СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ ТП

Демидович Д.И.

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Скудняков Ю.А.– доцент каф. ИСиТ, к.т.н., доцент

В данной работе рассматриваются основные проблемы информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) и меры их нейтрализации.

Под защитой информации в автоматизированных системах управления технологическим процессом (АСУ ТП) следует понимать комплекс практических взаимосвязанных мероприятий, направленных на предотвращение раскрытия, несанкционированного использования, изменения, искажения, уничтожения, копирования, шпионажа и прочих негативных вмешательств в АСУ ТП.

Типичная АСУ ТП имеет от двух до трѐх уровней сетевой архитектуры. На современных предприятиях всѐ чаще реализуется единая среда управления в корпоративной локальной

вычислительной сети (ЛВС), в которой размещены компьютеры и системы, посредством которых осуществляется управление организационной и финансовой деятельностью. Часть компьютеров ЛВС может иметь доступ к серверам АСУ ТП, содержащим накапливаемую о технологическом процессе информацию. Сеть АСУ ТП может иметь верхний уровень (станции операторов и инженеров АСУ ТП, серверы баз данных, серверы приложений), средний уровень (программируемые логические контроллеры) и нижний уровень (датчики сбора данных и исполнительные механизмы). Связь между уровнями обеспечивается коммуникационными серверами или контроллерами. Доступ к датчикам осуществляется по протоколам и полевым шинам (RS485, RS232, Fieldbus, ProfiBus, CAN, OPC и др.). Современной тенденцией является использование IP и Ethernet сетей на верхнем и среднем уровнях. Всѐ чаще промышленные устройства имеют Ethernet порты и IP протоколы, которые используются на всех уровнях сети АСУ ТП. Таким образом, особенностью сетей АСУ ТП является использование в дополнение к IP ещѐ и специализированных протоколов, которые если и затрудняют проникновение, то, как показывают инциденты, не для профессионалов. Следует отметить, что соединение по специальным протоколам, как правило, не предусматривает средств защиты. Приведѐм перечень основных угроз АСУ ТП, отмеченных в реальных инцидентах: – атаки на SCADA; – атаки на PLC, уязвимости PLC (пароль по умолчанию, неавторизованный доступ к фирменному программному обеспечению, удалѐнное изменение пароля и т. д.); – атаки на инфраструктуру и оперативную систему (вирусы, троянские программы, черви, DDoS-атаки, ARP-спуфинг – перехват трафика после объявления себя маршрутизатором); – атаки на протоколы, уязвимость протоколов (OPC – переполнение буфера, нестойкий пароль); – атаки баз данных (несанкционированный доступ, SQL инъекция); – практические атаки (переполнение буфера – Buffer Overflow, раскрытие информации – Information Disclose, отказ в доступе – Denial of Access, отказ в управлении – Denial of Control, отказ в представлении – Denial of View, подмена представления – Manipulation of View).

Вследствие длительности эксплуатации АСУ ТП (разработка и эксплуатация могут составлять более десяти лет) и существенного изменения состава и качества современных угроз необходимо проектировать и реализовывать информационную безопасность систем с учѐтом тенденций развития киберугроз. С другой стороны, необходимо проводить регулярную работу по нейтрализации возникающих или потенциальных угроз на работающих системах. Совокупность нейтрализующих мер можно разделить на две группы: административно-организационные и программно-технические. Первая группа мер связана с формированием программы работ по обеспечению информационной безопасности (ИБ) АСУ ТП и разработкой набора документов, которые регламентируют высокоуровневый подход по обеспечению ИБ, а также описывают политику развития системы ИБ АСУ ТП. Кроме того, формируется пакет организационной документации, направленной на создание и поддержание режима ИБ АСУ ТП. Программно-технические меры образуют основной набор средств обеспечения ИБ АСУ ТП. На этом уровне реализуются следующие сервисы ИБ: управление доступом, обеспечение целостности, обеспечение безопасного межсетевого взаимодействия, антивирусная защита, анализ защищѐнности, обнаружение вторжений, управление системой ИБ (непрерывный мониторинг состояния, выявление инцидентов, реагирование). Конкретные требования к перечисленным сервисам предъявляются на основании анализа обрабатываемой информации и оценки угроз безопасности АСУ ТП. Каждая группа мер в зависимости от необходимости и возможностей предприятия может осуществляться на одном из трѐх уровней. Базовый уровень включает механизмы, традиционные для большинства информационных систем. Средний уровень предполагает выполнение начальных мероприятий, обеспечивающих реализацию управляемых защитных функций по обеспечению ИБ. На расширенном (высоком) уровне реализуются мероприятия, поддерживающие и расширяющие базовый и средний уровень, но для их реализации может потребоваться дополнительная экспертиза. Так, для первой группы мер на базовом уровне предполагается разработка документов, описывающих политику кибербезопасности, внедрение политик и процедур из государственных стандартов по безопасности критически важных объектов. На среднем уровне ведутся работы по внедрению лучших индустриальных практик, осуществляется контроль выполнения политик и процедур. На расширенном уровне внедряется процесс непрерывного улучшения политик и процедур ИБ, периодически проводится обучение и аудит. На базовом уровне требуется внедрение электронного периметра и отключение всех необязательных для основного процесса соединений. Составляется и поддерживается в актуальном состоянии список критических объектов. На среднем уровне электронный периметр разделяется на зоны: ЛВС АСУ ТП, демилитаризованная зона и зона корпоративной ЛВС. Анализируется и минимизируется количество ресурсов, доступных одновременно из сети АСУ ТП и сети корпоративной ЛВС. Поставщики оборудования и интеграторы периодически проводят обучение сотрудников. Так, схема зонирования в архитектуре Cisco SAFE for PCN (Process Control Network) разделена на 6 уровней.

Зона ЛВС АСУ ТП (уровень 0 – уровень 3) отделяет критичные системы АСУ ТП и состоит из нескольких функциональных зон. Нулевой уровень – датчики сбора данных и исполнительные механизмы. Первый уровень – узлы коммутации, обеспечивающие подключение датчиков к ПЛК. Второй-третий уровень – ПЛК, рабочие места операторов, серверы хранения данных. Могут использоваться межсетевые экраны и IDS. Демилитаризованная зона обеспечивает связность корпоративной ЛВС и ЛВС АСУ ТП. Она

содержит только некритичные системы, которым необходим доступ к корпоративной ЛВС и ЛВС АСУ ТП, состоит из нескольких функциональных зон и отделена межсетевыми экранами и IPS. Зона корпоративной ЛВС содержит типичные бизнес-приложения: почта, АСУП (четвертый уровень), Интернет (пятый уровень). На расширенном уровне осуществляется внедрение VLAN, PVLAN, NIPS/HIPS, средств обнаружения аномалий и вторжений, интеллектуальных коммутаторов и т. п. В области защиты систем управления (Control Systems, SCADA) в настоящий момент существует целый ряд стандартов и рекомендаций.

При этом каких-либо обязательных требований к соответствию определенным критериям безопасности для коммерческих компаний не предъявляется. Процесс с выпуском стандартов по информационной безопасности АСУ ТП явно затягивается, и, таким образом, сохраняется некоторая неопределѐнность для интеграторов и структур, обеспечивающих безопасность АСУ ТП. Однако перед научным сообществом поставлены серьѐзные задачи в области развития фундаментальной и прикладной науки, технологий и средств обеспечения безопасности автоматизированных систем управления.

Список использованных источников:

1. URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 &tabid=2 (дата обращения: 01.04.20).

2. URL: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (дата обращения: 01.04.20).