Новая концепция защиты критичных сегментов информационной инфраструктуры, ситуационных центров и промышленных сетей

Алексей МАЛЬНЕВ,
начальник отдела защиты КСИИ,
АМТ-ГРУП

В последние годы ситуация в области ИБ АСУ ТП характеризуется всеобщим пониманием проблематики, однако проекты ИБ в отрасли реализуются крайне медленно, особенно с учетом размера рынка (по некоторым данным, в России насчитывается более 3000 категорированных КВО, из которых значительная часть содержит АСУ ТП). Тем не менее понимание государством и рынком проблемы – это уже шаг вперед.

У большинства владельцев КСИИ созданы собственные подразделения безопасности, которые не только курируют вопросы физической (режимной) безопасности, но и берут на себя задачи информационной безопасности. В соответствии с давно ожидаемым проектом Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» должны определиться роль и полномочия регуляторов в вопросах защиты КСИИ. Помимо всего прочего становится актуальной задача формирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, в рамках которой будет действовать Национальный координационный центр по компьютерным инцидентам. Кстати, примерно аналогичная задача была определена и в 2012 г., в «дорожной карте» Совета Безопасности РФ («Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации»).

Итак, есть проблема, есть понимание проблемы и есть дополнительные задачи, определяемые законодательством в рамках этой же проблемы. Что в первую очередь следует из этого для подразделений ИБ, работающих в данных отраслях?

Во-первых, наконец-то появляется законодательное обоснование информационной безопасности на объектах КСИИ. Сейчас мы наблюдаем заметное замедление развития направления информационной безопасности на объектах КСИИ относительно актуальных угроз безопасности в отрасли. Наметилось существенное отставание от ведущих западных стран, где давно работают соответствующие законы, более десяти лет оттачиваются отраслевые стандарты, накоплен богатый опыт, работают учебные полигоны для тестирования всевозможных комплексов ИБ в промышленных системах. Тем не менее наверстать это отставание нам вполне по силам, опыт и наработки уже появляются: об одном результате наших исследования будет рассказано в данной статье.

Во-вторых, мы получаем новый спектр специализированных задач ИБ, существенно отличающихся от задач ИБ корпоративного сегмента. Одна из наиболее очевидных задач, которые предстоит решать, – создание упомянутых государственных систем обнаружения, предупреждения и ликвидации последствий компьютерных атак. Здесь проблема заключается в явном противоречии задач централизации функций мониторинга и управления ИБ и задач обеспечения высокого уровня ИБ на объектах КСИИ. Необходимость центров информационной безопасности на государственном уровне и уровне отраслей/холдингов/организаций сомнению не подлежит – это обеспечит и проактивность в реагировании, и своевременное обнаружение и ускорение расследований инцидентов ИБ. Но территориальная распределенность объектов КСИИ означает необходимость использовать открытые, общедоступные каналы для передачи информации. Географическая распределенность выделенных каналов не позволяет обеспечить им физическую защиту, значит, они должны рассматриваться как недоверенные каналы связи.

Очевидно, что для объектов подобного уровня критичности классические корпоративные подходы к защите не подходят по определению. Если говорить о задаче защиты государственных (и отраслевых) центров информационной безопасности и мониторинга, то необходимо одновременно обеспечить и территориальную

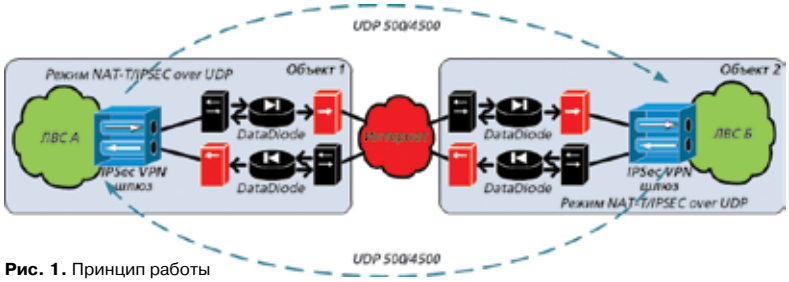

Рис. 1. Принцип работы

распределенность, и гарантируемый высокий уровень защиты периметра. Другими словами, технически задача такова: следует объединить критичные сегменты КСИИ через открытые каналы. Но при этом достигнуть такой изоляции объектов КСИИ, которую не способны обеспечить любые известные внешние периметры, использующие классические схемы с межсетевым экранированием, т. е. требуется исключить бóльшую часть внешних угроз.

