Этапы создания эффективной системы автоматизации подстанции

Это четвёртая и пятая части в серии статей, посвящённых интеллектуальным энергосистемам. В четвёртой части рассматривается вопрос о необходимости временно́й синхронизации сети Ethernet на электрической подстанции, перечисляются основные протоколы, решающие данную задачу, описываются их принципы работы, достоинства и недостатки. В пятой части поднимается проблема уязвимости вычислительных сетей современных подстанций перед киберугрозами и хакерскими атаками. Приводятся стандарты безопасности, применение которых улучшает защищённость сетей, описываются технологии, протоколы и средства повышения уровня кибербезопасности.

Часть 4. Что такое временна́я синхронизация на электрической подстанции?

Для обеспечения взаимосвязанного функционирования распределительных сетей на подстанции необходима точная временна́я синхронизация всех узлов сети. Временна́я синхронизация означает проверку точности временно́го согласования всех активных узлов, отвечающих за управление системой, сбор данных о состоянии процесса и пр. Временна́я синхронизация особенно важна при съёме показаний тока и напряжения, для обеспечения точных часов внутри средств автоматики защиты (описано в стандарте IEC 61850-9-2), средств измерения, контроля, терминальных устройств, преобразователей ток/напряжение и сетевых коммутаторов. Синхронизация помогает обеспечить точный контроль и тщательный анализ времени отклика сети, точно определить время и место возникновения сбоя.

В сети Ethernet подстанции временно́й синхронизации требуют работы следующих приложений:

- передача протоколов Ethernet высокого уровня, таких как GOOSE и MMS;
- сбор данных средствами измерения в режиме реального времени;
- контроль функционирования блоков релейной защиты и прочего оборудования в реальном масштабе времени;
- протоколирование сбоев для последующего анализа на надёжность и производительность.

Существуют два основных метода временно́й синхронизации на подстанциях: прямая временна́я синхронизация и синхронизация по локальной сети.

Какие протоколы применяются для временной синхронизации на подстанциях?

Обычно внутренние часы сетевых устройств синхронизируются со специальным сервером времени, подключённым к GPS-генератору точных сигналов (или к двум – для резервирования). В зависимости от сетевых приложений временна́я синхронизация часов для событий и сбоев может происходить с различной точностью: от нескольких миллисекунд до долей микросекунд. Точность временно́й синхронизации в сети зависит от таких факторов, как используемые протоколы, степень загрузки трафиком, тип используемой среды и длина кабельной сети.

Прямая синхронизация часов

Как правило, прямая синхронизация внутренних часов конечных устройств производится специальными таймин-говыми сигналами, передаваемыми по выделенным каналам связи, таким как оптические линии, коаксиальные кабели или витая пара. Для системы достаточно одного сервера времени, с мастер-часами которого синхронизируются остальные. Однако из-за необходимости прямого подключения к серверу каждого устройства и ограниченного количества портов синхронизации лишь небольшой набор конечных устройств может быть синхронизирован. Прямая синхронизация часов применяется внутри отсеков с устройствами релейной защиты и автоматики (РЗА) и на уровне процесса автоматизированной подстанции. Стандартными протоколами для прямой синхронизации считаются GPS, IRIG-B и 1PPS.

*Первая и вторая части статьи опубликованы в «СТА» 1/2013, третья часть – в «СТА» 2/2013.

- **GPS** – протокол глобального спутникового позиционирования. GPS-системы высоконадёжны и могут быть использованы для прямой синхронизации часов или как источники точного времени для других протоколов. GPS-система способна обеспечить точность синхронизации в 10 наносекунд относительно значения универсального координированного времени UTC.
- **IRIG-B** – промышленный стандарт GPS-синхронизации, разработанный компанией Inter-Range Instrumentation Group (США). IRIG-B может применяться на объектах энергетики (электрических подстанциях) для контроля качества и стабильности процессов. В этом случае последовательность событий с временно́й синхронизацией записывается с шагом 1 мс. Коды временно́й синхронизации IRIG-B могут быть переданы только по выделенным кабелям типа витой пары или коаксиальных кабелей, что делает реализацию данного протокола довольно дорогой. IRIG-B также требует внешнего источника точного времени. Точность передаваемых значений точного времени лежит в микросекундном диапазоне, типовое значение – 100 мкс.
- **1PPS** (Pulse Per Second) передаёт один синхроимпульс в секунду. Это высокоточный временно́й сигнал от источника точного времени (GPS-ресивера), который означает начало каждой секунды. Сигнал 1PPS посылается конечному устройству по выделенной линии, что влечёт за собой серьёзное удорожание системы. Точность временно́й синхронизации по протоколу 1PPS также находится в микросекундном диапазоне, типовое значение – 1 мкс.

