Бевалекс

Актуальные вопросы обеспечения информационной безопасности промышленных АСУ ТП

как критически важных объектов информатизации (КВОИ) с использованием ПАК «Цитадель»

Базелев Вячеслав Юрьевич,
руководитель направления
информационной
безопасности
СП «Бевалекс» ООО

1. Компьютеры ненадежны, но люди еще ненадежнее.
2. Любая система, зависящая от человеческой надежности, ненадежна.
3. Число ошибок, которые нельзя обнаружить, бесконечно в противовес числу ошибок, которые можно обнаружить, — оно конечно по определению.
4. В поиски повышения надежности будут вкладываться средства до тех пор, пока они не превысят величину убытков от неизбежных ошибок или пока кто-нибудь не потребует, чтобы была сделана хоть какая-то полезная работа.

Законы ненадежности Джилба

Производство современной конкурентоспособной высокотехнологичной продукции или предоставление ресурсов, к примеру, в топливно-энергетической сфере, невозможно представить без использования автоматизированных систем управления технологическим процессом (АСУ ТП), предназначенных для выработки и реализации управляющих воздействий на совокупность технологического оборудования и реализованных на нем по соответствующим инструкциям или регламентам технологических производственных процессов.

В настоящее время АСУ ТП характеризуются:

- унификацией и стандартизацией сетевых (общепринятых в ИТ-сфере) и индустриальных технологий (протоколов);
- созданием и внедрением АСУ ТП на базе серийно выпускаемых промышленных контроллеров, совместимых с персональными компьютерами и серверным оборудованием со специальным прикладным программным обеспечением;
- заменой аппаратных помещений на серверные или центры обработки данных (ЦОД).

На современном предприятии инженеры подразделений АСУ отслеживают работу управляемых механизмов удаленно с автоматизированных рабочих мест. При этом работа, в большинстве своём, ведется под управлением операционных систем семейства Windows, к тому же, зачастую, с возможностью одновременного доступа во внешние сети (Интернет).

Результатом этих тенденций является то, что для АСУ ТП растет вероятность осуществления угроз извне. Примером служит широко обсуждаемое появление вредоносных программ типа «flame», «duqu» и «stuxnet» («червь», созданный конкретно под Siemens SCADA-систему SIMATIC WinCC). Изнутри АСУ ТП также более уязвимы, чем прежде, — доступ к устройствам АСУ ТП могут получить всё большее количество сотрудников с использованием стандартных методов и средств сетевого доступа, растет зависимость АСУ ТП от непреднамеренных ошибок и намеренных негативных действий персонала.

Получается, что все производства с использованием АСУ ТП в степени не меньшей, чем широко распространенные компьютерные информационные системы, нуждаются в защите.