Это невозможно? Наши исследования показали, что возможно

Наша задача заключалась в оптимизации использования однонаправленных систем передачи данных (далее – DataDiode) в промышленных системах. Под оптимизацией понимается поддержка бóльшего количества TCP-протоколов без создания сложных логических конструкций.

В ходе исследования и анализа проблемы стало понятно, что оптимальное решение для передачи любого трафика через DataDiode – туннелирование трафика в протокол UDP. Это было первой задачей.

Вторая задача состояла в обеспечении полного дуплекса, что потребовало разделения туннелированного потока UDP на два однонаправленных и использования разнонаправленных контуров DataDiode, контролирующих оба потока в каждом направлении. О том, что такая схема дает, будет рассказано ниже.

Третья задача – обеспечение криптографической защиты трафика, туннелированного в данный UDP-поток.

Ответ оказался довольно очевидным и изящным по своей простоте: мы использовали IPSec и технологию NAT-Traversal (NAT-T), созданную разработчиками специально для установления IPSec-туннелей через NAT-устройства. Как известно, NAT-T позволяет инкапсулировать IPSec в UDP (порт 4500 по умолчанию на большинстве IPSec-шлюзов) для обхода NAT-устройств. Таким образом, эмулируя NAT и включая NAT-T-функционал на IPSec-шлюзах, мы решили первую и третью задачи. Что касается второй, то она решается посредством настройки маршрутизации и специальной настройки NAT на маршрутизаторах (межсетевых экранах) с обеих сторон схемы относительно DataDiode. Принцип такого взаимодействия показан на схеме (рис. 1).

Подобная схема позволяет связывать два критичных сегмента (ЛВС А и ЛВС Б) посредством VPN IPSec-шлюзов и DataDiode. Вопрос компрометации IPSec не является предметом обсуждения, но отмечу, что в такой схеме мы вольны использовать любые криптошлюзы (в том числе отечественные сертифицированные), самые стойкие криптоалгоритмы (в частности, ГОСТ 28147-89) и цифровые сертификаты для аутентификации криптошлюзов.

