Интеграция технологических и корпоративных сетей

Объекты крупных промышленных предприятий и предприятий нефтегазовой отрасли являются важнейшими элементами инфраструктуры государства и оказывают существенное влияние на устойчивое развитие экономики и социальной сферы, обороноспособность страны, стабильность и эффективность внешней и внутренней политики. Неудивительно, что в современных условиях все больше внимания уделяется вопросам безопасности "нервной системы" промышленных предприятий – автоматизированным системам управления технологическими процессами (АСУ ТП). Одним из элементов безопасности подобных систем является информационная безопасность.

Информационная безопасность, как неотъемлемая часть АСУ ТП, должна обеспечивать бесперебойное функционирование системы, невозможность несанкционированного прочтения или модифицирования передаваемых технологических параметров, а также оказывания какого-либо воздействия на управляющие команды системы.

До недавнего времени российские компании не уделяли должного внимания вопросам информационной безопасности АСУ ТП, полагаясь на изолированность этих систем. Однако сегодня все больше специалистов понимают экономические выгоды от интеграции АСУ ТП с системами управления предприятием (АСУП), производством и системами оценки экономической эффективности (СОЭ).

Примером подобной интеграции может служить использование ряда хранящихся и наблюдаемых параметров АСУ ТП в системах СОЭ. СОЭ способна предложить оператору АСУ ТП более экономически эффективные режимы эксплуатации, что позволяет уменьшить эксплуатационные расходы за счет увеличения межремонтного периода, сохранить ресурс оборудования, сократить затраты на энергоресурсы.

Однако эту задачу нельзя решить без организации единого мониторинга в реальном масштабе времени для всего предприятия, который, в свою очередь, диктует требования к сбору и анализу информации, поступающей от различных АСУ ТП. Часто требования информационного обмена предписаны государственными постановлениями или вызваны необходимостью обмена информацией с партнерами.

Успешно зарекомендовавшие себя системы управления предприятием и производством (ERP, MES) также будут иметь дополнительные преимущества при получении выборочной информации с уровня АСУ ТП. Такая интеграция упрощает финансовый мониторинг, схемы взаимодействия с поставщиками и клиентами и повышает финансовую прозрачность предприятия.

Однако использование интеграционных технологий невозможно без информационного обмена как в рамках одной АСУ ТП, так и при взаимодействии с системами СОЭ, ERP и MES, которые традиционно размещаются в сегментах корпоративной сети. В этих условиях вопросы организации защиты АСУ ТП от угроз ее информационной безопасности становятся весьма актуальными.

Несоблюдение мер безопасности в этой области может привести к нежелательным последствиям, таким, как:

- угроза национальной безопасности путем провоцирования техногенных катастроф в целях террора;
- угроза жизни или здоровью работников предприятия и гражданского населения;
- негативное воздействие на окружающую среду;
- нарушение требований регулирующих органов;
- потеря конфиденциальной информации;
- нарушение технологического процесса (ТП);
- ухудшение качества услуг или продуктов;
- снижение производительности и эффективности производства и т. д.

К сожалению, Россия не обладает собственной информационной базой по имевшим место инцидентам нарушения безопасности АСУ ТП. Информация, поступающая из СМИ, разрозненна, и по ней сложно судить о существующих тенденциях. Подобную базу – Industrial Security Incident Database (ISID) – поддерживает один из ведущих канадских технологических институтов The British Columbia Institute of Technology (BCIT). В ней регистрируются известные случаи вмешательства в АСУ ТП и нежелательные последствия, вызванные этими вмешательствами. По данным статистики, в более 50 % случаев убытки составили более 750 тыс. евро, в 41 % привели к потерям продукции, в 29 % компании потеряли возможность наблюдать и контролировать ТП.

Традиционно потенциальные угрозы информационной безопасности АСУ ТП разделяют на непреднамеренные, или случайные, и преднамеренные, или целевые. В свою очередь, аналогичные потенциальные угрозы по отношению к информационным ресурсам разделяются на внутренние и внешние.