Временна́я синхронизация по ЛВС

При временно́й синхронизации по ЛВС для передачи синхроимпульсов используется сеть Ethernet. Стоимость кабельной инфраструктуры при этом гораздо ниже, чем в предыдущих случаях, а сигналы временно́й синхронизации передаются в одной среде с данными. Обычно для синхронизации конечных устройств по сети на уровне станции используется протокол SNTP, а на уровне процесса и ячеек – протокол IEEE 1588 PTP (Precision Time Protocol).

Протокол SNTP (Simple Network Time Protocol) является производной от распространённого протокола NTP и отличается от последнего отсутствием многих внутренних алгоритмов, которые, как правило, не задействованы на всех типах серверов. SNTP широко распространён в Internet и распределённых локальных сетях, он обеспечивает точность синхронизации часов в миллисекундном диапазоне (1–10 мс). Протокол SNTP подходит для применения на уровне станции, но не обеспечивает достаточной точности синхронизации часов для передачи GOOSE- и SV-сообщений на уровне процесса.

IEEE 1588 PTP – протокол, получающий всё большее распространение в высокоточных системах. Он описан в стандартах синхронизации IEEE 1588 и IEEE 61588. Эффективность протокола достигается использованием существующей сети Ethernet для синхронизации внутренних часов интеллектуального оборудования подстанции. IEEE 1588 использует алгоритм ведущий/ведомый и аппаратную обработку синхроимпульсов.

Протокол IEEE 1588 PTP существует в двух несовместимых между собой версиях: PTP v1 и PTP v2. IEEE 1588 PTP v2 – протокол, востребованный на уровне процесса по стандарту IEC 61850-9-2 или стандарту IEEE C37.118-2005 на автоматизированных подстанциях. Может быть преобразован в IRIG-B. Внутренние часы распределённых конечных и промежуточных сетевых устройств могут быть синхронизированы с помощью IEEE 1588 PTP v2 с наносекундной точностью (30–50 нс).

Достоинства протокола IEEE 1588 PTP v2

Протокол IEEE 1588 PTP v2 используется для критически важных приложений, которыми являются процессы на электрической подстанции. Далее перечислены его основные преимущества.

- **Универсальность.** IEEE 1588 PTP v2 использует алгоритм BMC (Best Master Clock), автоматически определяющий самый точный источник времени для синхронизации. При этом выбранные мастер-часы также получают временны́е сигналы от других потенциальных мастер-часов. Все часы в сети используют одинаковую информацию и таким образом приходят к согласованному результату. Быстрая синхронизация может быть достигнута и при изменениях в сети. IEEE 1588 PTP v2 предотвращает накопление ошибки в каскадных топологиях, поддерживает отказоустойчивость и увеличивает гибкость системы.
- **Экономичность.** Протокол IEEE 1588 PTP v2 может использовать существующую сеть Ethernet для снижения стоимости кабельной инфраструктуры. Сигналы синхронизации пересылаются по сети в виде адресных unicast-кадров уменьшенного размера. Это способствует минимизации загрузки сети и сетевых процессоров. Протокол легко интегрировать в конечные устройства и сети Ethernet с многоадресной рассылкой.
- **Высокая точность.** Протокол IEEE 1588 PTP v2 способен синхронизировать часы с различной точностью и разрешением. Достигается точность синхронизации в наносекундном диапазоне.

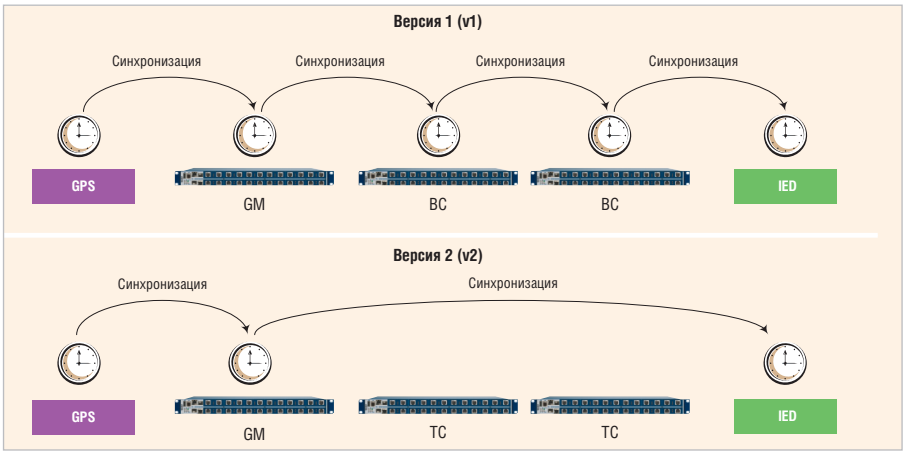
Как работает IEEE 1588 PTP v2?