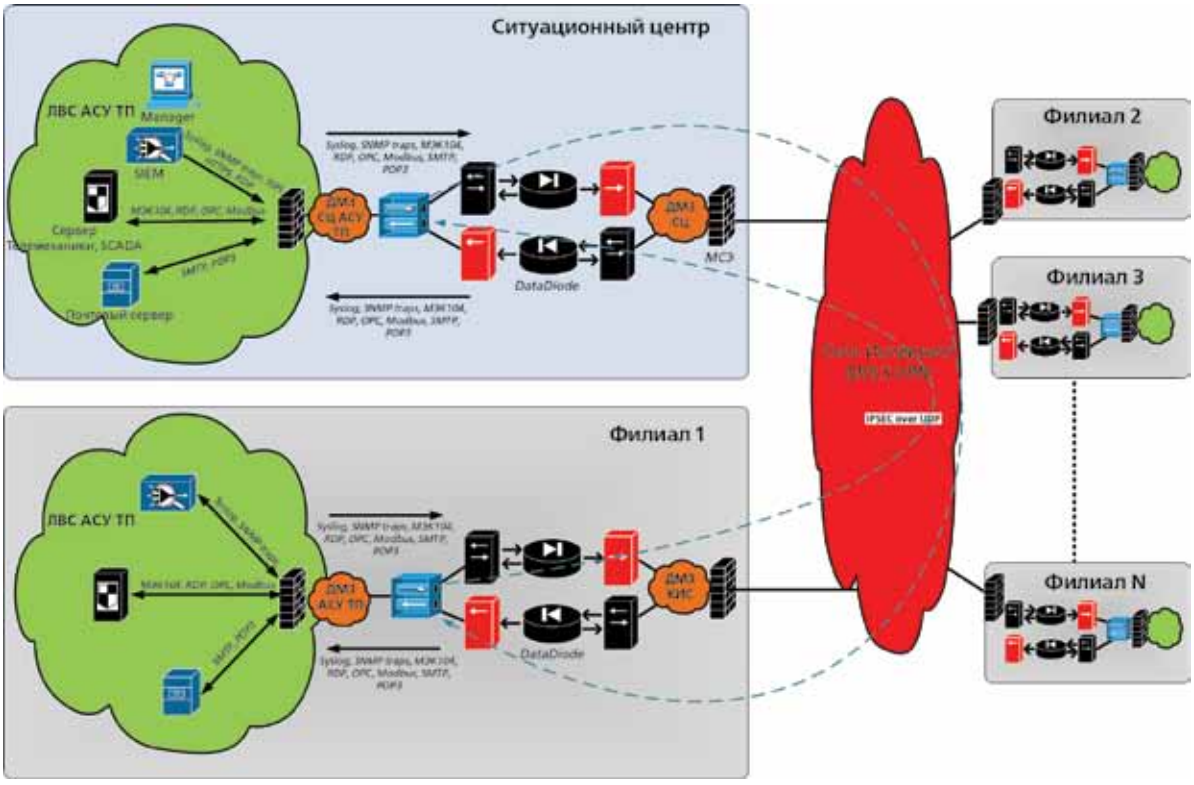

Рис. 2. Вариант применения схемы распределенной VPN-сети для защиты объектов КСИИ

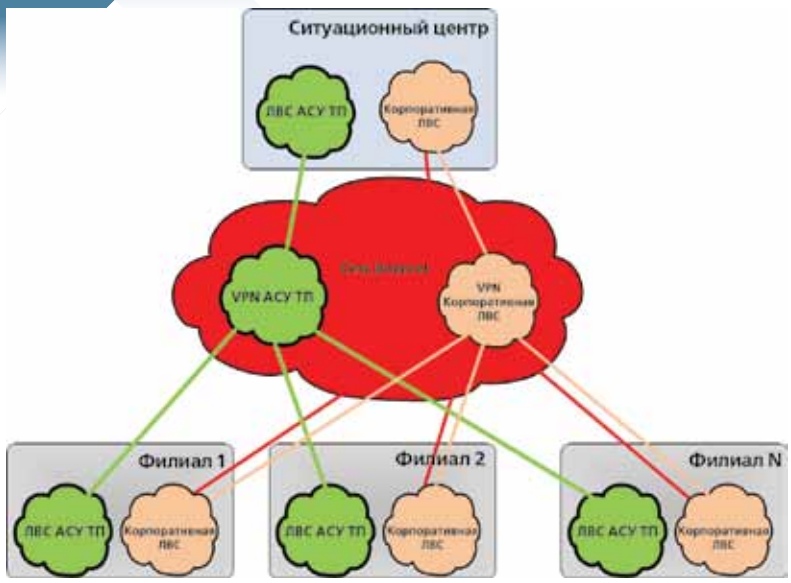

Рис. 3. Пример разделения VPN-критичных сегментов от VPN ЛВС корпоративной сети

В то же время мы получили два сегмента, способных полноценно взаимодействовать между собой по всему стеку TCP/IP, в том числе по технологическим протоколам Modbus, OPC, RDP, S7, IEC 104 и т. п.

Разумеется, подобная схема не исключает (и предусматривает) использование межсетевого экранирования, и в реальной ситуации схема может иметь примерно следующий вид (рис. 2).

Таким образом, были решены следующие задачи:

- сформирован защищенный внешний периметр с использованием систем однонаправленного межсетевого взаимодействия DataDiode;
- реализовано туннелирование трафика в шифрованный UDP IPSec-поток;
- обеспечено разделение шифрованных информационных потоков на два направления.