Зачастую в качестве источника внешних информационных угроз рассматривают только сеть Интернет, прямое подключение к которой не имеет практически ни одна сеть АСУ ТП в России. В то же время большинство нападений происходит по нескольким направлениям одновременно с использованием различных технологий и

протоколов. Например, современные сетевые вирусы – черви способны с большой скоростью распространяться в любых сетях передачи данных, с помощью почты, файлов документов, исполняемых файлов, используя уязвимости в системном и прикладном программном обеспечении АСУ ТП. Другим важным моментом является возможность пошагового распространения угрозы. Например, поразив внешний Web-сервер предприятия, червь проникает в офисную сеть и далее в сеть АСУ ТП. Таким образом, прямого соединения АСУ ТП с сетями общего пользования для этого не требуется.

По статистике BCIT, только 17 % внешних инцидентов связаны с угрозами, исходящими напрямую из сети Интернет, а 49 % – с подключением к WAN-сетям или к корпоративным сетям. Остальные внешние угрозы исходят от несанкционированного подключения через сети компаний партнеров (10 %), коммутируемые линии (7 %), виртуальные частные сети (7 %), сети операторов связи (7 %) и беспроводные сети (3 %).

Часто перед инициатором атаки не стоит каких-либо определенных целей, но даже в этом случае эти вторжения могут вывести АСУ ТП или ее компонент из строя, нарушить связность компонентов, что приводит к лишению оператора возможности управлять ТП. Пассивное прослушивание также является существенной угрозой, ибо в АСУ ТП могут циркулировать данные, составляющие государственную или коммерческую тайну. Также изолированные системы подвержены и внутренним угрозам, которые могут быть последствиями отказов технических средств, сбоев ПО АСУ ТП, действий неквалифицированного персонала и т. д.

Широкое использование операционных систем общего назначения при разработке серверов, контроллеров и АРМ является одним из факторов рисков, описанных выше. Все больше и больше операционных систем семейства Microsoft Windows и Unix-подобных используется не только для построения АРМ операторов АСУ ТП, но и при создании контроллеров. И хотя производители операционных систем постоянно совершенствуют свои технологии, уязвимости в них обнаруживаются с завидным постоянством. Например, с января по ноябрь 2007 года было опубликовано более 11 предупреждений об опасности для продуктов компании Microsoft, не считая уязвимостей другого прикладного и системного программного обеспечения. Такая же ситуация наблюдается и в отношении Unix/Linux-подобных систем.

Помимо операционной системы уязвимости могут присутствовать и в прикладном ПО, включая и сами АСУ ТП. Использование таких известных протоколов, как HTTP, SNMP, FTP, DHCP, OPC, DCOM, ActiveX, Java, на АРМ, контроллерах и серверах позволяет добиваться большей функциональности и удобства работы с этими системами, но может и привносить новые уязвимости в систему.

Ситуация усложняется задержкой с установкой на эти АРМ, серверы и контроллеры программ-"заплаток", которые должны устранить уязвимость в операционной системе или приложении АСУ ТП. Даже после выпуска программ-"заплаток" производителем операционной системы, что не может происходить мгновенно, требуется время на тестирование этой программы производителем АСУ ТП, на установку обновления с учетом окон технического обслуживания, что достаточно трудно сделать, учитывая практическую невозможность остановки технологического процесса. С годами число уязвимостей неминуемо нарастает, накапливаются программные ошибки.

Наиболее эффективным средством защиты операционных систем от распространения современных атак являются хостовые системы предотвращения вторжения Host Intrusion Protection System (HIPS), которые должны устанавливаться на все операционные системы общего назначения, такие как Microsoft Windows, Sun Solaris и Linux. Контролируя на системном уровне события, происходящие в операционной системе и приложениях, HIPS позволяет вовремя блокировать вредоносные воздействия самораспространяющихся червей или вирусов, ПО, имеющего несанкционированно установленные "закладки", предотвращать модификацию исполняемых файлов АСУ ТП и т. п.

Подобное ПО также включает в себя и персональный межсетевой экран, который снижает вероятность поражения АРМ, сервера или контроллера сетевыми червями и дает возможность пресечь нежелательные воздействия, исходящие с данного АРМ, сервера или контроллера. Необходимо отметить, что современная HIPS действует на принципиально ином уровне по сравнению с традиционными антивирусами. Здесь используется поведенческая модель, которая не зависит от свежести антивирусных баз данных. Кроме того, HIPS блокирует неправильные действия пользователя или любого ПО на нескольких уровнях, например блокирует распространение атак на уровне сканирования сети, заражения АРМ и т. д.