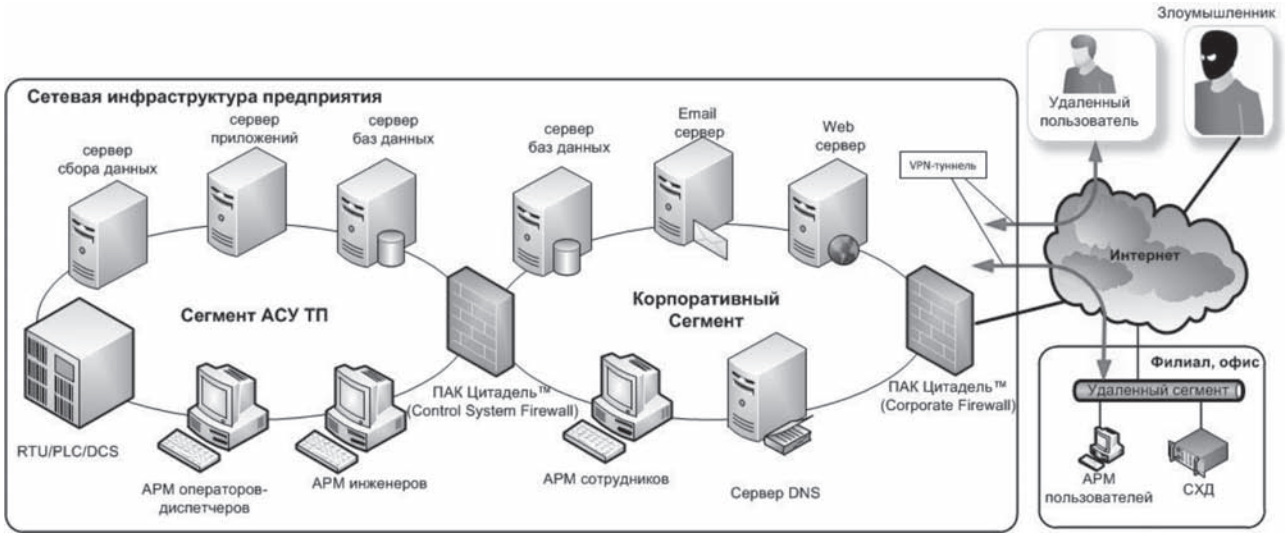

Рисунок 1. Вариант построения защищенной сетевой инфраструктуры предприятия, имеющего АСУ ТП

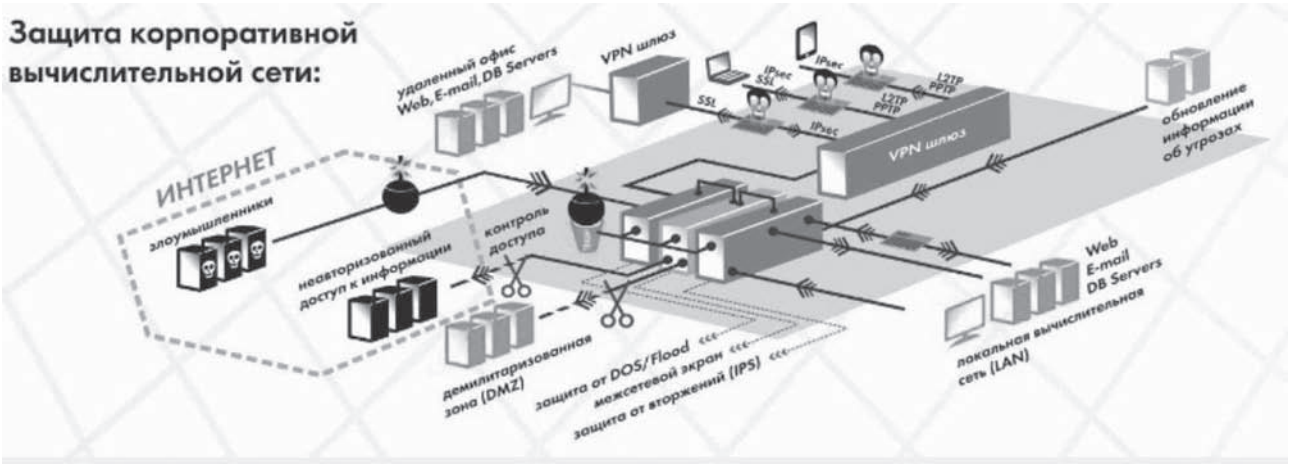

Рисунок 2. Вариант построения защищенной сетевой инфраструктуры на базе ПАК Цитадель™

Как организовать защиту АСУ ТП?

Следуя лучшим мировым практикам, при построении сетевой структуры предприятия, имеющего АСУ ТП, СП «Бевалекс» ООО предлагает пользоваться передовыми методиками в области управления ИТ и прислушаться к следующим рекомендациям:

Рекомендация 1

- *защищать корпоративную подсистему от «внешних» сетей межсетевым экраном **(Corporate Firewall)** (см. рисунок 1);*
- *отделять информационную подсистему, в которой происходит обработка данных АСУ ТП, от корпоративной подсистемы межсетевым экраном **(Control System Firewall)**.*

Указанный вариант построения защищенной системы позволит минимизировать риски, связанные с влиянием на АСУ ТП следующих видов угроз:

- подмена данных и модификация данных;
- "replay"-атаки;
- перехват информации (в том числе ключевой).

Рекомендация 2

В работе межсетевого экрана, «защищающего» сегмент АСУ ТП, акцент следует делать на обеспечение надежности, а именно: защиту от различного типа атак, направленных на выход из строя оборудования, каналов связи (DOS/DDOS, переполнение буфера, обнуление данных). А в работе межсетевого экрана, «закрывающего» корпоративный сегмент, наряду с обеспечением надежности важна защита конфиденциальных данных предприятия.

