Энергетика. Автоматика

УДК 620.9: 004.41/.42

О.М. Лисица

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНЫХ СЕТЕЙ

Цель статьи – освещение вопроса информационной безопасности современных интеллектуальных электроэнергетических систем в связи с тем, что в последнее время все больше распространяются подстанции, оснащенные различными цифровыми устройствами. Рассмотрены существующие проблемы в этой области и предложены пути их решения.

Ключевые слова: информационная безопасность, кибербезопасность, энергосистема, интеллектуальная сеть.

INFORMATION SECURITY INTELLIGENT NETWORK

The purpose of this article is to highlight the issue of information security advanced intelligent electric power systems due to the fact that more and more subject to the substation, with a variety of digital devices are wide spread recently. The existing problems in this area and suggested ways of solution were discussed.

Key words: information security, cyber security, power grid, smart grid.

Введение

Одним из приоритетных направлений развития в сфере электроэнергетики является внедрение цифрового оборудования и программно-аппаратных средств, в том числе разработка подстанций нового типа – цифровых подстанций, и в целом создание интеллектуальных сетей (Smart Grid).

Предпосылкой для создания таких сетей, без всякого сомнения, послужило распространение компьютерных технологий, повсеместное использование сети Интернет.

Эти тенденции присущи не только российской, но и мировой электроэнергетике. Повсеместно ведется активная работа над созданием модернизированных электроэнергетических сетей. Развитие данных технологий стало столь популярно потому, что они имеют большое количество преимуществ. Среди них выделяют повышенную надежность, качество, экономичность и экологичность.

Но так ли надежны эти сети? Ведь там, где имеются цифровые устройства, появляется и угроза информационной безопасности, или, как еще говорят, кибербезопасности. Возможны несанкционированные воздействия на аппаратуру, проникновение внешних сигналов, затрудняющих работу как отдельных сетей, так и электроэнергетической системы в целом. А так как электроэнергетика является отраслью национального хозяйства и играет значительную роль в жизни каждого человека, разработка мер для соблюдения информационной безопасности, несомненно, является серьезной задачей.

Проблема информационной безопасности

Новейшие энергетические объекты могут быть подвержены различным угрозам – таким как дефекты в программном обеспечении микропроцессорных устройств, кибератаки на энергооборудо-

вание через внешние каналы связи. А элементы, склонные к выходу из строя при этих процессах, – коммутаторы, маршрутизаторы, шины процессов и объектов, различные цифровые каналы связи и устройства релейной защиты и автоматики.

Основными средствами защиты являются антивирусы и межсетевые экраны. Первые представляют из себя программное обеспечение определенного типа, установленное на компьютере и помогающее обнаружить вредоносные программы. Вторые же позволяют создавать соединение только между заданными объектами, т.е. являются некими фильтрами.

Существует протокол МЭК 61850 (IEC 61850), в котором описаны требования к системам передачи данных на энергообъектах. В нем содержатся разделы, посвященные информационной безопасности.

Для защиты данных в этом стандарте предполагается применять цифровые подписи и шифрование [3].

Цифровая подпись подтверждает целостность и подлинность входящих сообщений и определяет, были ли отправлены эти данные из правильного источника. Чтобы определить, верен ли отправитель, перед началом работы формируется и высылается сертификат электронной подписи, т.е. некий документ, содержащий открытый ключ и всю необходимую о нем информацию. Далее осуществляются контроль и использование ключа для проверки поступающей информации.

Шифрование – это преобразование каких-либо данных для того, чтобы они в итоге могли быть прочитаны только определенными лицами.

Но, к сожалению, вопросы информационной безопасности, описанные в протоколе МЭК 61850 и иных нормативно-правовых документах, находятся в зачаточном состоянии, не говоря уже о реализованных технических решениях и технологиях. Об этом свидетельствует даже статистика инцидентов информационной безопасности по отраслям, энергетика занимает здесь ведущее место [2].

