Информационная безопасность критической инфраструктуры

Е.Л. Генгринович (Компания FOX-IT)

Критическая инфраструктура состоит из физических и информационных объектов, сетей, услуг и ресурсов, повреждение или уничтожение которых существенно влияет на здоровье, безопасность или экономическое благосостояние граждан. Критические инфраструктуры включают многие экономические секторы, в том числе банковский, транспортный, энергетический, продовольственный секторы, а также коммунальное хозяйство, здравоохранение, связь и ключевые государственные услуги.

Анализ текущей ситуации показывает, что модернизация оборудования и современный уровень информатизации привели к возможности доступа из сетей общего пользования к критической инфраструктуре большинства российских компаний. Вопросам информационной безопасности критической инфраструктуры уделяется недостаточно внимания. Одним из инструментов физического разделения сетей общего пользования и информационной среды критической инфраструктуры является программно-аппаратное решение ДатаДиод.

Ключевые слова: информационная безопасность критической инфраструктуры, сети общего пользования, ДатаДиоды.

Информационная безопасность критической инфраструктуры (ИБКИ) — относительно новая тема, ставшая актуальной с развитием IP-сетей и началом повсеместного использования международных стандартов для задач управления технологическими объектами (энергетика, газ, нефтепереработка, транспорт, ЖКХ, водоотведение, химическая промышленность и т. д.) [1, 2]. Возникает вопрос: значит, правы консервативно настроенные эксперты, утверждая, что новые технологии — это зло, и достаточно было старых аналоговых систем, выделенных каналов передачи данных, а отдельные рабочие места для диспетчерского персонала и бумажные отчеты для руководства устраивали всех?

С точки зрения ИБКИ, безусловно, устаревшие системы управления, использующие нестандартные протоколы передачи данных и не присоединенные к сетям общего пользования, лучше всего защищены от внешних атак. Проблемы здесь возможны только за счет некорректной настройки самих систем управления, ошибок персонала при их эксплуатации, а также из-за нерегламентированного использования внешних накопителей (жесткие диски, флэш-карты и. т.д.). С другой стороны, меняется первичное оборудование, требования рынков и законодательства, и как следствие, меняются технологические и аналитические задачи, которые необходимо решать. Сохранить конкурентоспособность могут только те компании, которые активно внедряют новые технологии, а в ряде случаев устаревшее аналоговое оборудование просто снимается с производства, и его эксплуатация становится неоправданно дорогой.

Есть еще одна точка зрения: «Прогресс не остановить, но сети передачи данных могут быть изолированы физически». Да, такая мысль имеет право на существование, но проблема состоит в том, что за все надо платить. Объем информации, используемый в технологических сегментах сети, за последние 10 лет увеличился на несколько порядков, а функционал вырос многократно. Например, электронная почта стала одним из основных средств рассылки уведомлений о тех или иных событиях в системе диспетчерского управления. Современные промышленные контроллеры оснащаются программными Web-серверами, которые позволяют обеспечить наблюдаемость объекта для руководства и сервисного персонала в любой точке мира, где есть выход в Internet. Диагностика и обслуживание современного оборудования обеспечивается квалифицированным персоналом, который физически может находиться за сотни километров от оборудования и работать по удаленному каналу. Современные ситуационно-аналитические центры реагирования, аналитические и финансовые системы также требуют наличия доступа к данным технологических процессов. Платой, и весьма существенной, за изоляцию критической инфраструктуры будет необходимость ручного переноса информации и ограничения по использованию автоматического функционала, уже установленного оборудования и систем. Предположим, что можно построить систему, используя принцип физического выделения технологических сегментов сетей и утверждения набора организационно-технических регламентов, регулирующих ответственность и вопросы обмена данными между физически разделенными сегментами сетей. Но это потребует решения большого числа неявных задач, таких как:

– наличие отдельных физических каналов передачи данных для каждого технологического объекта, отвечающих современным требованиям;

– отсутствие возможности оперативного контроля ситуации для руководства и внешних компаний (ситуационно-аналитические центры, сервисные компании, МЧС);

– наличие системы контроля ошибок и полноты данных при ручном переносе информации;

– наличие системы регистрации и контроля внешних носителей, предназначенных для переноса информации.