Другой проблемой, которую нельзя сбрасывать со счетов, является использование широко распространенной технологии передачи данных. Использование Ethernet при создании сетей передачи данных, голоса и видео хорошо зарекомендовало себя не только в корпоративных сетях, где они успешно применяются в течение уже 30 лет, но и при объединении АРМ, серверов АСУ ТП, контроллеров. С началом массового производства и, соответственно, удешевления компонентов для построения таких сетей становится возможным использование Ethernet как единой среды передачи данных для самого нижнего уровня АСУ ТП, где размещаются контрольные датчики и исполнительные механизмы, подключаемые по протоколам Modbus/TCP, EtherNet/IP, PROFInet и др.

Компания General Motors, один из гигантов тяжелой индустрии, широко применяющая АСУ ТП, заявила о поддержке плана перевода всех контроллеров, роботов, систем управления процессами (process-control equipment) на стандарт Ethernet/IP (Industrial Ethernet), так как он обеспечивает открытость, готовность, широкую доступность на рынке, возможность передачи трафика в реальном масштабе времени и позволяет использовать стандартное оборудование для сетевой инфраструктуры.

Спецификации Modbus/TCP, EtherNet/IP, Foundation Fieldbus High Speed Ethernet (HSE), Interface for Distributed

Automation (IDA), PROFInet используют протоколы Ethernet и IP, которые не являются совершенными с точки зрения обеспечения безопасности. Подобные ограничения, изначально заложенные при создании спецификаций протоколов Ethernet и IP, требуют дополнительного внимания при выборе технического решения.

Что хорошо для офисных сетей, не совсем годится для суровых условий эксплуатации в АСУ ТП. И здесь важны не только повышенные требования к климатическим условиям работы, уровню загрязненности окружающей среды, вибронагрузке, но и к средствам защиты передаваемых по этим сетям (шинам) контрольных значений и управляющих команд.

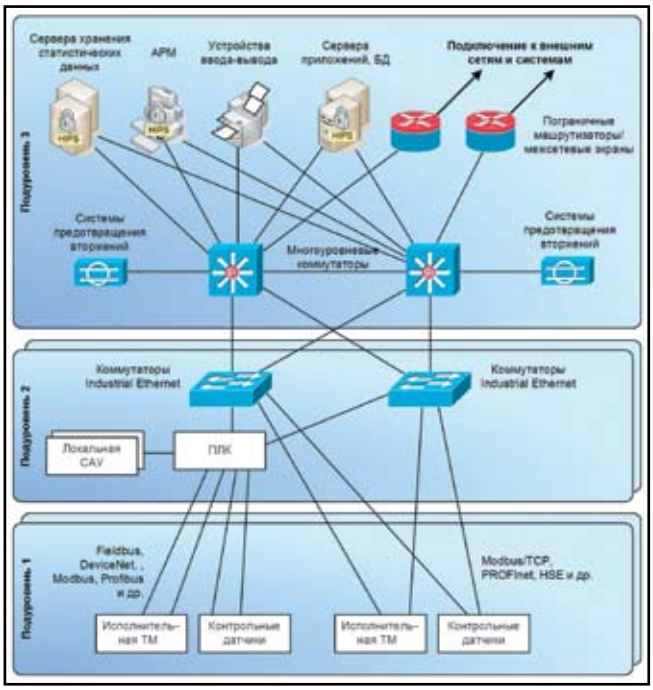

Рис. 1. Пример схемы организации связи и защиты локального сегмента АСУ ТП

Для подключения устройств всех уровней АСУ ТП рекомендуется использование коммутаторов Ethernet (рис. 1), способных обеспечивать защиту от таких угроз, как:

- прослушивание трафика (с использованием атак переполнения таблицы MAC);
- подмена адресов участников информационного обмена (с использованием атак подделки сообщений протокола ARP, подделки IP-адресов, подделки MAC-адресов);
- несанкционированная передача трафика в другие виртуальные сегменты сети (с использованием атак прохождения VLAN);
- атаки на сам коммутатор и сеть (с использованием особенностей протокола Spanning Tree, передачи анормального трафика и др.).

В некоторых случаях целесообразно использование технологии аутентификации устройств и/или пользователей при подключении к коммутируемой сети (например, по стандарту 802.1x).

