Иван Лопухов

Интеллектуальные электрические сети под угрозой

В статье поднимается вопрос об уязвимости сетей Ethernet на объектах энергетики перед вредоносными действиями компьютерных вирусов. Приводятся реальные примеры, иллюстрирующие данную проблему, проводится обзор программных и аппаратных средств, повышающих кибербезопасность сетей Ethernet.

О текущем положении

Термин *smart grid*, который дословно можно перевести как «интеллектуальные электрические сети», пока во многом условен – принятие соответствующих международных стандартов ещё в процессе. И пока все участники процесса согласования не пришли к единому знаменателю, ясно лишь то, что понятие *smart grid* определяет новые методы производства, передачи, распределения и потребления электроэнергии [1].

При реализации интеллектуальных электрических сетей важным моментом является взаимодействие основных автоматизированных компонентов. Устройства, измеряющие электрические параметры, должны обмениваться с управляющими устройствами в реальном времени на всех участках сети от генерирующих станций до конечных потребителей. Все устройства автоматизации должны быть связаны на программном уровне SCADA-системами, а эти системы, в свою очередь, обмениваться данными друг с другом.

Все соединения и линии передачи данных требуют открытых коммуникационных систем, таких как Ethernet и Internet. Это особенно важно при проектировании новых и модернизации старых систем. Использование открытых систем позволяет снизить расходы на оборудование и программные компоненты по следующим причинам [1]:

- аппаратное и программное обеспечение в открытых системах дешевле, так как базируется на открытых, а не собственных технологиях производителей;
- процесс инсталляции протекает с использованием знакомых инструментов и приёмов, более распространённых, чем аналоги для закрытых систем;
- возможно использование существующей инфраструктуры и оборудования, что может серьёзно снизить конечную стоимость системы;
- открытые протоколы обладают более низкой стоимостью интеграции за счёт широкого распространения;
- проще подобрать квалифицированный персонал для интеграции и обслуживания компонентов открытых систем.

Итак, открытые коммуникационные системы гораздо привлекательнее закрытых с точки зрения снижения стоимости конечной системы, однако они не лишены недостатков. Само их название наталкивает на мысль о большей уязвимости к кибератакам. В частности, этому способствуют следующие факторы [1]:

- большое число внутренних связей в системе создаёт больше потенциальных возможностей для атак;
- хакеры лучше знакомы с открытыми сетевыми протоколами;
- сервисы, основанные на Web-браузерах, создают возможные точки входа;
- рабочие станции с ОС Windows обладают известными «дырами» в системах безопасности;
- стек протоколов TCP/IP также обладает известной степенью уязвимости.

Очевидно, что сетевые атаки на коммуникационные сети могут нарушить работоспособность всех систем, генерирующих, передающих и распределяющих электроэнергию по потребителям. Поэтому важным понятием для открытых коммуникационных систем является кибербезопасность – способность систем противостоять сетевым атакам.

Сетевая безопасность подразумевает ограничение доступа с использованием как аппаратных средств (управляемых коммутаторов Ethernet, межсетевых экранов, шлюзов данных), так и программных средств. Программно-аппаратный комплекс должен работать по определённым правилам и соответствовать требованиям определённых стандартов. К сожалению, до сих пор большинство таких стандартов только на пороге принятия. Поэтому в одних существующих системах кибербезопасность реализована по собственным планам создателей с использованием доступных компонентов, в других же применяется принцип «сидеть и ждать», который хорош до первой кибератаки. Понимание текущего положения вещей в интеллек-

туальных электрических сетях – первый этап на пути к кибербезопасности.