Конечно, здесь приведен далеко не полный перечень, но он уже вполне достаточен для обдумывания целесообразности такого решения проблем ИБКИ.

Фактически сегодня мы находимся в ситуации, когда все крупные российские компании, имеющие инфраструктуру, которую можно отнести к разряду критической, используют сети общего пользования (физические каналы) или собственные бизнес-сети для передачи данных, формируемых внутри критической инфраструктуры. Для персонала, эксплуатирующего критическую инфраструктуру, ничего не изменилось. Сохранились старые регламенты, инструкции, система диспетчерского и технологического управления. Использование стандартов обеспечивает полную прозрачность сетевой инфраструктуры, и до момента возникновения аварий и проблем в системах управления вопросы ИБКИ вызывают негативную реакцию, что вполне оправдано. Регулирующие докумен-

ты либо отсутствуют, либо находятся в стадии разработки.

Функционал систем, влияющих на уровень ИБКИ, требует введения определенных ограничений и регламентов. Обычно для любой компании работоспособность критической инфраструктуры является важнейшим показателем и все, что даже косвенно может повлиять на ее эксплуатацию, подвергается очень серьезному критическому анализу. Складывается ситуация, когда потенциальная угроза ИБКИ не воспринимается как нечто реальное и непосредственно угрожающее.

Далее следует вопрос: «Как же так? Все же очевидно!» Чаще всего те, кто произносят фразы, типа «все очевидно» или «абсолютно понятно», к сожалению, не могут внятно сформулировать, что же в действительности угрожает ИБКИ, и насколько опасны данные угрозы. Попробуем разобраться, в чем тут дело. Начнем с того, что сегодня специалисты по информационной безопасности в основной своей массе имеют богатый практический опыт реализации проектов в административной и финансовой сферах, а с проблемами и особенностями защиты критической инфраструктуры знакомы лишь в теории. В свою очередь технологи, ответственные за эксплуатацию и развитие критической инфраструктуры, весьма поверхностно представляют телекоммуникационную составляющую эксплуатируемых ими систем. В результате прямое взаимодействие специалистов заканчивается ничем, они просто не понимают друг друга — разная терминология, различные уровни и сферы ответственности. Для преодоления этого разрыва сформулируем общие принципы, на которых могло бы строиться такое взаимодействие. Будем использовать термины, понятные обеим фокусным группам специалистов.

Уровень доступа и действия всех технологов, ответственных за эксплуатацию критической инфраструктуры (КИ) строго регламентированы, как и действия банковских служащих, работающих со счетами клиентов.

Объем информации, передаваемой в системах управления, относительно незначителен, а вот гарантированная скорость передачи данных — критически важный параметр.

Промышленные контроллеры, в том числе устанавливаемые на объектах критической инфраструктуры, имеют встроенные Web-сервисы для предоставления возможности дистанционного мониторинга объекта.

Если объект находится под управлением автоматической системы (без участия человека), то обычно высокая надежность достигается дублированием (троированием) автономных программно-аппаратных комплексов (ПАК). Технологические оперативно-информационные системы в стандартном режиме просто мониторят работу и обеспечивают диагностику состояния таких ПАК. Они не вырабатывают управляющих воздействий. В этом случае предусмотрены процедуры изменения конфигурации ПАК как локально, так и дистанционно.

Если система управления автоматизирована (с участием человека), то четко определены уровни оперативно-диспетчерского управления, которые имеют полномочия и техническую возможность управлять объектами критической инфраструктуры.

Установлена четкая иерархия ретрансляции технологических данных по уровням оперативно-диспетчерского и технологического управления. В среднем число потребителей информации (пассивный просмотр данных, получение отчетов и BI-показателей) на порядок выше числа технологов, вовлеченных в процесс непосредственного управления процессами.

