
- В случае если такое воздействие удалось обнаружить, неясно, как на него реагировать и какие меры принимать.

Продолжительный срок службы уязвимых компонентов

Срок службы устройств и систем защиты и управления длительный — 20-30 лет. Таким образом, продолжающие внедряться в настоящее время небезопасные системы будут заменены только через несколько десятков лет. Поэтапная частичная модернизация является крайне затруднительной, так как защищенные решения (например, использующие шифрование) несовместимы с обычными, уязвимыми решениями.

Кроме вышеперечисленных технических вопросов, важной проблемой является отсутствие регламентов по действиям в случае обнаружения подозрительной активности в информационном поле автоматизированной системы, а также нормативной документации и практики по расследованиям технологических нарушений с учетом потенциальной возможности внешнего преднамеренного деструктивного воздействия в информационной плоскости. Например, РД 34.35.516-89 «Инструкция по учету и оценке работы релейной защиты и автоматики электрической части энергосистем», которая до сих пор является одним из основных руководящих документов при расследовании и классификации технологических нарушений в части оценки работы системы РЗА, даже не предусматривает (в силу своего возраста) варианта неправильного срабатывания по причине инцидента информационной безопасности. Поэтому, даже если такой случай имел место, реальные причины произошедшего не будут выяснены. Соответственно, не будут приняты адекватные меры, и инцидент может повториться снова.

Таким образом, одним из важнейших компонентов автоматизированной системы защиты и управления в части обнаружения неправомерной информационной активности, а также при расследовании технологических нарушений всех видов является независимый доверенный сетевой монитор, регистрирующий все виды сетевой активности в технологическом сегменте, а также обладающий повышенной устойчивостью к целенаправленным попыткам повреждения, искажения и уничтожения содержащейся в нем информации.

Технические решения по предотвращению, обнаружению и смягчению последствий реализации угроз информационной безопасности

Стандарт МЭК 62351 «Управление электроэнергетическими системами и сопутствующий информационный обмен. Безопасность данных и коммуникаций» детально описывает возможные средства обеспечения комплексной информационной безопасности на объектах электроэнергетики. Однако большинство из предложенных решений могут быть реализованы только при полной замене устройств автоматизации, поскольку требуют внесения изменений в форматы и процедуры коммуникационных протоколов.

Несмотря на то, что полное применение стандарта МЭК 62351 в этой связи выглядит как отдалённая перспектива, часть требований можно выполнить применительно и к современным системам.

К техническим средствам, реализующим данные требования, относится решение Kaspersky Industrial CyberSecurity (KICS), предлагаемое «Лабораторией Касперского».

Решение состоит из двух компонентов:

- KICS for Nodes — компонент защиты конечных узлов технологической ЛВС с загружаемым ПО (инженерные станции, станции операторов и т.п.)
- KICS for Networks — компонент мониторинга и регистрации событий сетевого обмена с возможностью глубокого анализа прикладных протоколов МЭК 60870-5-104, МЭК 61850 и пр.

KICS for Nodes

KICS for Nodes – специализированный продукт для промышленных систем. Он представляет собой программное обеспечение, созданное для защиты серверов АСУ ТП, а также операторских панелей и рабочих станций инженеров и операторов под управлением ОС Windows.