С точки зрения функциональности все очевидно: в целом схема функциональна по части транспорта протоколов настолько, насколько функционален сам IPSec. Если мы используем Route-based IPSec VPN, то помимо всего прочего в защищенные каналы можно направлять и multicast-трафик, что позволяет существенно масштабировать схему, передавая данные динамических протоколов маршрутизации. Схема имеет следующие функциональные преимущества:

- в основе лежит сетевая технология (IPSec), а не прикладная, что обеспечивает более высокий уровень надежности, безопасности и производительности относительно прикладных решений;
- отсутствие ограничений по функциональности для сетевых протоколов стека TCP/IP;
- возможность поэтапного внедрения решения в традиционные VPN-сети;
- большие возможности по масштабированию: до тысяч VPN-узлов и производительность от 1Гб/с и выше.

В чем принципиальное преимущество повышения уровня защищенности внешнего периметра, построенного по описанной схеме?

В первую очередь использование двусторонней схемы Datadiode позволяет исключить для внешнего злоумышленника возможность установления соединений с внутренними ресурсами. Разделение и управление потоками в обе стороны реализованы посредством настройки маршрутизации и NAT. Кроме того, с каждой стороны от DataDiode определяются политики трафика на межсетевых экранах, что создает дополнительные сложности для злоумышленника. Но главное, любое сетевое соединение требует обратной связи, а в такой схеме это полностью исключается с помощью DataDiode, контролирующих UDP-потоки в каждом направлении. Проще говоря, внешний злоумышленник не имеет возможности перенастроить оборудование за DataDiode (в том числе сам DataDiode на защищенной стороне). Для перенастройки необходимы дуплексная связь и установление управляющего соединения, что данная схема исключает в принципе, следовательно, устраняется бóльшая часть внешних угроз. Например, в США аудитор в рамках проверок по стандарту NERC-CIP (Compliance Application Notices CAN-0024) автоматически исключает из рассмотрения большую часть внешних угроз при наличии на периметре объекта системы однонаправленной связи DataDiode.

Нужно отметить, что мы можем подбирать сертифицированные ФСТЭК и ФСБ (если речь идет о СКЗИ) компоненты решения. Например, используемый в нашем исследовании DataDiode в настоящий момент проходит процедуру сертификации ФСТЭК, что позволит использовать его для защиты КСИИ.

Крайне важно, что гарантия исключения большинства внешних угроз определяется на **аппаратном уровне:** DataDiode имеют аппаратный компонент, работающий без операционной системы. Это и является гарантией исключения возможности взлома и преодоления DataDiode, что исключает любую вероятность конфигурационных ошибок с ущербом для безопасности.

Именно поэтому системы DataDiode – единственные в мире продукты, сертифицированные в соответствии с ISO/IEC Common Criteria по максимальному уровню соответствия заявленному функционалу EAL7.

Если говорить о достигнутом уровне защищенности периметра, то данное решение при использовании всего комплекса средств защиты и специализированного дизайна позволяет:

- исключить любые возможности для внешнего злоумышленника по установлению сетевых соединений с защищаемыми ресурсами, т. е. решение исключает внешние угрозы:
  - сетевой взлом, использование уязвимостей для получения удаленного доступа;
  - удаленные вирусные атаки (вирусы, «черви»);

– перехват, кражу информации;
– перехват команд управления;
– получение удаленного нелегитимного доступа;
– нарушение обмена данных внутри защищаемого сегмента;
– перехват и подбор паролей доступа к сетевым сервисам управления и мониторинга;
– искажение и нарушение целостности пакетов данных;
DDoS-атаки на внутренние ресурсы;

- обеспечить возможность интеграции с традиционными МСЭ- и VPN-шлюзами: схема дополняет традиционные дизайны защищенного периметра, есть возможность гибкого определения политик движения трафика;
- исключить негативные последствия для ИБ от конфигурационных ошибок.

Важным обстоятельством является и то, что корпоративные сети передачи данных объектов в рамках холдингов ТЭК зачастую объединены через IPSec VPN-сети site-to-site. Иногда эти же корпоративные каналы используются и для передачи контрольно-измерительной информации, отчетов, данных телемеханики и т. д., полученных из критичных сегментов (например, АСУ ТП). Разумеется, при этом возникает вопрос: насколько безопасно использовать единое каналообразующее оборудование и «смешивать» корпоративные и индустриальные (либо любые другие критичные) потоки данных?

Кроме того, реализация описываемого решения предоставляет вполне четкую концепцию разделения корпоративных сетей и критично важных информационных систем. При этом корпоративные сети могут строиться как угодно функционально, с многочисленными выходами в сеть Интернет и иметь изолированные политики безопасности, оптимизированные под бизнес-задачи. А критичные сегменты будут взаимодействовать параллельно и независимо, представляя собой полностью изолированную от любых внешних сетей распределенную структуру с защищенными каналами связи и уникальным по уровню защищенности от внешних угроз периметром (рис. 3).

Представленную схему специалисты АМТ-ГРУП уже протестировали под нагрузкой, использовались оборудование разных производителей и модели VPN-шлюзов. Были протестированы различные реализации VPN Site-to-Site (в том числе DMVPN). Схема показала требуемую функциональность и стабильность работы. Также была успешно протестирована схема с каскадированием DataDiode посредством систем балансирования нагрузки.

При выборе DataDiode мы руководствовались критериями достижения максимального уровня соответствия заявленным функциям безопасности Common Criteria EAL7 и наличия аппаратного компонента без ПО. К слову сказать, системы DataDiode в некоторых развитых странах используются повсеместно для защиты КВО, в том числе информационных систем военных объектов (некоторые системы DataDiode уже имеют сертификацию NATO Secret для защиты военных информационных систем NATO уровня секретности Secret – аналог отечественного «Совершенно секретно»).

Протестированное нами специализированное решение по защите периметра не только позволяет повысить эффективность защиты внешних периметров, но и выводит ее на новый уровень. Разумеется, данное решение эффективно только при отсутствии других точек взаимодействия с недоверенными сетями и может применяться для защиты различных объектов КСИИ, КВО, АСУ ТП, объектов ТЭК, построения распределенных критичных информационных систем и ситуационных центров. ■

Конференция «Разумный город»: современные технологии для мегаполиса

Интеллектуальные системы управления городом, бизнес-процессами и домом переживают настоящий бум. Внедрение современных технологий позволяет оптимизировать затраты, автоматизировать системы жизнеобеспечения городов.

Содействие развитию информационно-коммуникационных и аудиовизуальных технологий для повышения эффективности управления городом – цель конференции «Разумный город», которая пройдет 29 октября в рамках выставки Integrated Systems Russia 2013.

Доклады будут представлены по трем тематическим группам: интеллектуальная система управления городом; безопасный город; ЖКХ и энергоэффективность.

Выступающие в первой части конференции расскажут, как информационно-коммуникационные технологии позволяют добиться повышения качества коммунального и транспортного обслуживания, обеспечить эффективность городского управления. Как сделать безопасным город и его транспортное сообщение с помощью различных интеллектуальных систем (охраны, видеонаблюдения, распознавания личности и т. д.) – вопросы второго тематического раздела. В третьей части конференции будут обсуждаться проблемы модернизации и реформирования ЖКХ, возможности управления объектами и структурой жилищного фонда, тема повышения энергоэффективности.

Участникам мероприятия будут продемонстрированы примеры использования перспективных решений на основе реализации международных проектов. Конференция продемонстрирует один из трендов отрасли – сближение AV и IT-индустрии.

В программе выставки по традиции предусмотрены презентации проектов «Цифровое образование», Digital Signage, Национальная премия в области интеграции профессионального аудиовидеооборудования ProIntegration Awards, семинары и курсы профессиональных ассоциаций CEDIA, InfoComm International, Форум KNX «Применение мобильных платформ (IOS, Android) в проектах KNX».

Впервые в новом формате будет представлен проект «Умный дом». В рамках выставки будет работать действующая модель «умного дома», и каждый желающий сможет попробовать себя в роли управляющего инженерными и мультимедийными системами.

Более подробную информацию о выставке Integrated Systems Russia 2013 можно найти на сайте: www.isrussia.ru. Там же можно пройти регистрацию для посещения форума.

www.isrussia.ru