Еще одним решением, которое должно обеспечить защиту информационного обмена, является создание демилитаризованных зон (рис. 2). Подобные зоны представляют собой точку обмена информацией между различными АСУ ТП с системами управления предприятием, обеспечивая баланс между доступностью информации и безопасностью. Использование модульного подхода при построении подобных центров позволяет провести четкую черту между функциональными модулями системы, планомерно развивать и масштабировать системы, облегчает поиск неисправностей, дает возможность четко определить правила контроля доступа на границе функциональных модулей и разделить административную и техническую ответственность между различными участниками информационного обмена. В этом контексте необходимо рассматривать корпоративную сеть в качестве внешнего, недоверенного сегмента и соответствующим образом обеспечивать как защиту информации, передаваемой из АСУ ТП во внешние системы, так и блокировать внешние несанкционированные обращения к АСУ ТП.

Для защиты демилитаризованных зон применяются межсетевые экраны, обладающие возможностью глубокого анализа проходящего трафика, совместно с системами потокового сканирования сетевого трафика (сетевыми системами предотвращения вторжения, NIPS). Применение комбинированных средств защиты увеличивает надежность решения в целом и позволяет обнаруживать атаки, находящиеся внутри пакетов легитимного трафика.

Зачастую сетевые системы предотвращения вторжения – единственный способ защиты для нижних уровней АСУ ТП, так как установка антивирусных программ на АРМ, контроллеры и серверы может быть затруднена или невозможна в принципе. Подобные системы могут функционировать как в режиме перехвата и блокирова-

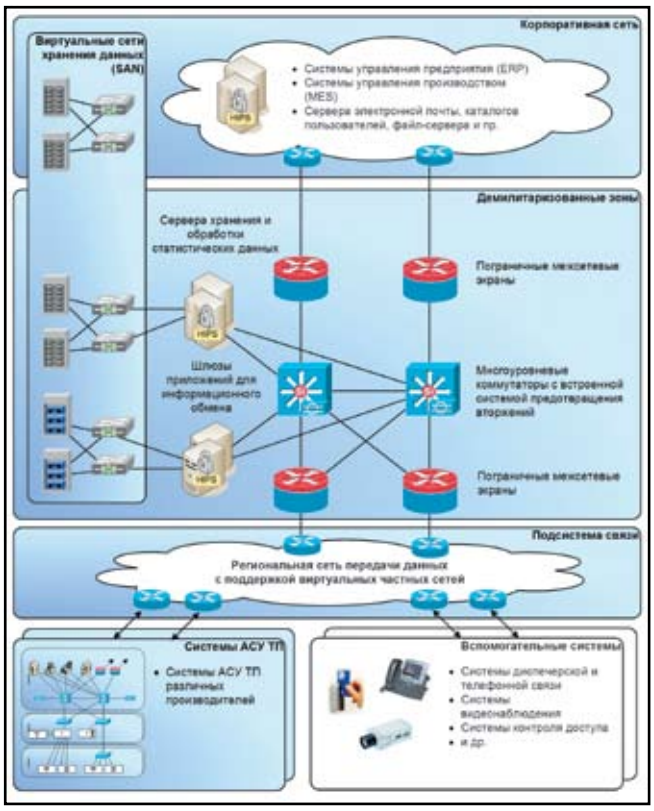

Рис. 2. Пример схемы организации связи и защиты информационного обмена с сетями общего пользования

ния нежелательных данных, так и в режиме прослушивания, сигнализируя о прохождении нежелательного трафика на консоль системы безопасности.

Необходимо кратко остановиться на общих вопросах, которые играют важную роль в построении комплексной системы безопасности АСУ ТП. Поддерживание приемлемого уровня информационной безопасности системы – процесс перманентный, что связано с постоянным появлением новых уязвимостей и угроз или модернизацией АСУ ТП.

Значительно повышают уровень защиты такие меры, как:

- регулярный аудит безопасности АСУ ТП;
- контроль настроек АСУ ТП и систем безопасности;
- поддерживание процедур резервного копирования и восстановления после отказов;
- управление конфигурациями;
- управление рисками ИБ;
- следование рекомендациям производителей оборудования и ПО;
- мониторинг событий ИБ;
- обучение и тренинг персонала.

Таким образом, использование зарекомендовавшей себя архитектуры информационной системы и АСУ ТП, комплексного подхода в вопросе обеспечения безопасности, эшелонирование защиты по уровням, применение различных типов средств защиты совместно с обеспечением отказоустойчивости и доступности и соблюдение принципов разумной достаточности позволяют обеспечить безопасное и надежное взаимодействие АСУ ТП с другими системами.