В качестве устройств, реализующих функции межсетевого экранирования, — Corporate Firewall и Control System Firewall — СП «Бевалекс» ООО предлагает использовать программно-аппаратный комплекс «Цитадель» ТУ BY 100944292.011-2011 (далее — ПАК Цитадель™) в составе:

– сервер Бевалекс™ (система менеджмента качества СТБ ISO 9001-2009);

– программное обеспечение «Astaro Security Gateway Software Network Appliance версия 8»[1], прошедшее проверку на соответствие требованиям безопасности (экспертное заключение № 281 от 19.09.2011 г. Оперативно-аналитического центра при Президенте Республики Беларусь).

При этом Intel-совместимая аппаратная платформа ПАК Цитадель™ является конфигурируемой и масштабируемой по производительности, а также количеству интерфейсов, ОЗУ, объему и RAID НЖМД, формату и типоразмеру соответственно текущим и перспективным потребностям предприятия, то есть наращиваемой согласно планируемому росту производственной нагрузки. Указанное свойство позволяет не только экономить средства предприятия при модернизации, но и относительно недорого проводить ремонт (замену) комплектующих из состава ПАК Цитадель™.

Рекомендация 3

Необходимо обеспечить высокий уровень отказоустойчивости системы и бесперебойное питание оборудования.

ПАК Цитадель™ позволяет настроить систему «горячего» резерва на случай сбоя основной системы (активно-пассивная конфигурация). А также создать кластер, распределяющий сетевой трафик между узлами в составе определенной группы (активно-активная конфигурация), с целью оптимизации использования ресурсов и ускорения вычислений (рисунок 3).

В качестве системы, обеспечивающей высокий уровень доступности, может использоваться кластер, состоящий из двух и более узлов на базе

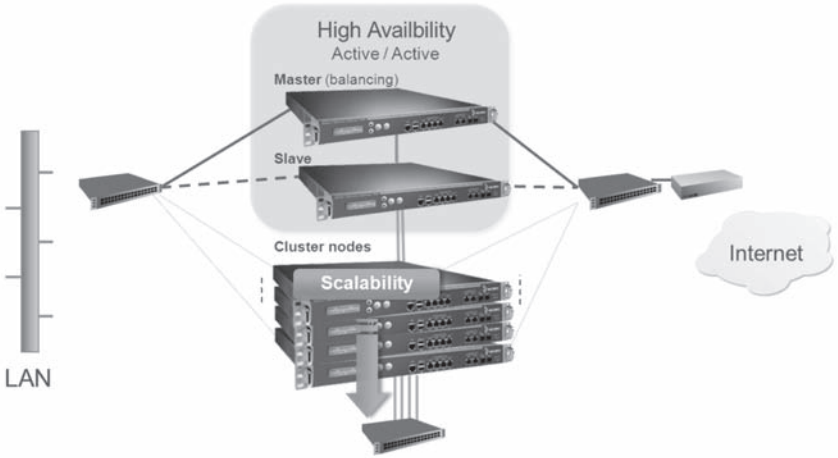

Рисунок 3. Работа ПАК Цитадель™ в режиме обеспечения отказоустойчивости

[1] Возможна поставка и установка программного обеспечения в виде виртуальной машины (сертифицировано VMware и Citrix)

ПАК Цитадель™.

Каждому узлу кластера назначается одна из следующих ролей:

– главный узел: главная система в составе кластера/конфигурации с «горячим» резервом, отвечает за синхронизацию и распределение данных.

– ведомый узел: резервная система в составе кластера/конфигурации с «горячим» резервом, принимает на себя функции главного узла в случае его сбоя.

– рабочий узел: обычный узел кластера, занимающийся только обработкой данных.

Все узлы осуществляют мониторинг состояния друг друга с помощью, так называемых, сигналов Heartbeat — периодически отправляемых многоадресных пакетов UDP, которые позволяют проверить, активен ли другой узел. Если по техническим причинам узел не отправляет этот пакет, его объявляют недоступным. В зависимости от роли, назначенной вышедшему из строя узлу, конфигурация меняется следующим образом:

– в случае сбоя главного узла его место занимает ведомый узел, а рабочий узел с самым высоким показателем готовности становится ведомым узлом;

– в случае сбоя ведомого узла его место занимает рабочий узел с самым высоким показателем готовности;

– в случае сбоя рабочего узла возможно снижение производительности по причине уменьшения количества доступных процессоров. Это событие не оказывает влияния на отказоустойчивость.