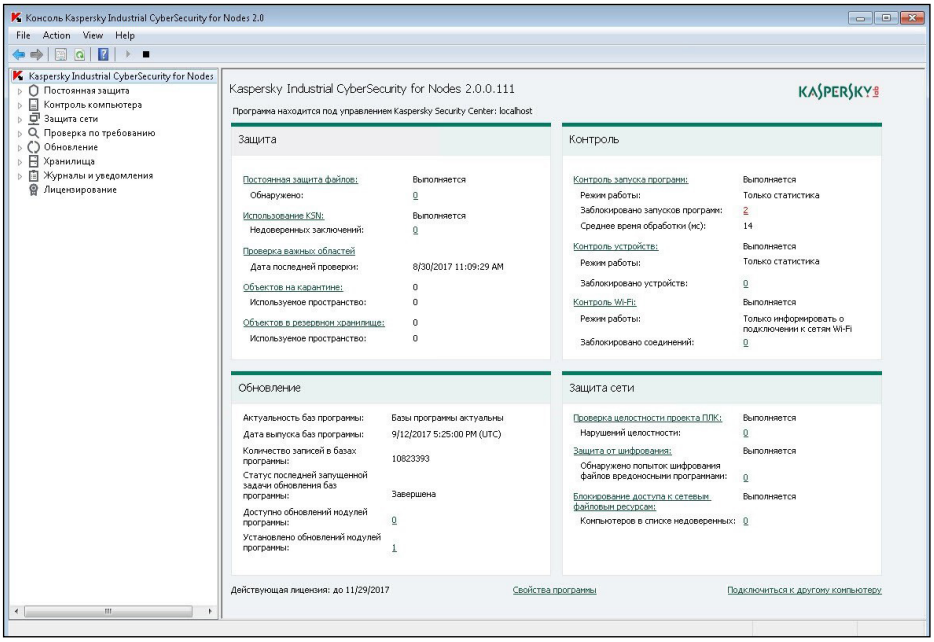


Рис. 1: Пример интерфейса KICS for Nodes

Ключевые функции KICS for Nodes:

- **Белые списки приложений** (контроль запуска приложений) — позволяют запретить запуск всех приложений, помимо явно разрешенных. Этот компонент можно использовать в тестовом режиме, чтобы упростить установку и снизить количество ошибок на этапе внедрения.
- **Контроль устройств** – позволяет администраторам определять, какие устройства разрешено подключать к защищаемым промышленным системам. Технология предотвращает возможность несанкционированного доступа и поддерживает применение масок для удобства управления и оперирования списком устройств.
- **Контроль беспроводных сетей** – позволяет отслеживать любые попытки подключения к неавторизованным сетям Wi-Fi.
- **Средства обнаружения вредоносных программ** (в т. ч. шифровальщиков) — сочетают сигнатурные и эвристические методы защиты и ограждают рабочие станции Windows от известных, неизвестных и сложных угроз. Технология Анти-Криптор защищает от попыток атак программ-шифровальщиков.
- **Межсетевой экран** – ограничивает возможность подключиться к узлам промышленной сети.
- **Проверка целостности ПЛК** — обеспечивает дополнительный уровень контроля конфигурации контроллера с помощью периодических проверок изменений в проектах.

KICS for Nodes после интеграции в инфраструктуру централизованно управляется из консоли Kaspersky Security Center, которая предоставляет следующие возможности:

- **Централизованное управление защитой и политиками безопасности** — позволяет создавать централизованные политики безопасности, а также настраивать параметры безопасности как для отдельных устройств, так и для групп.
- **Централизованное обновление антивирусных баз на защищаемых узлах сети** (в т. ч. когда технологическая сеть изолирована от интернета) — помогает поддерживать высокий уровень защиты за счет обновления агентов защиты с единого севера управления, установленного в технологической сети. Обновления могут быть загружены на сервер управления напрямую из интернета, либо с узла-ретранслятора (установленного в ИТ-сети или DMZ), а также принесены на сервер управления администратором на внешнем носителе
- **Тестирование обновлений перед внедрением** — позволяет проверить обновления на совместимость с промышленным ПО перед распространением на защищаемые узлы технологической сети.
- **Разграничение прав доступа на управление политиками, а также на действия с агентом защиты** — позволяет исключить неавторизованное изменение политики безопасности на сервере управления, а также препятствует отключению защиты или изменению настроек решения на конечных узлах.
- **Централизованный сбор данных о событиях безопасности со всех узлов сети** – позволяет производить качественный всесторонний анализ событий, относящихся к информационной безопасности, точно выявлять причины инцидентов и планировать меры противодействия угрозам.

Следует отметить, что работа KICS for Nodes принципиально построена так, чтобы исключить влияние на технологические процессы предприятия.

KICS for Networks

KICS for Networks является специализированным программно-аппаратным средством мониторинга сетевого обмена между узлами в промышленной сети систем защиты и управления, которое позволяет определять и регистрировать аномальные и важные с точки зрения обеспечения безопасности эксплуатации оборудования электроустановок и бесперебойного электро- снабжения потребителей информационные события. Об обнаруженных отклонениях KICS for Networks оповещает обслуживающий персонал (в том числе специалистов ИБ).