К чему может привести организованная кибератака на энергообъект? Если, например, какой-либо вирус изменит параметры работы цифровых устройств или вовсе удалит программное обеспечение, то восстановление работоспособности может занять несколько дней, недель, даже несколько месяцев. А это может обернуться отключением значительного числа потребителей различных групп.

Еще одной причиной нарушения информационной безопасности называют человеческий фактор. Сотрудники, работающие на местах, могут, сами того не зная, способствовать распространению вредоносных программ путем использования зараженных карт памяти, открытия электронных писем и сообщений с вирусами. Но, по данным исследований, человеческий фактор является все же далеко не главным и занимает меньшую долю среди угроз информационной безопасности [2].

Многие вопросы кибербезопасности интеллектуальных сетей еще не изучены. Но об этом задумываются и пытаются решить их различными способами. Проводятся не только форумы и конференции, на которых обсуждают данные проблемы, уже несколько лет подряд организуются конкурсы информационных технологий для молодых специалистов. Им предлагается «взломать» цифровую подстанцию [1]. На основе полученных результатов можно увидеть слабые места, уязвимости в защите и работать над их устранением.

Еще одной проблемой, которая требует решения, является квалифицированный персонал. В идеале это должны быть люди с профильным образованием и в сфере электроэнергетики, и в сфере информационных технологий. Каждая организация, использующая элементы интеллектуальных сетей, должна иметь такого специалиста.

Заключение

Проблема информационной безопасности в современных интеллектуальных сетях существует на нескольких уровнях, ее необходимо решать как можно быстрее, так как модернизированное обо-

рудование уже появляется на энергообъектах, а цифровая подстанция – не далекое будущее, а текущая реальность.

Прежде всего следует усовершенствовать нормативно-техническую документацию, а также модернизировать проектирование и производство устройств с учетом средств безопасности. На предприятиях, где вводится новое цифровое оборудование, необходимо проводить технику информационной безопасности для всех сотрудников и привлекать специалистов в области информационных технологий.

1. Kaspersky Industrial CTF Quals [Электронный ресурс] – URL: http://kaspersky-industrial-ctf.ru / contests/194/

2. Киберугрозы систем управления современной электрической подстанции [Электронный ресурс] – URL: http://www.slideshare.net/phdays/nikandrov-ph-days-iv-rev27

3. Проблемы информационной безопасности подстанции и способы их решения [Электронный ресурс] – URL: http://digitalsubstation.ru/blog/2016/02/17/problemy-informatsionnoj-bezopasnosti-podstantsii-i-sposoby-ih-resheniya/

УДК 620.9 (075.8)

В.Г. Гаврилов, А.Н. Козлов

ПОТЕНЦИАЛ ВОЗОБНОВЛЯЕМЫХ ИСТОЧНИКОВ ЭНЕРГИИ В АМУРСКОЙ ОБЛАСТИ

В статье проведен анализ потенциала возобновляемых источников энергии на территории Амурской области с целью определить наилучший вариант развития данной отрасли.

Ключевые слова: возобновляемые источники энергии, топливно-энергетический комплекс, гелиоэнергетика, ветроэнергетика, гидроэнергетика, биоэнергетика.

POTENTIAL OF RENEWABLE ENERGY SOURCES IN THE AMUR REGION

The renewable energy sources potential in the Amur region is analyzed in this article in order to determine the best way of development of this industry.

Key words: renewable energy, fuel and energy sector, solar power, wind power, hydropower, bioenergy.

Лишь в последние годы в России начинают вплотную заниматься развитием производства энергии на основе возобновляемых источников (ВИЭ). В основном это касается регионов автономного энергоснабжения, где осуществляется строительство солнечных и ветряных электростанций с целью экономии дизельного топлива. Развитие ВИЭ будет способствовать решению следующих основных проблем:

1) тепло- и электроснабжение населения и промышленности в зонах децентрализованного энергоснабжения, в первую очередь в северных районах;