Протокол IEEE 1588 PTP существует в двух версиях: PTP v1 (стандарт IEEE 1588-2002) с поддержкой оконечных и граничных часов и PTP v2 (стандарт IEEE 1588-2008), которая дополнительно вводит понятие «прозрачных» часов.

В первой версии для граничных часов требуются мастер-часы, контролируемые, например, GPS-ресивером (рис. 16). Мастер-часы определяют базовое время системы и синхронизируются с ведомыми часами (граничные часы коммутаторов сети или оконечные часы конечных устройств), подключаемыми к ним на каждом этапе. В ведомых часах восходящий порт, подключённый к PTP мастер-часам, является ведомым, а остальные порты выполняют роли мастер-часов для подключённых к ним устройств.

На первом этапе работы протокола PTP корректируется разница между временем мастера и ведомых устройств (компенсация). Затем измеряется задержка по времени между мастером и ведомыми устройствами по задержке между запросом и ответом. В финале часы промежуточных и конечных устройств синхронизируются с мастер-часами в соответствии с задержкой и необходимым временем компенсации. Наилучший результат синхронизации часов достигается при минимизации количества узлов между главными мастер-часами и оконечными часами конечных устройств.

В версии 2 для механизма «прозрачных» часов корректируется так называемое время нахождения (рис. 17). Это



Условные обозначения: BC (boundary clock) – граничные часы; **GM** (ground master clock) – мастер-часы; **TC** (transparent clock) – «прозрачные» часы; **IED** – интеллектуальное конечное устройство.

Рис. 16. Схема работы протокола PTP версий 1 и 2

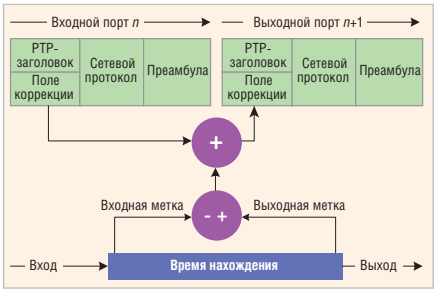
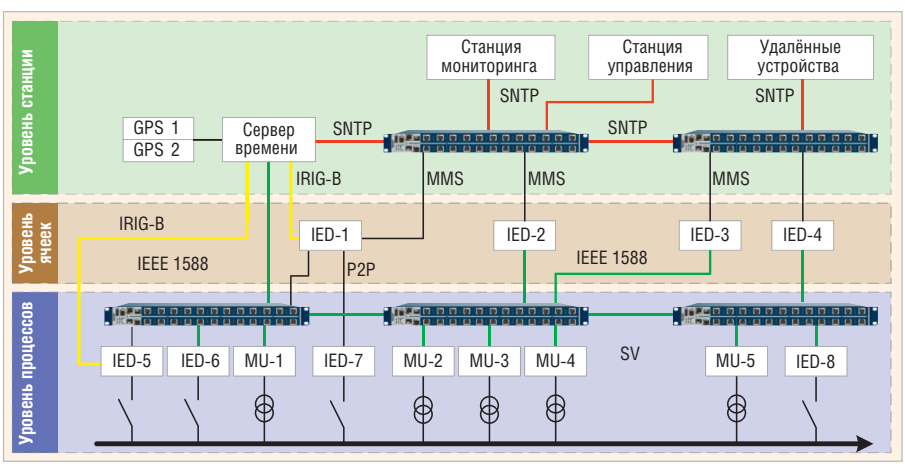


Рис. 17. Механизм учёта времени нахождения в PTP версии 2

время для часов промежуточных устройств (например, Ethernet-коммутаторов), затрачиваемое Ethernet-трафиком на прохождение через устройство, оно вычисляется по временны́м меткам входа кадра данных и выхода его из устройства. Время нахождения аккумулируется в специальном поле кадра (поле коррекции) для реализации механизма синхронизации. Так как «прозрачные» часы выполняют только фиксирующую функцию, они не влияют на такие параметры сети, как время восстановления кольца и т.п. Каждый такой коммутатор по поведению приближен к физическому проводу, который не ухудшает время прохождения пакета данных через него. Таким образом, не накапливается погрешность измерения времени синхронизации в многокаскадных коммутируемых сетях.

В стандарте IEEE 1588-2008 поддерживаются два типа «прозрачных» часов: конечный–конечный (end-to-end –E2E) и участник–участник (peer-to-peer – P2P). «Прозрачные» часы типа E2E только измеряют время, потраченное PTP-сообщением (тем, которое получает временну́ю метку) на прохождение коммутатора, и передают эту информацию принимающим часам в поле коррекции. Часы типа P2P измеряют задержку на прохождение пакетом коммутатора и прибавляют к нему время прохождения по линии связи, используя механизм запрос–ответ.



Условные обозначения: —— – протокол SNTP в шине станции; —— – протокол IEEE 1588 в шине процессов; —— – протокол IRIG-B в шинах станции и процессов; **IED-1…IED-8** – интеллектуальные конечные устройства 1…8; **MU-1…MU-5** – объединяющие устройства 1…5.

Рис. 18. Синхронизация времени в сети подстанции

Как применять синхронизацию времени для автоматизации подстанции?

К синхронизации времени в шинах станции и процесса предъявляются разные требования. Рис. 18 показывает пример того, как можно реализовать синхронизацию времени на подстанции, используя разные протоколы. На рисунке видно, что точные значения времени передаются от GPS-приёмника к серверу времени, с которым будут синхронизироваться конечные устройства и коммутаторы. Для повышения надёжности системы применяется дублированная схема с резервным GPS-приёмником. В шинах станции и процесса, в которых используется синхронизация времени, часто применяется топология типа звезда. Обычно схемы синхронизации часов на уровне ячеек и процесса реализуются независимо друг от друга, однако может использоваться и общий источник точного времени.

Протокол SNTP используется только на уровне станции для синхронизации коммутаторов сети с удалёнными устройствами, станциями мониторинга и управления. В соответствии с требованиями на подстанции синхронизация часов по протоколу IEEE 1588 PTP v2 с «прозрачными» часами применяется для оборудования на уровне ячеек и процесса. Для этого, начиная с уровня процесса, используются специальные коммутаторы с поддержкой IEEE 1588. Так как на уровне процесса не применяется протокол IP, стек IEEE 802.3 используется для PTP-сообщений. Протоколы IRIG-B и 1PPS требуют отдельной кабельной инфраструктуры и синхронизируют устройства на уровне ячеек и процесса. Для достижения высокой точности синхронизации могут использоваться связи типа точка–точка между блоками РЗА, преобразователями и прочими устройствами без применения промежуточных коммутаторов.

Выводы по части 4

Динамично развивающийся стандарт синхронизации часов IEEE 1588 создаёт условия для повышения надёжности сети подстанции. Качественная реализация положений и требований данного стандарта невозможна без специализированных коммутаторов, таких как коммутаторы серий MICE, MACH, RPS, EES торговой марки Hirschmann.

Часть 5. Вопросы кибербезопасности сетей электрических подстанций

Угрозы и возможные кибератаки на электрических подстанциях

Электрическая подстанция – критически важный объект для энергетической отрасли. Вопросы обеспечения безопасности подстанций должны охватывать не только ограничение доступа к их физическим активам. Объектами посягательств может стать и виртуальное содержимое систем электроподстанции: информация, базы данных, программные приложения и средства доступа к ним. Кибербезопасность данных становится неотъемлемым элементом надёжности подстанции. Статистика свидетельствует о росте количества киберпреступлений и их проникновении в промышленный сектор.

До сих пор кибербезопасность не признавалась важным вопросом и серьёзно не рассматривалась при проектировании подстанции. Персонал подстанции, как правило, не имеет понятия о возможных угрозах безопасности объекта и не видит необходимости менять эту ситуацию. Однако большинство коммуникационных сетей электроподстанций открыто, а потребность в доступе к информации растёт. Сети Ethernet, открытые протоколы (такие как TCP/IP) уязвимы. Атаки против них могут быть проведены стандартными средствами. Большинство оборудования, например блоки РЗА, имеет удалённый доступ по IP-сетям, Internet, и технологии глобальных сетей предоставляют множество возможностей для кибератак.

Потенциально интересными для хакеров являются блоки РЗА, SCADA-система, система управления нагрузкой, базы данных, приложения и Web-сервисы. Даже если сеть передачи данных изолирована от глобальной сети и внешнее оборудование с удалённым доступом не подключено, угроза может исходить от персонала станции, не обладающего специальными знаниями и техникой безопасности.

В целом можно выделить четыре типа киберугроз:

- несанкционированный доступ к информации,
- несанкционированное изменение или кража данных,
- отказ сервисов,
- отсутствие обнаружения ложной информации (lack of repudiation/unaccountability).

Стандарты обеспечения безопасности сети передачи данных на электроподстанции

IEC 61850

Требования к обеспечению безопасности коммуникационной среды на подстанции описаны в рекомендациях по безопасности стандарта IEC 61850 (дополнительно см. стандарт IEC 62351-6 «Безопасность по IEC 61850»).

IEC 62351

Данный стандарт охватывает вопросы информационной безопасности энергетических систем, о чём красноречиво свидетельствует его полное название – «Управление энергетическими системами и связанный с ним обмен информацией. Защита данных и коммуникационная безопасность».

Таблица 3

Стандарты кибербезопасности CIP

CIP 001	Протоколирование хакерских нападений
CIP 002	Определение критически важных активов
CIP 003	Элементы управления безопасностью
CIP 004	Подготовка и обучение персонала
CIP 005	Электронный контур безопасности
CIP 006	Физическая защита информационных активов
CIP 007	Управление безопасностью системы
CIP 008	Протоколирование инцидентов и планирование ответных действий
CIP 009	Планы по восстановлению критически важных активов

NISTIR 7628

Это инструмент и набор инструкций для организации кибербезопасности в интеллектуальных электрических сетях, опубликованный американским Национальным институтом стандартов и технологий (National Institute of Standards and Technology – NIST). Интеллектуальная электрическая сеть – это развивающаяся информационная сеть с модернизированными системами генерации энергии, её передачи и распределения. Все сегменты сети могут быть целями для кибератаки. Автоматизированная подстанция является своего рода защищённой магистралью для сетей генерации и распределения, поэтому её защита должна быть надёжной.

NERC CIP

Ещё один важный стандарт для обеспечения кибербезопасности был опубликован американской корпорацией NERC (North American Electric Reliability Corporation). Стандарт CIP (Critical Infrastructure Protection) определяет типы и характер возможных угроз для повышения надёжности и уровня защищённости от террористических угроз. Спецификации NERC CIP 002–009 требуют консолидации правил, политик, процедур и технологий производителей для организации баз данных важных параметров и списков доступа к ним. Стандарт использует разные методы авторизации, политики и уровни доступа для ранжирования данных по степени секретности и ограничению доступа к ним (табл. 3).

IEEE 1686-2007

Это стандарт безопасности для интеллектуальных конечных устройств, например РЗА. Он устанавливает правила безопасности для устройств согласно уже упоминавшемуся стандарту NERC CIP. Этот стандарт определяет особенности и функции интеллектуальных конечных устройств в соответствии с программой защиты сетевой инфраструктуры. Также IEEE 1686-2007 предоставляет специальную таблицу соответствия, по которой производители оборудования могут проверять, насколько их изделия отвечают требованиям стандарта.

Технологии обеспечения кибербезопасности на объектах энергетики

Для обеспечения высокой доступности систем электроподстанции необходим расширенный набор средств безопасности. Требуются глубокий анализ и контроль возможных киберугроз для охраны периметра, внутренней сети, конечных устройств.

Базовая идея обеспечения безопасности на подстанции – определить безопасный трафик внутри каждого протокола, например, установить, кто – отправитель, а кто – получатель. Даже в случае полной изолированности сети и отсутствия внешних подключённых устройств требуются такие средства обеспечения безопасности, как специальные протоколы, записи действий пользователей, пароли, ограничение доступа, ограничение свободных портов, шифрование. Это поможет избежать последствий неправильной установки и конфигурирования оборудования и ПО.

Можно выделить два разных типа кибербезопасности в коммуникационных сетях электрических подстанций: физическую и сетевую.

Для обеспечения физической безопасности коммуникационной сети коммутационные шкафы запирают на ключ, используют нестандартные винтовые коннекторы M12, отключают неиспользуемые порты устройств и коммутаторов, то есть предотвращают нежелательный доступ к сетевым портам. Также применяют проверку пользователей по портам устройств. Коммутаторы Ethernet позволяют устройствам подключаться по заранее разрешённому списку IP- и MAC-адресов, подключения с незарегистрированных адресов отклоняются.

Для обеспечения сетевой безопасности базовым механизмом является стандарт AAA. Стандарт установления подлинности, разрешения и учёта (Authentication, Authorization and Accounting – AAA) применяется в отношении пользовательского доступа и учёта трафика для всего сетевого оборудования. Он определяет, кто или что имеет доступ, к каким ресурсам, используя списки правил и управление доступом для фильтрации входящего трафика. Наконец, не стоит пренебрегать элементарными правилами, такими как ограниченный допуск к удалённому управлению сетевым оборудованием, многоуровневый доступ для пользователей и администраторов.

В рамках стандарта AAA могут применяться описываемые далее технологии.

- **SNMP v3** – третья версия протокола сетевого управления Simple Network Management Protocol (SNMP). Протокол базируется на стандартах информационного обмена и позволяет осуществлять внешний мониторинг заранее определённого контента через специального клиента. Протокол SNMP v3 предлагает такие функции безопасности, как пользовательская модель безопасности (User-based Security Model – USM), зашифрованный процесс проверки пользователей и хранения их данных, своевременная проверка сообщений, визуальный контроль доступа. Это делается с целью предотвращения манипуляций с информацией, пассивного прослушивания сети, имитаций соединений.
- **RADIUS** (Remote Authentication Dial in User Service) – технология удалённой проверки пользователей, основанная на модели клиент–сервер. RADIUS-сервер уже стал базовой технологией для проверки пользователей и устройств до того, как им даётся доступ в сеть. Кроме того, эта технология позволяет применять индивидуальные профили к каждому пользователю, определять наборы доступных и запрещённых сервисов и узлов сети. Все шлюзы, предоставляющие доступ в сеть с RADIUS-сервером, должны иметь IEEE 802.1x RADIUS-клиента.
- **TACACS** (Terminal Access Controller Access-Control System) – система аутентификации сервера доступа к сети. Протокол TACACS использу-

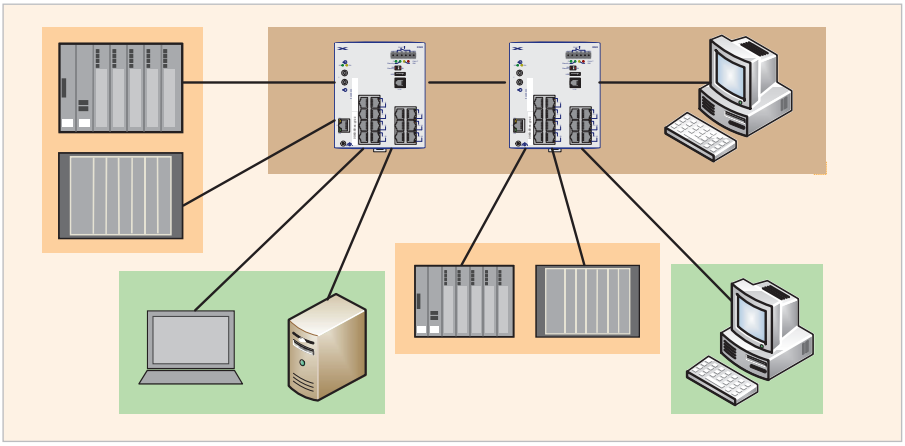


Рис. 19. Множественные сети VLAN

ется для коммуникаций сервера удалённого доступа с сервером контроля доступа. Его также можно использовать для аутентификации клиента при доступе в сеть подстанции.

- **SSH** (Secure Shell) – технология, которая может быть использована для безопасного удалённого доступа к коммуникационным устройствам сети подстанции. При этом данные, удалённые команды и ответы на них между двумя сетевыми устройствами передаются в зашифрованном виде. SSH использует криптографическую защиту с публичным ключом, а также проверяет, действительно ли контролируемый клиент владеет правильным персональным ключом.

«Контурный» подход к обеспечению кибербезопасности

Кроме физического уровня безопасности и протокола AAA можно выделить ещё и несколько контуров безопасности.

- **Контур коммутаторов сети.** Коммутаторы являются основными активными компонентами сети. Логически изолированные сегменты сети подстанции могут быть построены с использованием технологии VLAN внутри одной физической сети. Клиенты, подключённые к разным коммутаторам, могут обмениваться данными при условии, что они находятся в одной виртуальной сети; в свою очередь, клиенты, принадлежащие разным виртуальным сетям, попросту не видят друг друга. Для реализации потребуются управляемые коммутаторы с поддержкой множественных VLAN (рис. 19). Такое тотальное разделение обеспечивает первичный контур безопасности на уровне коммутаторов Ethernet.
- **Контур маршрутизаторов сети.** Маршрутизатор, или роутер, – это устройство, направляющее трафик сети через стандартные или резервированные линии данных между коммуникационными сетями подстанций, между самими подстанциями и от подстанций к единому центру управления. Роутеры с поддержкой VLAN могут также осуществлять маршрутизацию трафика для различных виртуальных сетей. При прохождении пакета данных по сети промежуточные роутеры считывают адрес получателя

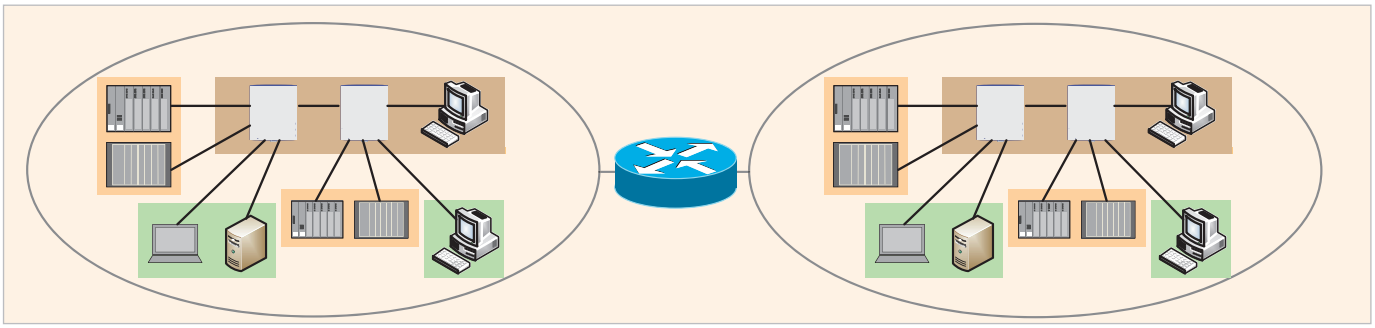


Рис. 20. Разделение подсетей VPN с помощью межсетевого экрана

из его IP-заголовка. При этом одной из базовых технологий администрирования и обеспечения безопасности является использование списков контроля доступа ACL (Access Control Lists). С их помощью предотвращается несанкционированный доступ в сеть: по ним роутер должен обработать каждый пакет данных, прежде чем отправить его дальше по сети. Также ACL-списки могут применяться в качестве средств прослушивания (снифферов) для фильтрации пакетов, не удовлетворяющих заданным условиям. Их следует использовать в роутерах между разными сетями VLAN и интерфейсами для повышения безопасности сети подстанции.

- **Контур межсетевых экранов.** Некоторые роутеры могут выполнять функции межсетевых экранов (firewall), с помощью которых создаются защищённые сегменты сети. Межсетевой экран – это программное или аппаратное средство (или комплекс устройств), усиливающее контроль между двумя сетями. Он может защищать от несанкционированного доступа во внутреннюю сеть и скрывать её внутреннюю структуру. Прозрачные межсетевые экраны (мосты) также могут использоваться для повышения безопасности в существующей сети (рис. 20). Межсетевые экраны могут вести журнал сетевого доступа и анализировать его для генерации тревоги в случае атак и ошибок. Их традиционными функциями являются пакетная фильтрация, фильтрация контента, контроль доступа, авторизация пользователей, управление протоколами и сервисами, контроль данных на защищённых электрических подстанциях. В целом с помощью роутеров создаются защищённые ячейки сети или зоны внутри сети с ограниченными коммуникациями по отношению к внешней сети – это средства глубокой защиты.
- **Контур шлюзов.** Когда сеть подстанции является удалённой и доступ в неё осуществляется через глобальную сеть, требуется дополнительное обеспечение безопасности сети на уровне шлюзов данных. Шлюзы собирают измерительную информацию с модулей РЗА и терминальных устройств, данные о состоянии автоматики, событиях в сети, ошибках и обеспечивают их доставку к ERP-системе или обслуживают внешние подключения, например операторов через Web-браузер. Шлюзы обеспечивают контроль и фильтрацию трафика, защищают устройства автоматики (РЗА и пр.) от несанкционированного доступа. Для этого в шлюзах часто используются виртуальные сети VLAN с шифрованием.

Также здесь следует упомянуть VPN (Virtual Private Network) – это защищённое зашифрованное соединение между двумя точками через незащищённую сеть. VPN используется для создания тоннеля между двумя сетями, данные в тоннелях шифруются. Есть два основных способа создания VPN-сетей. Первый – это OpenVPN, открытый инструмент создания VPN-соединений типа точка–точка и сайт–сайт. Он позволяет пользователям идентифицировать друг друга, используя механизм Pre-Shared Key, сертификаты безопасности, логины и пароли. OpenVPN создаёт TCP- и UDP-тоннели с зашифрованными данными внутри незащищённой сети. Второй способ – протокол IPSec (Internet Protocol Security), открытый стандарт, позволяющий обеспечить закрытое и защищённое соединение поверх IP-сетей путём использования криптографических сервисов. IPSec обеспечивает безопасность данных на уровне IP-пакета, поддерживает целостность данных на сетевом уровне, конфиденциальность данных, оригинальную проверку данных и защиту от дублирования. Таким образом обеспечивается защита в глубину против сетевых атак, повреждений данных, кражи данных, захвата пользовательских данных или несанкционированного доступа к компьютерам или сети.

Рис. 21. Аппаратно-программный комплекс EAGLE Tofino для комплексной защиты промышленных сетей от различных киберугроз

Выводы по части 5

Сети передачи данных на электроподстанции относятся к критически важным объектам. Сетевые устройства (блоки РЗА и пр.) и сетевые приложения могут быть атакованы путём использования доступных средств, например бесплатных утилит типа Nessus (популярный в мире сканер уязвимостей). Соответственно, необходимо обеспечение безопасности на уровне портов сетевых устройств, реализации стандарта AAA, сетей VLAN, межсетевых экранов, роутеров, шлюзов, системных журналов для повышения стойкости сети к инсталляционным и конфигурационным ошибкам, а также сетевым атакам. Кибербезопасность усиливает надёжность и безопасность системы управления в целом и снижает операционные расходы на электроподстанции.

Компания Belden предлагает широкий спектр сетевого оборудования для электроподстанций под марками Hirschmann и GarrettCom. Для защиты в глубину ею совместно с дочерней компанией Byres Security разработано программно-аппаратное решение Hirsch-

mann EAGLE, которое учитывает специфику возможных угроз, используемых протоколов и трафика на электрических подстанциях.

Под маркой Hirschmann представлены две серии продукции: промышленный межсетевой экран и VPN-роутер EAGLE 20 и система EAGLE Tofino (рис. 21), ориентированная на инженеров по автоматизации с начальной IT-подготовкой.

Основные функции EAGLE 20:

- стационарный межсетевой экран включает в себя список правил для входящих/исходящих подключений, модемного доступа и управления, предоставляет функции маскировки IP, трансляции адресов 1:1 NAT, ограничения DoS, фильтрации по MAC-адресам, пользовательский экран для удалённого управления правилами;
- многоточечное VPN-соединение с поддержкой протоколов IPSec, шифрования IKEv2, DES, 3DES, AES (128, 192, 256 бит), ключей PSK, сертификатов X.509v3, а также с поддержкой MD5, SHA-1, NAT-T, раздельных правил для VPN-соединений, Web-интерфейса и удалённого управления подключениями.

Преимущества системы EAGLE Tofino:

- определение правил в графическом режиме методом drag-and-drop (трафик, не подпадающий под правила, автоматически блокируется, о чём сигнализируется);
- более 50 предопределённых IT- и промышленных протоколов (PTP, OPC, PROFINET, Modbus и многие другие);
- более 25 шаблонов для ПЛК различных производителей;
- предопределённые специальные правила для глубокой фильтрации трафика и защиты от угроз;
- защита контроллеров от известных и потенциальных угроз.

Технологии обеспечения безопасности Hirschmann упрощают сквозной обмен информацией внутри электрической подстанции, повышая её безопасность и производительность. ●

Рекомендуемая литература

1. IEC 61850 – Communication Networks and Systems in Substations : [Part 1–10]. – IEC, 2002.
2. IEC 61850-90-4 – Technical report: Network Engineering Guidelines. – IEC, 2012.
3. Service & Support [Электронный ресурс] // Belden. – Режим доступа : http:// www. beldensolutions.com/de/Service/index.phtml.
4. CIP Standards [Электронный ресурс] // NERC. – Режим доступа : http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
5. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, 2010 [Электронный ресурс] SGIP. – 2010 – Режим доступа : http://www.nist.gov/ smartgrid/ upload/ nistir-7628_total.pdf.
6. IEC 62351-1 – Data and communication security : [Part 1: Introduction and overview]. – IEC, 2006.
7. Shailendra Fuloria, Ross Anderson, Kevin McGrath, Kai Hansen, etal. The Protection of Substation Communications [Электронный ресурс]. – Режим доступа : http://www.cl.cam.ac.uk/~sf392/publications/S4-2010.pdf.
8. Andreas Dreher, Eric Byres. Get Smart About Electrical Grid Cyber Security [Электронный ресурс] // Hirschmann, White Paper. – 2010 – Режим доступа : http://www.belden.com/pdfs/techpprs/PTD_Cyber_SecurityWP.pdf.

**Перевод Ивана Лопухова,
сотрудника фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru**