ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ

В.Н. Мухаметшин
Научный руководитель: И.П. Скирневский, ассистент кафедры АиКС
Томский политехнический университет
valerim@live.ru

Введение

В настоящее время, вопрос безопасности автоматизированных систем управления (АСУ ТП) является одним из важнейших. Безопасность таких систем в целом, и тем более на критически важных объектах – одна из наиболее острых проблем на сегодняшний день. АСУ ТП может быть реализована как одноуровневая или локальная, либо как централизованная, включающая несколько контроллеров с программируемой логикой и автоматизированных рабочих мест, оснащенных, обычно, системой сбора и визуализации данных SCADA-системой в зависимости от типа предприятия и решаемых задач.

Обеспечение безопасности АСУ ТП – совокупность согласованных по цели, задачам, месту и времени мероприятий, направленных на нейтрализацию внутренних и внешних угроз безопасности информации в АСУ ТП и на минимизацию ущерба от возможной реализации таких угроз. Ранее, системы управления, в начале их появления, были изолированными. Переход таких систем в разряд открытых представил новые возможности, способные сократить расходы и повысить производительность:

- удалённый доступ для обслуживания системы;
- интегрирование специальных приложений автоматизации;
- мгновенный доступ к информации.

Однако вместе с использованием открытых стандартов в современных системах управления, обозначились и новые угрозы. Все угрозы, направленные на АСУ ТП, можно разделить на 3 класса:

- угрозы техногенного характера;
- угрозы антропогенного характера;
- угрозы несанкционированного доступа.

В зависимости от особенностей функционирования АСУ ТП и её назначения состав угроз безопасности может различаться. Взаимодействие компонентов системы управления с локальной вычислительной сетью предприятия с целью передачи информации о состоянии системы – может рассматриваться как угроза несанкционированного доступа к АСУ ТП. Угрозы техногенного характера, обусловливаются физическими воздействиями на АСУ ТП, защита от угроз техногенного характера заключается в применении систем физической защиты, средств обеспечения безопасности, осуществляются меры, предотвращающие несанкционированный доступ нарушителей на охраняемую территорию и обеспечивающие технический контроль к основным компонентам АСУ ТП. Угрозы антропогенного характера – угрозы преднамеренного и непреднамеренного действия людей, обслуживающих АСУ ТП, в том числе ошибки персонала или ошибки в организации работ с компонентами АСУ ТП. В этой связи, обязательным становится формирование выделенных технологических сетей передачи данных и использование специальных средств защиты – средств межсетевого экранирования, обнаружения вторжений криптографической защиты каналов связи. Можно выделить следующие источники угроз для АСУ ТП:

- обслуживающий персонал;
- отдельные посторонние лица или группы лиц;
- террористические организации;
- представители организаций и конкурирующих структур;
- иностранные разведывательные и специальные службы (шпионаж).

Говоря об угрозах, стоит выделить типы уязвимости АСУ ТП: уязвимость системной политики и процедур безопасности, уязвимость платформ, уязвимость сетей. Часто в применяемой системе безопасности системная политика не учитывается вообще или учитывается недостаточным образом, что может привести к уязвимости системы.

Большинство систем не имеет защитного антивирусного программного обеспечения, поскольку его базу необходимо часто обновлять, иначе оно неспособно оставаться современным и эффективным, ранее платформы использовали собственные сетевые протоколы, которые должны были обеспечить безопасность, поскольку встроенные функции безопасности отсутствуют. Уязвимые места платформ можно разделить на следующие категории [1]:

- уязвимость конфигурации платформы;
- уязвимость технических средств платформы;
- уязвимость программного обеспечения платформы;
- уязвимость защиты платформы от вредоносного ПО.

Уязвимости в сетях обычно возникают вследствие недоработок при проектировании, недостаточного технического обслуживания сетей, а

также при недостаточном понимании сетевых требований.

