Информзащита
Системный интегратор

Особенности обеспечения информационной безопасности АСУ ТП

Спасенных Елизавета,
компания «Информзащита»

Справка ТБ

Спасенных Елизавета Михайловна, менеджер по развитию бизнеса ЗАО НИП «Информзащита». Высшее образование: специалист по защите информации (НИЯУ МИФИ); экономист-менеджер в ИТ отрасли (НИЯУ МИФИ). Значительный опыт работы консультантом на проектах по защите персональных данных, анализу рисков, разработке нормативных документов, защите АСУ ТП, анализу эффективности бизнес-процессов и др.

Каждый сотый объект информационных систем подвергался кибиратакам. Каждый тринадцатый подозревается в наличии реализованной уязвимости. Безопасность каждого третьего подвергается сомнению специалистами, которые не знают, были ли их ресурсы атакованы, или нет. Таковы результаты исследования компании Symantec[1] в области защиты критически важных объектов.

То же исследование содержит результаты анализа уровня защищенности по различным направлениям обеспечения безопасности. В соответствии с ним, российские компании существенно проигрывают западным по степени реализации мер по защите сетей, мониторингу событий безопасности, контролю доступа и аудиту информационной безопасности. Аналогичная тенденция прослеживается и в области осведомленности о защищенности автоматизированных систем управления технологическими процессами (АСУ ТП).

Обеспечение информационной безопасности АСУ ТП предполагает некоторые специфические аспекты. Они связаны с условиями эксплуатации систем и долгим жизненным циклом используемых технологий. На практике это влечет за собой:

– использование нетиповых физических топологий

– большое число устройств специального назначения с ограниченной функциональностью

– большое количество устаревшего оборудования

– сложности установки антивирусных средств

– недостаточные механизмы авторизации, аутентификации, логирования, мониторинга и т.д.

Учет особенностей функционирования АСУ ТП существенно затрудняет создание эффективной системы защиты. Однако это вовсе не означает, что реализовывать меры защиты не нужно. Возможные последствия от угроз, связанных с использованием вредоносного программного обеспечения, известные инциденты со Stuxnet и Duqu свидетельствуют об обратном. Построение комплексной системы защиты АСУ ТП позволяет минимизировать риски информационной безопасности.

Построение системы защиты должно начинаться с понимания назначения, функционала и особенностей работы АСУ ТП. На первом этапе составляются перечень бизнес-процессов, реализуемых системой, описания информационных потоков, выявляются «узкие» места, потенциальные угрозы и нарушители. К последним могут относиться обслуживающий персонал, аудиторы и контролеры, администраторы и ИТ персонал центрального офиса, лица, официально допущенные в контролируемую зону, разработчики, хакеры, лица, осуществляющие коммерческую разведку и другие.

Затем выявляются факторы, которые способствуют реализации угроз нарушения свойств доступности, целостности и конфиденциальности информации, обрабатываемой в АСУ ТП. На практике самыми распространенными уязвимостями являются:

– предоставление удаленного доступа в технологическую сеть

– несоблюдение правил сегментации сети

– недостаточные требования по безопасности к службе поддержки и разработчикам

– ошибки администрирования и известные уязвимости программного обеспечения

– возможность установки модифицированной прошивки PLC или несанкционированной смены настроек

– использование паролей по умолчанию

– недостаточное использование средств аутентификации, шифрования, контроля целостности и т.д.

Результатом анализа бизнес-процессов, угроз, уязвимостей и потенциальных нарушителей должны стать требования к обеспечению информационной безопасности. Они должны основываться не только на особенностях работы АСУ ТП и бизнес-процессов, но также учитывать требования законодательства и регуляторов. Целесообразно использовать рекомендации международных стандартов и практик. Сформированный подход к обеспечению информационной безопасности АСУ ТП должен быть комплексным и включать требования к реализации организационных, технических, физических и технологических мер защиты.

На основании сформированных требований осуществляется проектирование системы защиты и ее дальнейшее внедрение. Проектируемая система должна охватывать все уровни функционирования АСУ ТП:

– IP сети — на данном уровне должны использоваться стандартные механизмы защиты сетевой инфраструктуры (межсетевое экранирование, антивирусная защита, патч- менеджмент, IPS, VPN, DMZ и другие). Выбор средств защиты определяется на основании предъявленных требований к мерам, средствам и процессам обеспечения информационной безопасности АСУ ТП.

– PLC, датчики, устройства и инструменты, обеспечивающие реализацию технологического процесса. Защита на данных уровнях, осуществляется в соответствии со стандартами безопасности производителей оборудования и общим подходом к обеспечению информационной безопасности АСУ ТП.

С целью совершенствования системы защиты необходимо обеспечить регулярное проведение аудита, анализа рисков, анализа эффективности мер защиты. Данные процессы должны охватывать все направления, которые могут прямо или косвенно влиять на защищенность АСУ ТП. Это позволит своевременно реагировать на новые угрозы и уязвимости АСУ ТП.

Внедрение комплекса организационных мер, технических средств и процессов управления информационной безопасности АСУ ТП позволит минимизировать риски, связанные с прямыми финансовыми и репутационными потерями, остановками или нарушениями технологического процесса, ущербом окружающей среды, а также возможными человеческими жертвами.

ЗАО НИП «ИНФОРМЗАЩИТА»
127018 Москва, ул. Образцова, д. 38
Тел.: (495) 980-2345
E-mail: market@infosec.ru
www.infosec.ru

[1] Статистика 2010: Защита объектов критической инфраструктуры в России и мире. Угрозы и их последствия на примере кибератаки на ядерный завод в Иране