Обзор электрических сетей

Как видно из мировой практики, большинство существующих распределительных сетей работает по централизованному принципу. Энергия вырабатывается на генерирующих подстанциях и далее через сети передающих и распределительных станций доставляется конечным потребителям. Подстанции являются интеллектуальными узлами этой сети. Линии передачи между генерирующими и распределительными станциями требуют непрерывного контроля в реальном времени. Основной задачей для подстанций является постоянное поддержание баланса между генерируемыми и потребляемыми мощностями, особенно в случае с возобновляемыми и распределёнными источниками энергии. Примеры таких источников – ветряки и солнечные батареи. Величина вырабатываемой ими энергии постоянно и непредсказуемо меняется, источники энергии распределены на большой территории.

Множество распределительных сетей контролируется устаревшими системами автоматизации, имеющими весьма ограниченные средства защиты от кибератак. Такие закрытые нестандартизированные системы автоматизации обычно интегрированы со SCADA-системой (рис. 1), использующей открытые коммуникационные каналы для передачи данных. Сети smart grid предполагают тотальное использование открытых сетей Real-Time с высокой пропускной способностью для мониторинга и контроля производимой и потребляемой энергии. Однако использование открытых протоколов типа Ethernet связано с серьёзной проблемой – уязвимостью перед несанкционированным доступом.

Определённой уязвимостью обладают и сами SCADA-системы. Многие слышали про «дыры», обнаруживаемые в системе безопасности различных версий ОС Windows, и про выпускаемые компанией Microsoft «заплатки» для их ликвидации. SCADA-системы занимают куда более узкий сегмент рынка, потому их взлом является существенно более редким событием. Тем не менее, прецеденты уже имеются.

Уязвимость SCADA-систем

Чуть больше года назад сразу 13 уязвимых мест было обнаружено в SCADA-системах ICONICS GENESIS32 и GENESIS64. Данное программное обеспечение (ПО) популярно в российских объединённых генерирующих компаниях, установлено на нескольких гидроэлектростанциях и многих объектах, не относящихся к энергетике.

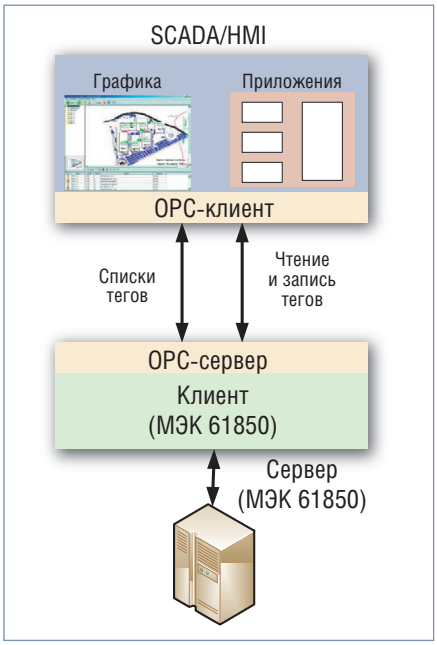

Рис. 1. Интеграция SCADA в систему автоматизации подстанции

Модуль GenBroker версий GENESIS32 9.21 и GENESIS64 10.51 (а также более ранних) содержал ряд «дыр», связанных с освобождением памяти и целочисленным переполнением. Его разработчики довольно быстро отреагировали на это событие и рекомендовали не использовать удалённый доступ к системе из Internet, а также применять межсетевой экран. Через пару недель было выпущено обновление программного продукта, ликвидирующее обнаруженные уязвимости. Вредоносного ПО, использующего их, зарегистрировано не было.

SCADA-системы и кибератаки

Примером того, как кибератаки могут повлиять на системы автоматизации генерирующих, передающих и распределительных станций, служит вирус Stuxnet, появившийся в июле 2010 года. В отличие от предыдущих хакерских атак данный «червь» нацелен именно на промышленные системы автоматизации: SCADA-продукты, в частности Siemens WinCC, ПО для S7 и PCS7.

Stuxnet был способен получать специфическую информацию о технологическом процессе, вносить различные изменения в логику контроллеров и «заметать следы», пряча программные изменения от диагностического ПО. Так как множество объектов энергетики используют системы автоматизации производства Siemens, угроза от такого вредоносного ПО очевидна.