Безопасность автоматизированных систем управления

Особенностью автоматизированных систем управления является работа в режиме реального времени. Большой проблемой построения системы безопасности АСУ ТП становится процесс выявления ключевых рисков, те риски, ради снижения которых внедряются средства защиты, оказываются минимальными по сравнению с риском остановки оборудования, связанным с внедрением средств защиты. Персонал, ответственный за работу, защиту и поддержку АСУ ТП, в большинстве случаев отлично разбирается в вопросах физической безопасности на объекте и абсолютно не знаком с целями и задачами информационной безопасности (ИБ). Проекты по ИБ ориентированы на защиту определенных ресурсов, будь то централизованное хранилище данных или защита конечных точек сети. Обеспечение безопасности АСУ ТП – комплексная задача, которая должна решаться на административном, процедурном уровнях и уровне программно-технических мер. Важность безопасности Главная цель мер административного уровня – формирование программы работ по обеспечению ИБ АСУ ТП с учетом общей концепции защиты [2]. Цель процедурного уровня ИБ АСУ ТП является определение и выполнение требований по обеспечению безопасности компонентов АСУ ТП за счет формирования и принятия пакета организационной документации. На уровне программно-технических мер реализуются управление доступом, обеспечение целостности и безопасного межсетевого взаимодействия, антивирусная защита, анализ защищенности, обнаружение вторжений и общее управление системой.

Для разных проектов применяются различные средства защиты. В случае с технологическими сетями критичны как отдельные логические контроллеры, так и сервер централизованного управления, который имеет доступ к логическим контроллерам, поэтому любой проект будет требовать высококвалифицированной защиты всего объекта, без возможности дробления системы безопасности. АСУ ТП взаимодействует с аппаратным устройством, поэтому внедрение любого средства защиты потребует определенных этапов тестирования решений и их воздействия на канал взаимодействия с, что еще больше усложняет проект. При этом в эксплуатируемых системах отсутствуют средства обновления указанного функционала. В результате ряд старых решений имеют целые классы уязвимостей, которые непременно требуют закрытия.

Мониторинг сетевой инфраструктуры АСУ ТП часто ограничивается выявлением [3] неисправностей или сбоев сетевого оборудования. В отсутствии средств обнаружения вторжений невозможно определять атаки на сетевые ресурсы и своевременно противодействовать им.С учетом требований (ГОСТ 34.603-92) к непрерывности технологических процессов рекомендуется использовать системы пассивного обнаружения вторжений, которые будут осуществлять анализ сетевого трафика [4] без вмешательства в процессы передачи данных.Осведомленность сотрудников в области информационной безопасности является еще одной существенной проблемой для безопасности АСУ ТП. Знание и соблюдение простейших правил информационной безопасности может предотвратить как минимум реализацию непреднамеренных угроз безопасности АСУ ТП, а осознание того, что служба безопасности отслеживает и контролирует действия обслуживающего персонала, может снизить вероятность реализации преднамеренных угроз. Одной из важных проблем для обеспечения безопасности промышленных объектов является жизненный цикл решений, применяемых для АСУ ТП.

Заключение

Функционирование автоматизированной системы управления техническими процессами затрагивает не только нормальную деятельность предприятий, использующих подобные системы, но и отдельного человека. Вероятность атаки на подобные системы ниже, чем на многие другие, но ответственность, связанная с их защитой, несоизмеримо выше. Важно понимать, что такие системы уязвимы, как и любые другие, что они также могут стать целью злоумышленников, но риски при этом гораздо более высоки, вплоть до нарушения работоспособности системы и остановки производства, не говоря о человеческих жертвах. АСУ ТП является сверхкритичным объектом, ведь даже её непродолжительная остановка может привести к очень тяжёлым последствиям, внимание к этой проблеме должно быть усилено.

Литература

1. Schneider-Electric – Журнал «Техническая коллекция Schneider Electric выпуск №36» [Электронный ресурс]. - Режим доступа: http://www.ops-ecat.schneider-electric.com, свободный.
2. Издательская группа «Индустрия» – Аналитический журнал «Нефть и Капитал» №03/2013 [Электронный ресурс]. - Режим доступа: http://www.indpg.ru/nik/2013/03, свободный.
3. PC Week Review: «Информационная безопасность критически важных объектов» [Электронный ресурс]. - Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=155219, свободный.
4. Digital Security: «Современные угрозы информационной безопасности АСУ ТП» [Электронный ресурс]. - Режим доступа: http://dsec.ru/ipm-research-center/article/how_not_to_disconnect_the_city_modern_threats_to_information_security_apcs, свободный.