УДК 621.3

Влияние кибербезопасности объектов электроэнергетики на надёжность функционирования электроэнергетических систем

Плешко Д.Ю.
Научные руководители – к.т.н., доцент БЛАДЫКО Ю.В.,
ст. препод. САПОЖНИКОВА А.Г.

Вопросы кибербезопасности современных электроэнергетических объектов, оснащенных цифровыми системами мониторинга, управления, релейной защиты и противоаварийной автоматики, становятся очень актуальными в виду новизны проблемы. На построенных в последние годы объектах, весь функционал устройств релейной защиты (РЗА), противоаварийной автоматики (ПА) и автоматизированного диспетчерского управления сосредотачивается на объединяемых единой цифровой информационной сетью компьютерных подсистемах энергообъекта: микропроцессорных терминалах РЗА и ПА, автоматических системах управления технологическими процессами (АСУ ТП).

Необходимо рассмотреть влияние надежности цифровых подсистем, их кибербезопасности на общую надежность отдельных энергообъектов и электроэнергетических систем (ЭЭС) и их объединений. В большинстве публикаций и нормативных документах, посвященных вопросам кибербезопасности объектов электроэнергетики, основным способом ее обеспечения видится применение соответствующих технических средств, которые обеспечивают требуемую защиту от различных несанкционированных действий. Авторы, не отрицая необходимость применения специальных технических средств обеспечивающих кибербезопасность, предлагают сосредоточить внимание на человеческий фактор, как основную угрозу кибербезопасности, так как именно человек (сотрудник энергопредприятия, сотрудник поставщика и подрядчика, или стороннее лицо) является основной причиной потенциальной киберугрозы.

Надежность электроэнергетической системы обеспечивается двумя категориями.

Первая – надежность функционирования всей производственной цепочки: производство электроэнергии, ее транспорт и распределение до электроустановок потребителей. Ключевая роль здесь отводится надежности основного электроэнергетического оборудования, которая обеспечивается соответствующими мероприятиями на этапах жизненного цикла (проектирования, производства, монтажа, наладки, эксплуатации).

Вторая – адекватность и эффективность управления. Известно, что функционирование ЭЭС возможно только при соответствующем непрерывном управлении, как отдельными электроустановками, так и ЭЭС вцелом.

Цифровые технологии, микропроцессорная техника со значительными вычислительными ресурсами позволяют создавать в рамках ЭЭС достаточно сложные и совершенные алгоритмы управления как в рамках оперативно-диспетчерского управления нормальными режимами, так и противоаварийного управления. Это в сочетании с новым поколением первичного оборудования, имеющим высокие эксплуатационные характеристики, и обладающим возможностями мониторинга и управления, позволяет повысить общую надежность ЭЭС.

С другой стороны, цифровым технологиям и микропроцессорной технике свойственна возможность резкого изменения своего функционала путем перепрограммирования, которая, при правильном применении, позволяет совершенствовать технологии и алгоритмы управления без замены оборудования. Но именно это и является основой новых видов угроз для ЭЭС – угроз кибербезопасности.

Киберугрозы по своей сути – это выполнение непредусмотренных функций: от несанкционированной передачи информации третьим лицам, до выполнения зловредных функций, что есть по сути частичный или полный отказ системы управления энергообъектом.

В качестве возможных угроз (возмущающих факторов) с позиции кибербезопасности

для современных электроэнергетических объектов можно отметить следующие:

– невыявленные ошибки в программном обеспечении, вследствие чего информационные и управляющие системы энергообъекта работают по неверному алгоритму;

– злонамеренные программные дефекты (закладки), встроенные в программное обеспечение микропроцессорных устройств энергообъекта, с целью управляемого вывода из строя системы;

– кибератаки извне, через внешние цифровые каналы связи энергообъекта, путем перехвата каналов телемеханики и телеуправления, каналов общекорпоративного управления или встраивания зловредного программного кода в объектовые системы управления;

– ошибки оперативного и эксплуатационного персонала энергообъекта, которые приводят к снятию систем защиты внешних каналов связи, к замене программного обеспечения на непроектный вариант, к заражению вирусами и др.

Средствами повышения надежности и живучести являются:

– дублирование – установка нескольких одинаковых устройств;

– функциональное резервирование – реализация одинаковых или схожих функций с использованием разных физических и алгоритмических принципов;

– декомпозиция – разделение различных функций между разными устройствами, физическое разнесение кабелей и устройств;

– упрощение – применение простых, понятных и однозначных алгоритмов управления (снижается вероятность ошибок).

При переходе от традиционных энергообъектов к цифровым на основе МЭК-61850 происходит отказ от следующих принципов:

– отказ от функционального резервирования, т.к. коммуникационные сети (включая коммутаторы и маршрутизаторы), которые являются ключевыми в цифровых технологиях, работают на одном и том же принципе;

– отказ от декомпозиции, т.к. одни и те же коммуникационные сети (включая коммутаторы и маршрутизаторы), обеспечивающие шины процессов и шины объектов, выполняют функции доставки информации до всех устройств мониторинга и управления;

– отказ от упрощения, т.к. алгоритмы передачи и обработки цифровой информации по коммуникационным сетям сложны.

Для обеспечения надежности и живучести цифровых энергообъектов применяют только дублирование устройств, дублирование сетей и каналов связи, функциональное резервирование и декомпозицию исключительно на уровне прикладных электроэнергетических функций, но не на уровне цифровых технологий.