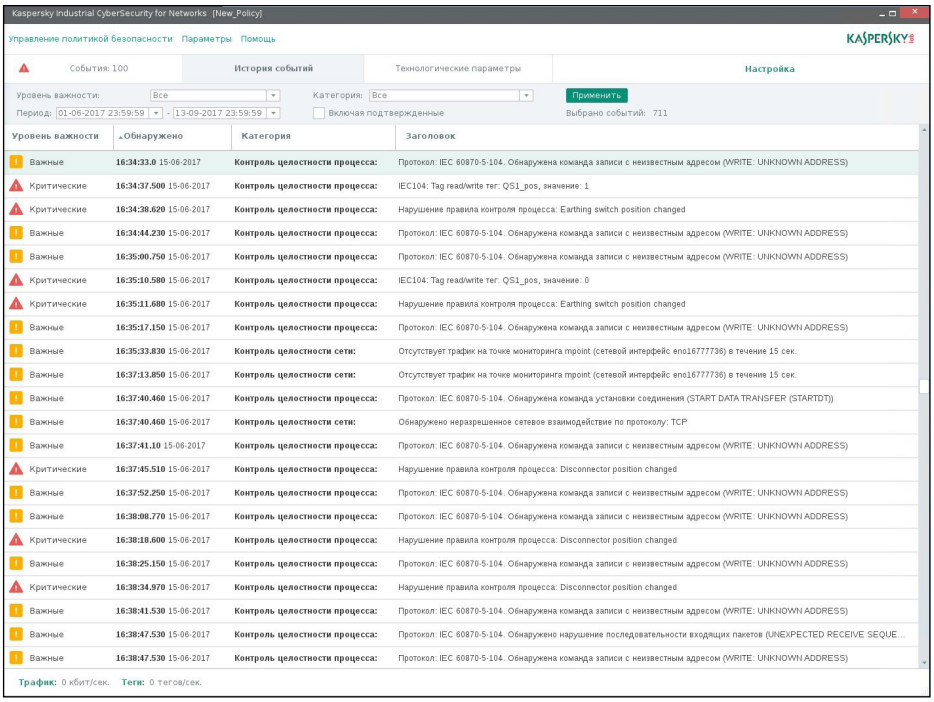
Ниже представлен список основных функциональных возможностей решения.

1. Мониторинг целостности технологической ЛВС:

- Режим самообучения, позволяющий выявить и зарегистрировать все существующие узлы ЛВС и коммуникации между ними, с целью последующего использования этой модели сети в качестве опорной и для отслеживания изменений.
- Обнаружение и регистрация подключения новых сетевых устройств к контролируемым сегментам технологической сети.

- Обнаружение и регистрация новых сетевых коммуникаций между узлами по признакам: адрес узла-отправителя, адрес узла-получателя, протокол обмена, порт, количество допустимых соединений и т. д.
- Обнаружение и регистрация сетевых подключений к ИЭУ с использованием прикладных технологических протоколов, используемых для конфигурирования.

Рис. 2: Пример интерфейса KICS for Networks с историей событий ИБ, полученных при тестировании вируса Industroyer



2. Анализ прикладных технологических протоколов:

- Разбор, анализ и регистрация важных сообщений прикладных технологических протоколов, в соответствии с конфигурацией и с учётом их возможного влияния на исполнение технологического процесса, а именно:
  - Обнаружение команд телеуправления оборудованием электроустановки (например, включения/выключения коммутационного аппарата) по промышленным сетевым протоколам (МЭК 61850, МЭК 60870-5-104).
  - Обнаружение команд телеуправления параметрами функционирования системы защиты и управления (например, переключения группы уставок) по промышленным сетевым протоколам (МЭК 61850, МЭК 60870-5-104).
  - Обнаружение фактов управления и параметрирования ИЭУ сервисным ПО через контролируемый сегмент сети — как при использовании стандартных, так и специализированных протоколов.
- Мониторинг сообщений телеизмерений и телесигнализации.

3. Хранение информации о событиях:

- Система KICS for Networks обеспечивает хранение выявленных событий во внутренней защищенной базе.
- Глубина хранения данных о событиях определяется сроком хранения и верхней границей размера архива.