Определен четкий порядок информирования причастных должностных лиц при различных событиях и происшествиях от временного пропадания канала передачи данных до крупной аварии, повлекшей серьезные последствия. Большинство современных систем управления имеют встроенный SMTP сервер для рассылки соответствующих извещений по электронной почте.

В целом ряде случаев в качестве основного или резервного канала ретрансляции информации между уровнями оперативно-диспетчерского управления используется IP-облако компании или арендованные каналы передачи данных. Приняв систему управления в эксплуатацию от подрядчика, технолог уверен, что теперь любые изменения в архитектуре системы могут быть выполнены только по четко регламентированной процедуре заявок и отчетов о выполнении сервисно-эксплуатационных работ. При этом контроль изменения правил маршрутизации потоков данных на интеллектуальных телекоммуникационных устройствах у диспетчера отсутствует.

Антивирусные базы и стандартное ПО в технологических сегментах сетей обычно не обновляется, что обосновывается совместимостью ранее установленного ПО конкретного производителя с существующей операционной средой. Более того, зачастую производитель системы управления выпускает патчи (дополнения) к своему ПО (например, в случае выявления уязвимости по информационной безопасности), но оно не устанавливается, так как при этом необходимо провести полные функциональные испытания системы управления и внести изменения в организационно-методические документы.

Диагностика и сервисное обслуживание устанавливаемого оборудования, в том числе и импортного, часто требует привлечения инженерно-технического персонала производителя для обеспечения его эксплуатации. Это влечет за собой необходимость организации удаленных рабочих мест и обеспечения внешнего доступа к объектам критической инфраструктуры.

Растет число бизнес-приложений, использующих данные, формируемые внутри критической инфраструктуры. Это значит, что обеспечивается полноценное взаимодействие технологического и бизнес сегментов корпоративных IP сетей.

Проанализировав таким образом системы оперативно-диспетчерского и технологического управления, можно говорить о конкретных угрозах ИБКИ.

Одним из решений, позволяющих значительно повысить степень ИБКИ и одновременно обеспечить доступ к оперативно-технологической информации, является использование ДатаДиодов. Это программно-аппаратное решение, обеспечивающее на физическом уровне одностороннее соединение сегментов IP-сетей с разным уровнем требований к безопасности. Сеть с более низким уровнем

требований называется "черной", с более высоким уровнем — "красной". В основе решения лежит использование двух оптических карт. Оптическое волокно, используемое для передачи в сторону "черной" сети физически отсутствует, то есть данные не могут быть переданы в принципе.

В настоящее время для реализации ДатаДиода ведется поддержка широкого спектра технологических протоколов и приложений: IEC 60870-101, IEC 60870-103 (Siemens, ABB, Micom и др.), IEC 60870-104, IEC 61850, OPC 2.0, DNP3, ICCP, Modbus RTU, ABB (SCADA, SPA), OSIsoft PI Server, GE iHistorian, Wonderware Historian, ION, SATEC. Это позволяет обеспечить гарантированный доступ к технологическим данным, имея при этом гарантию неуязвимости самой критической инфраструктуры, так как физически канал доступа в защищаемый сегмент отсутствует.

Основные характеристики ДатаДиодов

- Однонаправленное коммуникационное устройство:
  - аппаратная реализация (нет ПО, прошивок);
  - не может быть взломано;
  - нет возможности on-line-атак;
  - нет потерь данных;
  - большое число внедрений по всему миру.
- Более 300 поддерживаемых приложений (FTP, TCP, UDP, SMTP, Kaspersky, MS SQL, Oracle, PI, WSUS и т. д.).
- Поддержка промышленных протоколов, в том числе российских.

Перечень внедрений ДатаДиодов достаточно широк: от оборонных до крупных энергетических компаний. В США, например, приняты стандарты, напрямую предписывающие использование ДатаДиодов для защиты критической инфраструктуры (NERC3). Международное агентство по атомной энергии МАГАТЭ использует их для контроля оперативной ситуации на атомных станциях. В России одной из первых начал применять данное решение холдинг ОАО «РусГидро».