А. А. Гречин,
компания Cisco

НОВОСТИ

Новое решение для администрирования BI-приложений и хранилищ данных

Корпорация IBM представила новый интегрированный комплекс программных продуктов, который поможет клиентам лучше управлять производительностью информационных хранилищ. Пакет DB2 Warehouse Performance Management Suite предлагает передовые средства формирования отчетов и анализа использования данных и систем, которые позволят предприятиям быстрее и проще развертывать, администрировать и масштабировать приложения для бизнес-анализа (Business Intelligence) и хранилищ данных (Data Warehouse).

Новое решение IBM для управления производительностью предоставит компаниям возможность максимально эффективно использовать ресурсы своих базовых систем, а также новые функции DB2 Warehouse 9.5 для управления экстремальными рабочими нагрузками. Кроме того, это ПО дает возможность эффективно управлять сложными средами Business Intelligence и Data Warehouse на основе комплексного, всестороннего мониторинга, позволяющего получать полное представление обо всех аспектах жизненного цикла данных – от перемещения данных, конфигураций баз данных и систем и качества программного кода до поведения пользователей и приложений, а также потребностей в расширении инфраструктуры хранения и бизнес-анализа.

IBM сотрудничает с компанией Appfluent Technology с целью расширения возможностей ПО DB2 Warehouse Performance Management и предоставления клиентам полного решения для управления жизненным циклом хранилищ данных, сочетающего средства повышения производительности Performance Optimization, включенные в DB2 Warehouse, с новой функцией Performance Monitoring на базе программного обеспечения Appfluent для мониторинга и анализа рабочих нагрузок.

Объединяя технологию фонового мониторинга запросов и средства анализа рабочих нагрузок Appfluent с функциями DB2 Warehouse в области мониторинга, углубленного анализа и оптимизации, IBM предоставляет клиентам возможность получать важнейшую информацию, необходимую для управления жизненным циклом приложений, систем, процессов и действий пользователей.

"Новый комплекс Performance Management Suite будет поддерживать реализацию нашей инициативы Dynamic Warehousing, предоставляя клиентам самый полный в отрасли набор инструментов для обеспечения максимальной производительности хранилищ данных, – отметил Арвинд Кришна (Arvind Krishna), вице-президент подразделения IBM Data Services. – Эти новые возможности обеспечивают клиентам IBM беспрецедентный уровень понимания того, как функционируют приложения и инфраструктура бизнес-анализа и хранения данных, чтобы лучше управлять ими".

Новый комплекс IBM DB2 Warehouse Performance Management Suite был специально разработан для того, чтобы предоставить организациям возможность проще расширять свои среды хранения данных и справляться с растущими потребностями в выполнении бизнес-анализа в масштабе всего предприятия. Предлагаемая методика позволит организациям понимать влияние различных приложений для бизнес-анализа на базовую информационную инфраструктуру и эффективнее поддерживать расширение своих хранилищ данных.

Новая версия CPCI-компьютеров жесткого исполнения

Компания Kontron и ее стратегический партнер в России "РТСофт" начали поставку новой версии популярных одноплатных компьютеров жесткого исполнения в стандарте 3U CompactPCI с двухъядерным процессором – CP307-E2. Новинка отличается высокой вычислительной производительностью при низком уровне энергопотребления за счет применения процессора Intel Core Duo и способна работать при температурах от -40°C до +85°C.

Одноплатный компьютер CP307-E2 – это идеальный компонент для построения систем с длительным жизненным циклом, таких как автоматизированные системы управления, оборонные комплексы, робототехника, системы видеонаблюдения и сбора данных, различные встраиваемые системы аэрокосмического, транспортного и морского назначения.

Запаянные непосредственно на плату CP307-E2 микросхемы процессора и оперативной памяти, а также отсутствие вентиляторов позволяют эксплуатировать компьютер в самых неблагоприятных условиях (удары, вибрация, расширенный температурный диапазон).

Помимо двухъядерного процессора Intel Core Duo (1,2 ГГц), компьютер CP307-E2 оснащен высокопроизводительной памятью DDR2-SDRAM (до 4 Гбайт) с частотой 533 МГц. Обмен данными с портами Ethernet обеспечивается по высокоскоростным каналам PCI Express.