

Человеческий фактор при обеспечении кибербезопасности объектов электроэнергетики



А.Б. Осак, Д.А. Панасецкий, Е.Я. Бузина
ИСЭМ СО РАН, г. Иркутск
osakalexey@mail.ru

Проблема

Важно отметить, что основной упор в разрезе кибербезопасности делается на вирусную стойкость и устойчивость к сетевым атакам различного вида.

Стандарты и подходы к кибербезопасности нам говорят о логическом разделении потоков на уровне маршрутизаторов (firewall, VLAN), контроле доступа, шифровании, тестировании на кибератаки и т.п.

Все это хорошо работает только, если все это правильно спроектировано и правильно настроено. Кроме того, в программном обеспечении всех коммуникационных устройств **не должно быть ошибок.**

В теории, **все должно быть идеальным.** Но не утопия ли это?

Проблема

Традиционные подходы к кибербезопасности электроэнергетических объектов, в том числе для цифровых подстанций, основаны на **предположении о 100% адекватности, квалифицированности, внимательности, дисциплинированности, честности, лояльности от всех сотрудников**, в том числе производителей, проектировщиков, наладчиков и эксплуатационных организаций.

Но, если активное сетевое оборудование и системы контроля доступа заведомо настроить неправильно, то с любой точки планеты **можно будет буквально за несколько минут нарушить функциональной любого энергообъединения**, даже такого масштабного, как ЕЭС России (ЕЭС/ОЭС). В традиционной энергетике, хотя бы расстояния выполняли роль барьера.

Проблема

Можно отметить, что при построении цифровых подстанций на основе стандарта МЭК 61850 возникает **системное противоречие**:

- предлагается существенно упростить физическую (аппаратную) часть цифровой подстанции
- за счет принципиального усложнения алгоритмической и программной частей.

Ослабление кибербезопасности является неизбежным следствием **увеличения объема системного и коммуникационного программного обеспечения**, которое раньше выполняло вспомогательные функции, а теперь станет ключевым элементом цифровой подстанции.

Слабое звено

Ключевыми элементами, которые могут быть подвержены кибератаке с последующим нарушением функционирования цифровой подстанции являются:

- **внешние цифровые каналы**, по которым осуществляется технологическая и оперативная связь с другими энергообъектами и диспетчерскими пунктами;
- **коммуникационные сети энергообъекта**, включая коммутаторы и маршрутизаторы;
- **шины процессов и шины объектов** (в соответствии с МЭК-61850), которые в цифровой подстанции являются неотъемлемыми элементами любой функции РЗА, ПА, мониторинга и оперативного управления.

Угрозы

В качестве возможных угроз (возмущающих факторов) с позиции кибербезопасности для цифровых подстанций можно отметить следующие:

- **Кибератаки извне**, через внешние цифровые каналы связи энергообъекта.
- **Невыявленные ошибки** в программном обеспечении устройств цифровой подстанции.
- **Злонамеренные программные дефекты** (закладки), встроенные в программное обеспечение микропроцессорных устройств цифровой подстанции, с целью управляемого вывода из строя системы.
- **Ошибки оперативного и эксплуатационного персонала** энергообъекта.

Способы повышения надежности

В традиционных подстанциях основными средствами повышения надежности и живучести являются:

- **дублирование** – установка нескольких одинаковых устройств;
- **функциональное резервирование** – реализация одинаковых или схожих функций с использованием разных физических принципов;
- **декомпозиция** – разделение различных функций между разными устройствами, физическое разнесение кабелей и устройств, выделение отдельных кернов для разделения цепей разных устройств;
- **упрощение** – применение простых, понятных и однозначных алгоритмов управления.

Способы повышения надежности

Для обеспечения надежности и живучести цифровых подстанций применяют только:

- **дублирование** устройств;
- **дублирование** сетей и каналов связи;
- **функциональное резервирование и декомпозиция** исключительно на уровне **электроэнергетических функций**, но не на уровне цифровых технологий.