Бесперебойное питание оборудования достигается тем, что связь между устройством ИБП и ПАК Цитадель™ осуществляется через интерфейс USB. Как только устройство ИБП начинает работу с использованием батареи, администратору отправляется уведомление. Если сбой питания сохраняется в течение более длительного периода времени и напряжение устройства ИБП приближается к критическому значению, администратору отправляется другое сообщение — «ПАК Цитадель™ отключится автоматически».

Рекомендация 4

Руководителям предприятий и лицам, ответственным за информационную безопасность, стоит понимать, что построение системы информационной безопасности — это организационно-технический процесс, начинающийся с разработки соответствующих внутренних документов.

В противном случае возможно появление серьёзных инцидентов из-за, казалось бы, незначительных факторов:

– не произведённого вовремя обновления системного программного обеспечения какого-либо модуля АСУ ПК;

– доступа на территорию предприятия неуполномоченных лиц или нерегламентированного доступа сотрудников в нерабочее время;

– проведение сервисных работ с сетевыми устройствами или устройствами системы защиты информации в штатном режиме в рабочие часы.

Рекомендация 5

После выполнения всех рекомендаций вернуться к рассмотрению рекомендации №1, так как обеспечение информационной безопасности — это циклический процесс.

Подводя итог, сообщаем, что ПАК Цитадель™ включает в себя базовые функции межсетевого экранирования, NAT, удаленного доступа по протоколам PPTP/L2TP, а также опциональные дополнительные функции, активируемые исходя из потребностей пользователя.

Таким образом, для ПАК Цитадель™, в качестве Control System Firewall (см. рисунок 1), достаточно активировать функции Network Security (Сетевая безопасность). При этом будут обеспечены: защита информационной системы предприятия от различного рода сетевых атак (IPS, AntiDoS), возможность резервирования ширины канала и поддержка набора протоколов туннелирования для создания удаленных соединений (SSL Remote Access, IPSec Remote Access), интеграция с серверами Active Directory, eDirectory, RADIUS, TACACS+, LDAP). А на ПАК Цитадель™, защищающий корпоративный сегмент Corporate Firewall (см. рисунок 1), целесообразно дополнительно к Network Security возложить функции:

– Web Security (Безопасность веб-технологий) — URL-фильтрация, антивирусное сканирование при работе в веб-средах, Spyware Protection, сканирование HTTPS, IM/P2P-фильтрация.

– Mail Security (Безопасность электронной почты) — защита электронной почты, принимаемой и отправляемой из сети (Anti Spam, Antivirus, Email Encryption);

– Web Application Security (Безопасность веб-приложений) — обеспечение защиты URL-адресов от переопределения, механизмов «обратного прокси», идентификации и предотвращения использования SQL-инъекций и межсайтового скриптинга, направленных против находящихся в сети веб-серверов и их приложений;

К сожалению, это не значит, что покупка одного, двух или более устройств ПАК Цитадель™ или любого другого средства обеспечения безопасности является панацеей от инцидентов информационной безопасности. Единственный путь обеспечения комплексной и системной безопасности — отношение к информационной безопасности как к процессу.

При выборе ПАК Цитадель™ в качестве средства защиты корпоративной сети и АСУ ТП предприятие получает:

– возможность построения отказоустойчивых решений;

– возможность одновременного централизованного управления несколькими ПАК Цитадель™;

– наличие функций балансировки нагрузки;

– управление качеством сервисов (QoS, quality of service);

– гибкость в выборе функциональных модулей;

– возможность использования резервных каналов доступа во внешние сети (с поддержкой UMTS/3G-модемов);

– встроенные средства резервного копирования и восстановления;

– возможность сохранения и восстановления полной конфигурации в одном файле;

– мониторинг, анализ и полный контроль трафика, используемого отдельными пользователями, отделами, сетевыми узлами, приложениями;

– развитые средства формирования отчетов, настраиваемый уровень детализации отчетов.

При построении систем информационной безопасности СП «Бевалекс» ООО в своей работе руководствуется:

– международными стандартами и лучшими практиками (COBIT, ITIL, ISO);

– нормативно-правовыми актами Республики Беларусь;

– принципами уважения к своим клиентам.

СП «Бевалекс» ООО
220137, г.Минск, ул. Солтыса, 191
Тел.: (17) 330-16-16
Факс: (17) 330-16-30
E-mail: info@bevalex.by
www.bevalex.by