Вирус Stuxnet проникает в промышленную сеть через USB-ключ. Оказавшись внутри, «червь» использует как минимум 4 метода для заражения окружающих рабочих станций. Для запуска этого процесса достаточно простого чтения файлов в памяти USB-ключа.

Появление вируса стало возможным из-за нескольких известных «дыр» ОС Windows, а также системы паролей в ПО от Siemens. Stuxnet мог заражать компьютеры с разными версиями ОС: от старенькой Windows NT до современной Windows 7. Более двух недель с момента первого обнаружения вируса не было ни одного «патча» от Microsoft. Нет их и до сих пор для некоторых старых версий Windows. А ведь ещё до обнаружения вредоносное ПО могло работать от 1 до 6 месяцев. По разным оценкам вирус смог заразить от одной до нескольких сотен тысяч машин.

Изначально считалось, что цель написания вируса Stuxnet – промышленный шпионаж и кража интеллектуальной собственности из SCADA-систем и систем контроля технологических процессов. Последующий анализ показал, что суть действий вредоносного ПО – перехватывание контроля технологическим процессом и его саботаж. Зачем это нужно было авторам вируса – не совсем понятно; возможно, тому имелись какие-то политические мотивы.

Вирус был чрезвычайно опасен из-за двух моментов. Во-первых, он использовал доселе неизвестные «дыры» операционной системы Windows; во-вторых, это был первый «червь», направленный не на традиционные офисные сети, а именно на промышленные системы управления. Это означает, что с имеющимся «удачным» опытом хакеры теперь вполне способны атаковать промышленные системы автоматизации. Как вариант, части кода вируса Stuxnet могут быть взяты за основу для более масштабной атаки на предприятия энергетики. В связи с этим будущие атаки на системы автоматизации и контроля объектов энергетики уже не кажутся чем-то маловероятным, и шаги по их предотвращению должны быть предприняты заранее.

Кибербезопасность сегодня

Регулирование развития и совершенствования интеллектуальных электри-

ческих сетей smart grid происходит при поддержке Североамериканской корпорации по обеспечению надёжности электрических сетей NERC (**N**orth **A**merican **E**lectric **R**eliability **C**orporation). Цель этого процесса заключается в разработке и улучшении стандартов безопасности, мониторинге систем энергетики, обучении и сертификации персонала энергетической отрасли.

На сегодняшний день существует целый ряд стандартов, касающихся кибербезопасности. Это, прежде всего, NERC CIP [2]. Стандарты CIP (**C**ritical **I**nfrastructure **P**rotection) охватывают отчётность о случаях отказов систем, идентификацию киберугроз и действия по их устранению, вопросы управления безопасностью, физические средства её обеспечения, подготовку персонала. Свои инструкции опубликовала организация NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology) [3], а также самый известный «двигатель» стандартов – **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers (IEEE) [4].

В 2009 году в сенате США комитету по торговле, науке и транспорту был представлен отчёт федеральной комиссии по энергетике FERC (**F**ederal **E**nergy **R**egulatory **C**ommission). Основной его вывод заключался в том, что текущий уровень безопасности промышленных систем управления едва дотягивает до уровня коммерческих корпоративных систем 15-летней давности, а на трети объектов средства по предотвращению сетевых угроз не являются критически важными, поэтому нужно срочно пересмотреть сложившийся стиль обучения IT-персонала на предприятиях. По оценкам исследовательской компании Pike Research, до 2015 года на обеспечение безопасности энергетических сетей в мире будет потрачено около 200 миллиардов долларов.

Где же в структуре smart grid находятся средства обеспечения кибербезопасности?