В тоже время, коммуникационные сети и микропроцессорные устройства цифровых энергообъектов универсальны, и без существенной модернизации могут решать любые информационные задачи, например, выполнять заведомо зловредные функции в процессе кибератаки, чего нельзя сказать об устройствах на традиционных подстанциях (особенно на электромеханической базе).

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

– 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;

– цифровые устройства РЗА, ПА, управления и мониторинга электрооборудованием;

– внешние цифровые каналы, по которым осуществляется технологическая и оперативная связь с другими энергообъектами и диспетчерскими пунктами.

Если все устройства РЗА, ПА, системы управления первичным оборудованием будут выполнены на цифровой базе и будут объединены в единую информационно-управляющую систему, то результатом кибератаки может быть полная потеря управляемости

энергообъектом или заведомо ложное управление. В результате кибератаки возможна даже «перепрошивка» цифровых устройств или удаление на них системного и прикладного программного обеспечения. В последнем случае для восстановления работоспособности потребуется полный цикл пусконаладочных работ длительностью до нескольких месяцев.

Если несколько смежных подстанций подвергнется целенаправленной кибератаке, то вполне возможны случаи полного обесточивания значительной группы потребителей (включая ответственных). Также возможны случаи повреждения дорогостоящего первичного оборудования вследствие неустраненного КЗ или длительной неустраненной перегрузки. При этом классические средства дальнего резервирования на смежных цифровых подстанциях могут быть также неработоспособны по все той же причине.

Традиционные подходы к кибербезопасности электроэнергетических объектов, в том числе, для цифровых подстанций, основаны на предположении о полной адекватности, квалифицированности, внимательности, дисциплинированности, честности, лояльности 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 функционирование любого энергообъединения, даже такого масштабного, как ЕЭС России (ЕЭС/ОЭС). В традиционной энергетике, хотя бы расстояния между энергообъектами играли роль защитного барьера.

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 и общей надежности цифровых энергообъектов, является неизбежным следствием увеличения объема универсального системного и коммуникационного программного обеспечения, которое раньше выполняло вспомогательные функции, а теперь станет ключевым элементом цифровой подстанции.

Поэтому можно констатировать, что проблема кибербезопасности объектов электроэнергетики становится ключевым элементом общей надежности ЭЭС. При этом в текущее время эта проблема явно недооценена и часто не принимается во внимание.

Как бы не совершенствовались в устойчивости к кибератакам программные и аппаратные средства, выполняющие прикладные и коммуникационные функции на цифровых подстанциях, и какие бы дополнительные специальных технические средства не применялись для защиты от кибератак, все это не решает проблему человеческого фактора.

В нынешнее время вопросы кибербезопасности уже перешли из области только технических проблем, и перешли в область политики и межгосударственных отношений. При этом киберугрозы могут быть совершенно различными, при этом объектом первичных атак могут быть общекорпоративные информационные сети, которые в той иной степени соприкасаются с технологическими и производственными сетями.

Ключевой проблемой кибербезопасности является то, что одно и тоже 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. 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. Дилетант в вопросах кибербезопасности вообще не сможет выявить проблему путем каких-то периодических осмотров оборудования. Более того, есть риск создания уязвимостей как раз во время выполнения планово-предупредительных ремонтов, обслуживания, перенастройки и наладки оборудования. Поэтому, требуется привлечение специально обученных специалистов, которые способны решать задачи кибербезопасности на объектах электроэнергетики.

Вероятность целенаправленных кибератак зависит главным образом от двух

составляющих: цены «услуг взлома» и масштаба последствий. Чем выше негативный масштаб последствий, тем большую цену будет готов заплатить потенциальный заказчик кибератаки. Электроэнергетика является ключевой инфраструктурной отраслью для современного государства и общества, является необходимой основой для всех других инфраструктурных отраслей. Соответственно можно ожидать, что потенциальный заказчик может заплатить очень большую цену для решения своих задач (коммерческих или даже геополитических).

При большой цене за «услуги взлома» решающую роль будет играть лояльность специалистов. Соответственно, масштаб последствий, по сути, и определяет вероятность серьезной кибератаки.

Поэтому, 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. Если ничего не предпринимать, то 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. Но готов ли электроэнергетический бизнес к такому?

В реальности в настоящее время вообще полностью отсутствует какой-то значимый контроль на предмет кибербезопасности цифровых и программных прикладных технических средств в электроэнергетики. Максимум, что есть – это антивирусная защита компьютеров.

Поэтому с позиции надежности можно принимать возможность успешной кибератаки тем или иным способом как минимум: на одну технологическую подсистему, находящуюся в одной информационной сети; на один тип цифровых устройств/систем (если это связано с предусмотренной на заводе особенностью или невыявленной ошибкой); на все оборудование, обслуживаемое одним специалистом.

С учетом вышесказанного можно сделать вывод о том, что унификация и централизация приводит к снижению кибербезопасности, как минимум за счет потенциально возможного подкупа специалистов. Соответственно повышение кибербезопасности, и как следствие общее повышение надежности (с позиции последствий кибератак) может быть обеспечено только за счет правильно организованной структуры управления в электроэнергетике. Когда единичный взлом или единичный подкуп специалистов не приводит к масштабной аварии в ЭЭС с серьезными, особенно долго устранимыми последствиями.