4. Интеграция с внешними системами и уведомление пользователей:

- KICS for Networks можно интегрировать как один из компонентов в систему управления событиями безопасности (Security information and event management, SIEM) более высокого уровня, — например, HP ArcSight, либо в другую внешнюю систему, поддерживающую стандарт отправки и регистрации сообщений о событиях Syslog
- Уведомление ответственных лиц может быть дополнительно организовано при помощи сообщений электронной почты и SMS

Применение KICS for Networks позволяет определять большинство возможных событий в технологической сети, являющихся частью сценариев нарушения информационной безопасности. Тем самым обеспечивается своевременное информирование персонала о возможном инциденте, а также качественное расследование случаев технологических нарушений. Наличие KICS for Networks позволяет точно установить причину технологического нарушения и, соответственно, принять адекватные и эффективные меры для недопущения подобных инцидентов в будущем или защиты от них.

Пример развертывания средств обеспечения информационной безопасности KICS for Nodes и KICS for Networks на современной электрической подстанции

Пример решения, изображенный на рисунке 3 (см. стр. 9), показывает вариант развертывания оборудования и программного обеспечения средств обеспечения ИБ KICS for Networks и KICS for Nodes.

Защищаемая система защиты и управления имеет в своем составе два сегмента ЛВС кольцевой топологии. Первый сегмент, шина станции (Station Bus в соответствии с МЭК 61850), обеспечивает коммуникации ИЭУ между собой и между ИЭУ и подстанционными контроллерами, выполняющими роли коммуникационных фронтендов для SCADA, а также шлюзов телемеханики, через которые происходит информационное взаимодействие с вышестоящими уровнями диспетчерского управления. Помимо этого, по данному сегменту ЛВС, осуществляется обмен данными между серверами SCADA и подстанционными контроллерами, а также обеспечивается сервисный доступ к оборудованию системы защиты и управления посредством инженерного ПО.

Сервисный доступ может быть осуществлен как локально, так и удаленно. Локальный сервисный доступ производится с использованием ноутбука путем подключения непосредственно к ИЭУ или путем подключения ноутбука к ЛВС шины станции. Также сервисный доступ может быть выполнен с удаленного АРМ. Оперативные коммуникации между узлами сети в штатном режиме работы осуществляются по протоколу МЭК 61850 MMS. Сервисные коммуникации в части параметрирования устройств системы защиты и управления производятся по внутренним прикладным протоколам производителя оборудования. Вычитка файлов осциллограмм производится по протоколу FTP.

Физически сегмент ЛВС шины процесса представляет собой опорное кольцо, образованное двумя коммутаторами, соединенными между собой. Все устройства подключаются к опорным коммутаторам как узлы двойного присоединения (Double Attached Node, DAN). Таким образом в сегменте отсутствует единая точка отказа, что обеспечивает повышенный уровень безотказности сети. ИЭУ имеют встроенные коммутаторы и объединяются в цепочки, концы которых подключены к опорным коммутаторам, поэтому трафик между устройствами одной цепочки не проходит через коммутаторы. Управление сетью кольцевой топологии осуществляется при помощи протокола RSTP или его модифицированной производителем оборудования версии. Для организации удаленного сервисного доступа в сегменте установлен маршрутизатор/брандмауэр, способный также выполнять функции оконечной точки VPN соединения.

Второй сегмент, сегмент АРМ, представляет собой также ЛВС кольцевой топологии, предназначенный для взаимодействия между АРМ и серверами SCADA.

Взаимодействие с вышестоящими уровнями диспетчерского управления осуществляется непосредственно путем подключения подстанционных контроллеров к каналообразующей аппаратуре через маршрутизатор. Обмен осуществляется посредством протокола МЭК 60870-5-104.

Для полного мониторинга приведенной технологической ЛВС требуется инсталляция и подключение вычислительных средств с установленным ПО KICS for Networks в каждом выделенном сегменте сети. Таким образом, для приведенной схемы, должны быть установлены три сервера KICS for Networks для сегментов шины станции, АРМ и каналов связи вышестоящими уровнями управления. Для подключений серверов KICS for Networks требуется выполнить перенастройку коммутаторов в целях перенаправления на него трафика всех устройств. Интерфейсы серверов KICS for Networks настроены на работу только в режиме приема и неспособны оказать какое-либо влияние на работу системы защиты и управления. Устройства KICS for Networks производят первичную обработку трафика и определение аномалий. Полученные в результате данные передаются по защищенному каналу доверенной сети в зашифрованном виде на сервер Kaspersky Security Center, где производится агрегация информации и формируется окончательный список выявленных событий.

Для защиты вычислительных средств АСЗУ и системы обеспечения информационной безопасности под управлением ОС Windows на каждое из них устанавливается ПО KICS for Nodes. Данное программное обеспечение также пересылает обнаруженные события на сервер Kaspersky Security Center.