Таким образом, ДатаДиоды можно считать современным эффективным инструментом для решения задач ИБКИ, гарантирующем сохранение управляемости объектами критической инфраструктуры, при любых внешних атаках, изменениях телекоммуникационной инфраструктуры, ошибках сервисных компаний и ошибочных (предумышленных или нет) действиях не оперативного персонала компании.

Список литературы

1. *Васильев В.* Информационная безопасность критически важных объектов//PC Week Review: ИТ-безопасность. 2013. Сентябрь.
2. На повестке дня — безопасность АСУ ТП критически важных объектов//Connect! Мир связи. 2013.№ 9.

Генгринович Евгений Леонидович *— технический консультант компании FOX-IT.*
Контактный телефон (985) 928-86-02.
E-mail: geleon4@gmail.com

24 марта 2015 г. в Москве в гостинице Холидей Инн Сокольники состоится PTC Live Tech Forum

Это ключевое мероприятие PTC в России, которое позволит специалистам получить полное представление о новых разработках и достижениях в области передовых инженерных технологий, включая управление жизненным циклом изделий (PLM), САПР (CAD/CAM/CAE), управление обслуживанием (SLM), управление разработкой программного обеспечения (ALM), а также о главном технологическом тренде в производственной индустрии – Internet-вещей (IoT).

Контактный телефон (495) 646-29-66
E-mail: tgolub@ptc.com

Пятая юбилейная конференция «E3.series: Инновации в электротехническом проектировании»!

Компания ПОИНТ, эксклюзивный дистрибьютор E3.series компании Zuken (Германия) в России и СНГ, 19 марта 2015 г. проводит пятую инжиниринговую конференцию «E3.series: Инновации в электротехническом проектировании-2015. Транспортное машиностроение и приборостроение».

Мероприятие посвящено современным технологиям проектирования бортовой кабельной сети и конструирования жгутов в области аэрокосмической отрасли, машиностроении, судостроении, автомобилестроении, приборостроении и других отраслях.

Конференция будет интересна руководителям предприятий, техническим директорам и главным инженерам, начальникам проектных отделов, ведущим инженерам, а также сотрудникам отделов САПР и PLM-систем. По оценкам организаторов, в предстоящем мероприятии примут участие более 140 организаций и предприятий из России и стран СНГ.

Участие в конференции платное. Регистрация (http://e3series.ru/register) обязательна до 16 марта 2015 г.

Впервые в программе мероприятия, помимо выступлений с презентациями продуктов и примерами внедрений, пройдут тест-драйвы ПО E3.series.

Тест-драйвы проводятся под руководством специалистов компании ПОИНТ. Участники смогут самостоятельно выполнить небольшой электрический проект, получить отчетную документацию, связать электрические данные с 3D-моделями проектируемого изделия и проследить «жизненный» цикл документации проекта.

- «Проектирование в E3.series», включая создание: принципиальной электрической схемы Э3 (общей Э6), схемы соединений на жгут (Э4), развертки жгута на плоскость; а также автоматическое получение отчетной документации.
- Совместная работа E3.series с 3D-CAD и PLM (на примере NX и TEAMCENTER компании SIEMENS): включая передачу схем и отчетной документации в TEAMCENTER, синхронизация БД E3.series и TEAMCENTER, передачу состава изделия из E3.series в TEAMCENTER, выгрузку состава жгута и получение структуры сборки в NX, трассировку жгутов в NX, создание развертки жгутов в E3.series.

В ходе мероприятия будет возможность пообщаться с представителями предприятий, внедривших E3.series и обсудить интересующие вопросы.

В перерывах конференции будет проходить демонстрация ПО E3.series.

Место проведения: Гостиница Рэдиссон САС Славянская (г. Москва, пл. Европы, д. 2; м. Киевская).

Подробнее о мероприятии http://e3series.ru/conf2015.