Чтобы ответить на данный вопрос, надо, прежде всего, упомянуть интеллектуальные устройства автоматики (IED – **I**ntelligent **E**lectronic **D**evices) с подключением к Ethernet, обычно используемые на уровне подстанции. К ним относятся защитные реле, переключатели ответвлений под нагрузкой, автоматические выключатели, переключатели батарей конденсаторов, контроллеры автоматического повторного включения и регуляторы напряжения. IED-устройства подключаются к операторским терминалам, серверам данных, контроллерам и устройствам ввода/вывода. Стандарт IEEE 1686-2007 (Security for intelligent electronic devices – безопасность интеллектуальных устройств автоматики) устанавливает требования к IED-устройствам согласно NIRC CIP, определяя их функции и особенности. Также он содержит классификацию устройств по соответствию этим требованиям.

Помимо этого надо учитывать, что активное Ethernet-оборудование на подстанциях представлено шлюзами, коммутаторами, повторителями, мостами и прочим связным оборудованием. Из них строится сеть передачи данных между IED-устройствами. Поэтому ещё одним ключевым моментом кибербезопасности является контроль доступа к сети, который обеспечивается правильным выбором сетевого оборудования.

Как управляемые коммутаторы Ethernet влияют на безопасность

Простейший коммутатор Ethernet (рис. 2) выполняет 2 функции: коммутация пакетов в режиме Store&Forward и автосогласование скорости передачи. Управляемый коммутатор обеспечива-

ет необходимую для отказоустойчивых сетей дополнительную функциональность, составляющими которой выступают администрирование, фильтрация, приоритезация и управление трафиком и, наконец, сетевая диагностика и контроль доступа.

Фильтрация трафика обычно основана на типах трафика: широковещательный (broadcast), мультивещательный (multicast) и пр. Приоритезация необходима в мультисервисных сетях с одновременной передачей звука, видео и данных. К примеру, звук требует высокого приоритета, иначе разговор будет прерываться, или определённые данные могут иметь высокий приоритет для обеспечения условий реального времени.

Сетевая диагностика крайне актуальна для современных промышленных сетей, таких как сети электрических подстанций. Средства сетевой диагностики могут быть использованы для включения тревоги при изменении пропускной способности каналов. Если часть пакетов данных начала пропадать, это может означать частичное повреждение кабеля связи, которое скоро может повлечь обрыв. Ухудшение связи часто происходит из-за износа и повреждения кабеля, в частности, крысами или влагой. Поэтому мониторинг трафика можно считать превентивной мерой, направленной на предотвращение проблем со связью.

Современные промышленные управляемые коммутаторы, например, коммутатор Ethernet серии RSP компании Hirschmann для высоконадёжных сетей МЭК 61850 с функциями защиты от несанкционированного доступа, шифрованием, параллельным и кольцевым резервированием, сетевой диагностикой (рис. 3), также предоставляют функции защиты от несанкционированного доступа. Неиспользуемые порты можно отключать программным путём и даже настроить тревогу на срабатывание при попытке подключиться к ним. Подключения же к используемым портам можно ограничить списком разрешённых IP- и MAC-адресов, дополнительно настроив тревогу на срабатывание при появлении в сети непрописанного адреса.

Итак, управляемые коммутаторы помогают повысить безопасность сети предприятия. Однако, если сеть уже построена на сетевом оборудовании без функций ограничения доступа, замена всех активных устройств будет экономически невыгодна. Выходом в данной ситуации является сегментирование сети с помощью межсетевых экранов, которое к тому же служит дополнительной мерой защиты при использовании управляемых коммутаторов.

Межсетевой экран устанавливается между внутренней сетью подстанции и внешней сетью Internet. Устройство сканирует весь проходящий сетевой трафик, предотвращает неавторизованный доступ к сети, помогает анализировать производительность сети. Основная его цель – предотвращение неавторизированного подключения к внутренней сети извне. Также с помощью установленных правил можно контролировать весь поток данных между подсетями (см. врезку «Как защитить промышленную сеть подстанции с помощью межсетевого экрана EAGLE Tofino»).

Рис. 2. Неуправляемый коммутатор Ethernet EtherWAN EX47000 для автоматизации подстанций в соответствии со стандартом МЭК 61850

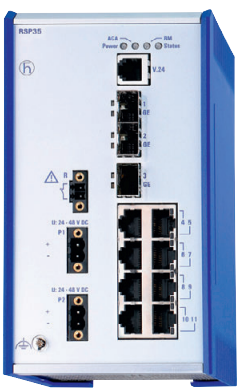

Рис. 3. Коммутатор Ethernet серии RSP компании Hirschmann

Ещё один фактор, повышающий безопасность сети – применение технологии VPN (Virtual Private Network). VPN – это виртуальная сеть из зашиф-

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

Lumineq – новое имя производителя электролюминесцентных дисплеев

Финская компания Beneq объявила о приобретении подразделения по производству и торговле электролюминесцентными дисплеями у компании Planar Systems (США), лидера в дисплейных технологиях для локальных цифровых видеосетей, используемых для демонстрации мультимедийной рекламы и информационных сообщений. Наименование нового подразделения компании – Lumineq. Это имя для Beneq связано с выпуском изделий по тонкоплёночной электролюминесцентной технологии (TFEL, Thin Film Electroluminescence) и промышленным производством продукции с применением технологии послойного атомного осаждения (ALD, atomic layer deposition). Указанная продукция дополнит номенклатуру изделий компании Beneq, получившей крупнейшие в мире производственные мощности по выпуску продукции на базе технологии ALD.

Компания Beneq, которая занималась производством оборудования на базе тонкоплёночной технологии, теперь будет предлагать услуги по нанесению покрытий и изготовлению изделий по техническим условиям заказчиков. Она взяла на себя обязательства по долговременному развитию линейки продукции Lumineq и ставит своей целью выпуск изделий для новых областей применения, которые являются коммерчески выгодными.

Beneq гарантирует существующим заказчикам Lumineq преемственность, стабильность и финансовую поддержку, необходимые для обеспечения непрерывных поставок продукции и услуг.

В настоящее время электролюминесцентные дисплеи, предлагаемые под торговой маркой Lumineq, можно заказать у официального дистрибьютора Lumineq – компании ПРОСОФТ. ●

рованных соединений (тоннелей) между сервером и конечными устройствами, находящимися в физической сети. Например, ноутбук, подключённый к Интернет, – это клиент, а сервером является роутер (по совместительству межсетевой экран), установленный в сети подстанции. Если ноутбук есть в списке авторизованных устройств на сервере, то сервер устанавливает защищённое VPN-соединение с ним и присваивает ему виртуальный IP-адрес, как если бы тот находился во внутренней сети сервера. Следует помнить, что VPN – это защита для соединения, но никак не для самих клиентов и сервера.

Заключение

Ситуация, когда большинство предприятий энергетической отрасли не соответствуют стандартам кибербезопасности и, как следствие, уязвимы перед кибератаками, должна быть изменена в ближайшее время. Необходимые меры для этого вполне очевидны, требуется лишь время на их осуществление. Модернизация существующих систем с помощью средств кибербезопасности может иметь подводные камни, но даже несмотря на это она нужна сейчас как первый шаг к защищённым интеллектуальным электрическим сетям. А в долгосрочной перспективе новые системы должны проектироваться с уже интегрированными средствами кибербезопасности, максимально возможный уровень которой будет являться одним из ключевых параметров. ●

Литература

1. Andreas Dreher and Eric Byres. Get Smart About Electrical Grid Cyber Security [Электронный ресурс]. – Режим доступа : http://www.belden.com/pdfs/techpprs/PTD_Cyber_SecurityWP.pdf.
2. NERC Standards: Critical Infrastructure Protection (CIP) [Электронный ресурс]. – Режим доступа : http://www.nerc.com/page.php?cid=2|20.
3. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements [Электронный ресурс]. – Режим доступа : http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.
4. Approved IEEE Smart Grid Standarts [Электронный ресурс]. – Режим доступа : http://smartgrid.ieee.org/standards/approved-ieee-smartgrid-standards.
5. Using EAGLE Tofino™ to Control the Spread of Stuxnet Malware [Электронный ресурс]. – Режим доступа : http://www.belden.ru/Belden_Russia_files/Stuxnet.pdf.