Для обеспечения данной функции, а также для обеспечения возможности удаленного централизованного конфигурирования ВС должны быть оснащены дополнительным сетевым интерфейсом для подключения к доверенной ЛВС СОИБ.

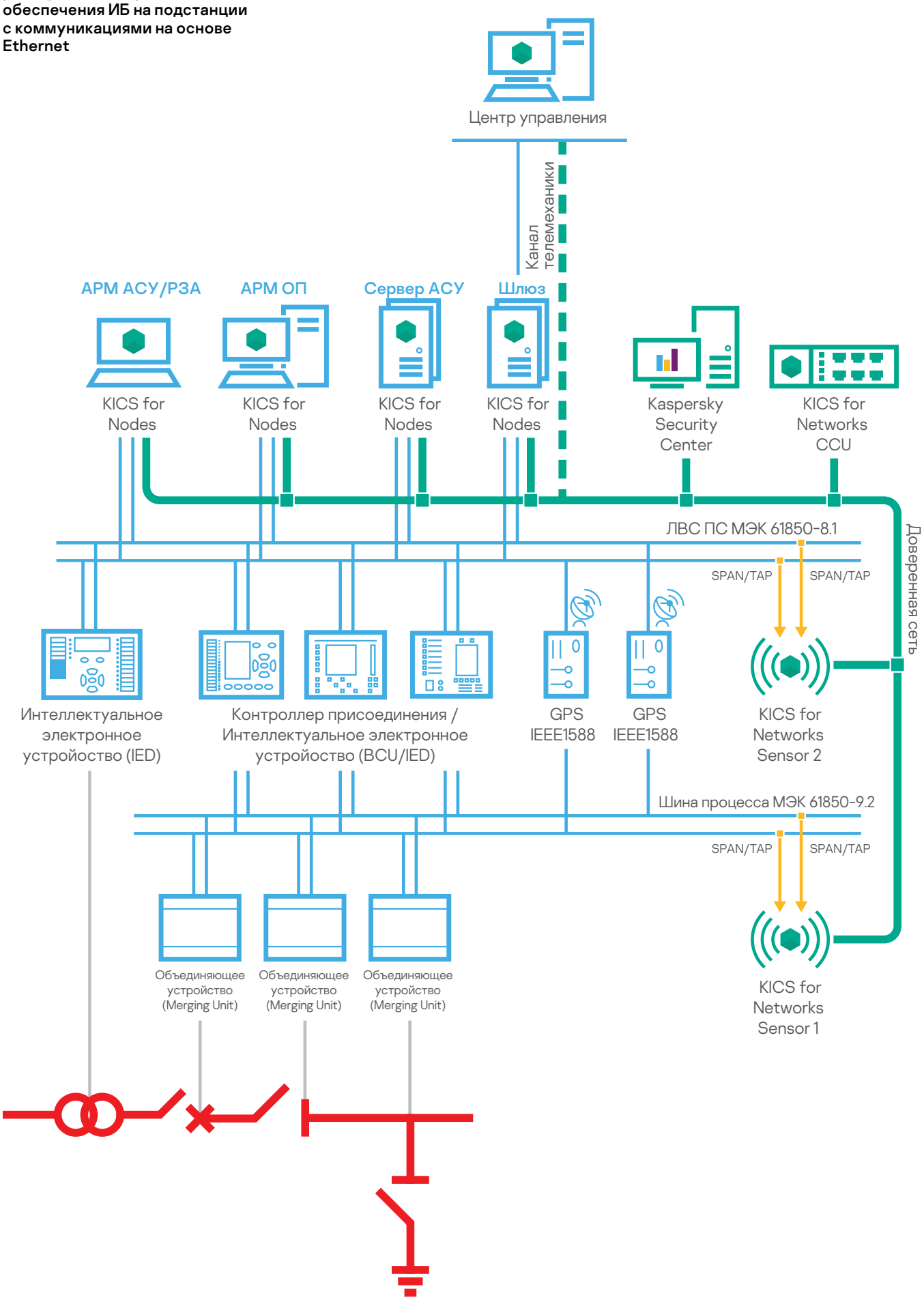
Весь информационный обмен по доверенной ЛВС СОИБ осуществляется в зашифрованном виде. В случае отказа доверенной сети, компоненты системы безопасности KICS for Networks и KICS for Nodes продолжат работу в изолированном режиме. Данные будут архивироваться локально и будут переданы на вышестоящий уровень при восстановлении работоспособного состояния сети.

На серверах SCADA, помимо базового функционала KICS for Nodes, установлен модуль периодического контроля конфигураций ИЭУ. Данный модуль может быть установлен а любое ВС, где установлен KICS for Nodes и есть сетевой доступ к контролируемым ИЭУ.

События, зафиксированные СОИБ, выводятся на выделенный АРМ СОИБ для информирования оператора.

При интеграции подстанционной СОИБ в систему предприятия (на схеме не показано) организуется защищенный канал передачи данных между локальным сервером Kaspersky Security Center и системой SIEM предприятия.

Рис. 3: Структурная схема развертывания средств обеспечения ИБ на подстанции с коммуникациями на основе Ethernet



Термины и определения

KICS — Kaspersky Industrial CyberSecurity. Специализированное решение «Лаборатории Касперского» для защиты критической инфраструктуры.

SCL — Substation Configuration Language (Язык конфигурирования подстанции). Язык и формат представления, описанный в МЭК 61850-6 и предназначенный для конфигурирования ИЭУ. Включает средства для описания информационной модели устройств, наборов данных для взаимодействия и коммуникационных сервисов. Основан на языке XML.

SPAN-port — Switched Port Analyzer. Порт сетевого устройства, на который перенаправляется сетевой обмен выбранных портов управляемого сетевого коммутатора в целях его анализа.

АСЗУ — автоматизированная система защиты и управления. Собирательный термин, обозначающий совокупность автоматических и автоматизированных систем управления различного назначения, установленных на рассматриваемом объекте.

АСУ ТП — автоматизированная система управления технологическими процессами. Человеко-машинная система на основе комплекса средств промышленной автоматизации и телекоммуникаций, обеспечивающая комплексное автоматическое и автоматизированное управление технологическими процессами на объекте управления с возможностью обеспечения дистанционного управления с удаленного диспетчерского пункта.

ВС — вычислительное средство. Техническое средство, способное производить обработку информации по заданной программе.

ИЭС ААС — интеллектуальная электроэнергетическая система с активно- адаптивной сетью. Представляет собой электроэнергетическую систему нового поколения, основанную на мультиагентном принципе организации и управления ее функционированием и развитием с целью обеспечения эффективного использования всех ресурсов (природных, социально-производственных и человеческих) для надежного, качественного и эффективного энергоснабжения потребителей за счет гибкого взаимодействия всех ее субъектов (всех видов генерации, электрических сетей и потребителей) на основе современных технологических средств и единой интеллектуальной иерархической системы управления.

ИЭУ — интеллектуальное электронное устройство. Специализированное многофункциональное вычислительное средство, выполненное на микропроцессорной элементной базе, обладающее развитыми цифровыми коммуникационными способностями.

РЗА — релейная защита и автоматика. Комплекс автоматических устройств, предназначенных для быстрого (при повреждениях) выявления и отделения от электроэнергетической системы поврежденных элементов этой электро- энергетической системы в аварийных ситуациях с целью обеспечения нормальной работы всей системы.

САУ — система автоматического управления.

СОИБ — система обеспечения информационной безопасности. Автоматизированная система, создаваемая и эксплуатируемая в целях обеспечения информационной безопасности защищаемого объекта.

ЛВС — локальная вычислительная сеть. Вычислительная сеть, охватывающая фиксированный набор взаимодействующих между собой узлов, объединённых по принципу территориальной близости.

ИБ — информационная состояние защищенности информации (данных), при котором обеспечиваются ее конфиденциальность, доступность и целостность.

Шина станции (Station Bus) — скоростная и высоконадежная локальная вычислительная сеть, обеспечивающая передачу данных интеллектуальными устройствами, реализующими технологические функции (уровень ячейки), и устройствами и ПТК, реализующими общеподстанционные функции (уровень подстанции) — например, SCADA, шлюз телемеханики и т. д.

В некоторых случаях по шине станции может осуществляться горизонтальные коммуникации между устройствами уровня ячейки. На электрических подстанциях, в целях исключения электромагнитных воздействий на каналы связи, шина станции зачастую выполняется на основе оптоволоконной среды передачи данных.

ics.kaspersky.ru
#активируйбудущее

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize