ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ СИСТЕМ РЕЛЕЙНОЙ ЗАЩИТЫ И АВТОМАТИЗАЦИИ

Юшкевич Р.А.
Научный руководитель – старший преподаватель Булойчик Е.В.

В последнее время все больше внимания уделяется вопросам создания цифровых подстанций. Ключевым свойством цифровой подстанции является минимизация аналоговых и дискретных трактов в системах мониторинга и управления, что обеспечивается за счет максимально полной цифровизации систем оперативного и автоматического управления, в результате чего весь функционал устройств релейной защиты, противоаварийной автоматики и автоматизированного диспетчерского управления сосредотачивается во взаимосвязанных компьютерных подсистемах энергообъекта.

Суть проблемы кибербезопасности заключается в том, что закрытость объекта больше не является барьером для кибератаки, которая может преодолеть изоляцию, и все данные на верхнем уровне АП с внедрением IEC 61850, если не принять специальные меры, могут стать доступными не по назначению. IEC 61850 лучше всего реализован через инфраструктуру Ethernet. Связь с сетью лишает преимуществ изоляции. Связь «клиент-сервер», поддерживающая более одного клиента, увеличивают возможность появления неавторизированного клиента.

Системы управления больше не защищены за счёт закрытости объекта, как это было раньше.

Используются TCP/IP и другие протоколы, характерные для обеих сред, что приводит к целому ряду проблем.

Для обеспечения требований по безопасности и для оценки её уровня предлагаем использовать семь основополагающих требований, кодифицированных в ISA 01.01.99:

– управление доступом (AC – Access Control), чтобы защитить от несанкционированного доступа к устройству или информации;

– управление использованием (UC – Use Control), чтобы защитить от несанкционированного оперирования или использования информации;

– целостность данных (DI – Data Integrity), чтобы защитить от несанкционированного изменения;

– конфиденциальность данных (DC – Data Confidentiality), чтобы защитить от подслушивания;

– ограничение потока данных (RDF – Restrict Data Flow), чтобы защитить от публикации информации на несанкционированным источниках;

– своевременный ответ на событие (TRE – Timely Response to Event), мониторинг и протоколирование связанных с безопасностью событий и принятие своевременных мер по ликвидации последствий в ответственных задачах и в критических ситуациях по безопасности;

– доступность сетевого ресурса (NRA – Network Resource Availability), чтобы защитить от атак «отказ в обслуживании».

При анализе существующих и разрабатываемых стандартов выяснилось, что ни один из рассмотренных документов не удовлетворяет всем семи требованиям. Значит необходимо искать правильные решения, потому что эти требования должны стать исходным руководством для инженеров-релейщиков.

Так же проблемой при обеспечении кибербезопасности на энергетических объектах является человеческий фактор.

Суть проблемы состоит в том, что одно и то же устройство или программное обеспечение может быть настроено так, чтобы обеспечивать кибербезопасность и не допускать кибератаки, а может быть настроено по-другому, т.е. способствовать кибератакам. Отличие исключительно в настройках. Нельзя выявить проблему путем каких-то

периодических осмотров оборудования. Требуется привлечение специально обученных специалистов.

Важно также обеспечить независимые от цифровых подсистем элементы защиты и управления, независимым оперативным током

Мероприятия по повышению кибербезопасности цифровых подстанций и объектов электроэнергетики в целом:

– разделение информационных потоков различных подсистем на физически не связанные сегменты коммуникационных сетей передачи данных внутри подстанции, т.е. предлагается создание независимых друг от друга шин процессов и шин объектов для каждой функции автоматического или автоматизированного управления, требующей повышенной надежности;

– отказ от монотехнологичности в коммуникационных сетях передачи данных внутри подстанции (чтобы Ethernet и TCP/IP не были единственными коммуникационными технологиями цифровой подстанции);

– применение симплексных каналов с односторонней передачей информации там, где это достаточно для выполнения прикладной функции, например, односторонняя передача информации от цифрового ТТ (ТН) к устройствам РЗА, исключающая возможность кибератаки на сам ТТ (ТН) от неисправного устройства РЗА и т. д.

Поскольку в настоящее время инженеры-релейщики не имеют ни одного руководства для решения любой из обозначенных проблем, они должны обратиться к изучению ряда стандартов и отчётов с информацией об основополагающих требованиях, кодифицированных в ISA 01.01.99 и к отчёту рабочей группы Исследовательского комитета B5 СИГРЭ.

В связи с внедрением глобальных распределённых систем мониторинга, защиты и управления (WAMS, WAPS, WACS) должна быть решена задача помехоустойчивого приёма сигнала ГННС, обеспечивающего возможность векторных измерений пространственно разнесённых устройств с высокой точностью синхронизации.