Угрозы снижения надежности

При переходе от традиционных подстанций к цифровым на основе МЭК-61850 произойдет отказ от следующих принципов:

- **отказ от функционального резервирования**, т.к. коммуникационные сети (включая коммутаторы и маршрутизаторы) работают на одном и том же принципе;
- **отказ от декомпозиции**, т.к. коммуникационные сети (включая коммутаторы и маршрутизаторы), обеспечивающие шины процессов и шины объектов, выполняют функции доставки информации до любых устройств мониторинга и управления;
- **отказ от упрощения**, т.к. алгоритмы передачи и обработки цифровой информации по коммуникационным сетям достаточно сложны.

Человеческий фактор

Ключевой проблемой является то, что одно и то же устройство или программное обеспечение **может быть настроено так**, чтобы обеспечивать кибербезопасность и недопускать кибератаки, а **может быть настроено по-другому**, т.е. способствовать кибератакам.

Внешний вид устройств при этом не меняется, однако их функциональность в части кибербезопасности принципиально разная.

Отличие исключительно в настройках, причем **отличаться может незначительное число параметров** из тысячи совпадающих.

Неспециалист в вопросах кибербезопасности вообще **не сможет выявить проблему** путем каких-то периодических осмотров оборудования.

Значит, **требуется привлечение специально обученных специалистов**, которые способны решать подобные задачи.

Человеческий фактор

Вероятность целенаправленных кибератак зависит главным образом от двух составляющих:

- **«Цена услуг» взлома;**
- **Масштаб последствий.**

Чем выше негативный масштаб последствий, тем большую цену будет готов заплатить потенциальный заказчик кибератаки.

При большой цене за «услуги взлома» решающую роль будет играть лояльность специалистов.

Соответственно масштаб последствий, по сути, и определяет вероятность серьезной кибератаки.

Человеческий фактор

Соответственно, важнейшим требованием к специалисту по кибербезопасности является **требование правильного и добросовестного выполнения своих обязанностей.**

Однако, учитывая масштаб последствий, а также то, что заинтересованными сторонами в кибератаке могут быть иностранные государства, на первый план выходят **вопросы политической и бизнес лояльности, патриотизма, эффективности спецслужб** и т.п. То есть вопросы, выходящие за рамки техники и энергетики.

Можно говорить о том, что любая **цифровая подстанция должна превращаться в некий закрытый и секретный объект**, наподобие военных и ядерных объектов, со всеми вытекающими затратами.

Готов ли электроэнергетический бизнес к такому?

Наши предложения

Альтернативным путем является **пересмотр структурной и функциональной схем цифровых подстанций** таким образом, чтобы в принципе исключить многие из потенциально возможных киберугроз.

Например, традиционные электромеханические реле, традиционные устройства вторичных коммутаций не подвержены кибератакам в виду отсутствия какой-либо цифровой части.

Поэтому некоторое **совмещение цифровых, аналоговых и механических устройств** может являться простым и **эффективным средством обеспечения кибербезопасности**, причем полностью понятным электроэнергетикам.

Эшелонированная РЗА и ПА (защита от киберугроз)

Эффективные цифровые РЗА и ПА (основные и резервные защиты, ближнее и дальнее резервирование), в т.ч. вовлеченные в централизованное иерархическое управление, имеющие дистанционное управление (подвержены киберугрозам)



Обеспечение минимального уровня функционирования ЭЭС (действующие при отказе или отключении цифровых РЗА и ПА): классические и надежные РЗА и ПА, реализованные на автономных микропроцессорных терминалах, м.б. с повышенными уставками по времени



Обеспечение физической сохранности оборудования при повреждениях (реализация на самой простой и надежной базе, даже на электромеханической базе, в т.ч. газовые и дуговые защиты, МТЗ по термической стойкости оборудования и т.п.)

Наши предложения

Авторами предлагаются следующие мероприятия по повышению кибербезопасности цифровых подстанций и объектов электроэнергетики в целом:

- **Разделение информационных потоков** различных подсистем на разные, 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 (отдельные виды РЗ, ПА, мониторинга и т.п.);
- **Отказ от монотехнологичности в коммуникационных сетях** передачи данных внутри подстанции, т.е. чтобы Ethernet и TCP/IP не были единственными коммуникационными технологиями цифровой подстанции;

Наши предложения

- **Создание выделенных сегментов коммуникационных сетей, использующих для настройки и переконфигурирования микропроцессорных и коммуникационных устройств, причем в процессе эксплуатации данные сегменты должны быть нормально отключенными** (снято питание с коммуникационных устройств или разобраны разъемы);
- Применение для выполнения ответственных функций управления **узкоспециализированных протоколов обмена информации**, позволяющих передавать только ту информацию, которая нужна для решения конкретной задачи, и **не позволяющие передавать что-либо иное**. Это должно быть сделано, в том числе, и с целью принципиального упрощения алгоритмов коммуникационных устройств.

Наши предложения

- **Применение симплексных каналов** с односторонней передачей информации там, где это достаточно для выполнения прикладной функции, с применением циклических или спорадических протоколов передачи информации, взамен дуплексных с передачей информации по запросу.
- Реализация исключительно только симплексных каналов с **односторонней передачей информации на цифровых трансформаторах тока и напряжения;**
- Для выполнения этого предложения можно рассмотреть варианты либо **установки** на передающих устройствах **множества симплексных портов** для передачи информации, либо создание технологии **передачи по симплексному каналу информации от одного передатчика до множества приемников.**

Наши предложения

- Применение **межсетевых экранов**, разделяющих различные сегменты коммуникационных сетей, которые **на физическом уровне не позволяют выполнять несанкционированные функции**, например, аналоговый способ разделения информации. Сегодня межсетевые экраны реализуются на уровне программного обеспечения, соответственно неправильная настройка программного обеспечения может привести к логическому объединению разных сетей;
- По существу, межсетевой экран должен представлять собой **два независимых полукомплекта, связанных между собой аналоговым или цифровым каналом с простым протоколом обмена**. Тогда хакерский взлом одного полукомплекта со стороны одной коммуникационной подсети не позволит получить несанкционированный доступ к другой коммуникационной подсети.

Наши предложения

- Создание специализированных коммутаторов, состоящих из двух полуккомплектов, связанных между собой только аналоговыми связями, в цепях которых установлены традиционные ключи, позволяющие оперативно размыкать цепи. Один полуккомплект подключается к одной коммуникационной подсети, и, например, получает GOOSE сообщения от устройств своей подсети, а другой полуккомплект транслирует заданные GOOSE сообщения в другую коммуникационную подсеть. Тогда можно будет **в оперативном порядке гарантированно отключить передачу конкретного GOOSE сообщения из одной подсети в другую**. Учитывая, что коммутация цепей будет происходить в рамках одного шкафа, то коммутируемые цепи могут быть выполнены на низком напряжении, что позволит сделать подобное устройство более компактным, чем традиционные панели управления.

Организационные проблемы

С позиции кибербезопасности, функционал микропроцессорного устройства цифровой подстанции определяется исключительно его программным обеспечением. Соответственно **сертификат соответствия должен быть на конкретную аппаратную версию и конкретную программную прошивку устройства.**

Учитывая общую сложность цифровых технологий и применяемых алгоритмов цифровой коммуникации, необходимо обратить внимание на **персональное лицензирование конкретных специалистов.** Сейчас допуск на определенные виды работ выдается организации в целом, а необходимо этот допуск давать конкретным специалистам, без привязки к организации, тогда существенно повышается персональная ответственность специалиста, и снижается возможность административного давления. Следует отметить, что подобный способ лицензирования специалистов успешно применяется в США.

Выводы

Необходимо, чтобы новые цифровые технологии повышали, а не снижали кибербезопасность электроэнергетических объектов и систем.

Поднятые в докладе вопросы – это еще не решение всех проблем.

Мы предлагаем активизировать дискуссию.