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

Как защитить промышленную сеть подстанции с помощью межсетевого экрана EAGLE Tofino

Устройство EAGLE 20 Tofino является симбиозом аппаратной платформы компании Hirschmann (входит в корпорацию Belden) и программной «начинки» от эксперта в области кибербезопасности – компании Byres Security Inc. Данное средство отвечает принятым стандартам кибербезопасности FERC/NERC CIP, ANSI/ISA-99, IEC 62443 и требует минимального вмешательства в свою работу.

Устройство выполнено в компактном корпусе с креплением на DIN-рейку (рис. 4) и имеет 2 порта Fast Ethernet (защищённый и внешний). EAGLE 20 Tofino поддерживает режимы стационарного межсетевого экрана, VPN-сервера/клиента, сетевого экрана для протокола Modbus. После включения в сеть Ethernet устройство не останавливает трафик, а в фоновом режиме сканирует все устройства в защищённом сегменте и формирует набор правил для обеспечения сетевой безопасности. Пользователь может менять и добавлять правила и своевременно реагировать на несанкционированные подключения или запрещённые действия, получая предупреждения от устройства.

Рис. 4. Межсетевой экран Hirschmann EAGLE 20 Tofino

Следующие несколько шагов кратко описывают процесс построения системы безопасности с помощью EAGLE 20 Tofino.

1. **Определение места размещения межсетевого экрана**. Каждую подсеть, обслуживающую важный участок предприятия, выделяют в «зону безопасности», отделяя от основной сети межсетевым экранам. Подробные рекомендации даны в стандарте ANSI/ISA-99.
2. **Определение типа возможных кибер-угроз**. EAGLE 20 Tofino позволяет загружать программное обеспечение в виде модулей, выполняющих различные функции. Например, если необходимо контролировать все подключающиеся к сети физические устройства, то существует модуль Secure Asset Management. Если нужен функционал классического стационарного межсетевого экрана (firewall) с контролем всех соединений согласно списку установленных правил, то предлагается модуль Stateful Firewall Module. При использовании популярного протокола Modbus можно поставить модуль Deep Packet Inspection, осуществляющий глубокий анализ команд-запросов и ответов, функциональных кодов, используемых регистров. Наконец, при необходимости использовать VPN можно догрузить модуль VPN-сервера/клиента.
3. **Выбор сервера или станции оператора для установки административного ПО**. Для централизованного управления группой межсетевых экранов EAGLE 20 Tofino существует программный пакет Tofino Central Management Platform.
4. **Настройка и запуск системы безопасности**. Если сеть большая и содержит несколько сегментов, разделённых межсетевыми экранами, то постепенный запуск и настройка устройств – процесс неудобный и порождающий лишнюю уязвимость системы на время своего проведения. Упомянутое ПО Tofino Central Management Platform позволяет проводить не только групповую настройку устройств EAGLE 20 Tofino, но и контролировать состояние сети в реальном времени. Настройка правил для межсетевого экрана не требует прерывания трафика и может осуществляться на лету в специальном тестовом режиме. Для удобства пользователей в устройство уже заложено более 50 предопределённых промышленных протоколов и более 25 шаблонов правил. В целях защиты от упоминавшегося ранее вирусного ПО Styxnet для межсетевого экрана EAGLE 20 Tofino разработаны конкретные инструкции, опубликованные в официальном бюллетене Belden [5]. ■