Безопасность АСУ ТП*

Б. Н. Пищик
Конструкторско-технологический институт вычислительной техники СО РАН, Новосибирск, Россия
e-mail: Boris.Pishchik@gmail.com

Дан краткий обзор проблем информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП). Приводится статистика уязвимостей, освещены проблемы безопасности, основные угрозы и меры их нейтрализации, перечисляются документы, регламентирующие работы по информационной безопасности АСУ ТП.

Ключевые слова: информационная безопасность, АСУ ТП.

Несмотря на аварии с катастрофическими последствиями, проблема безопасности автоматизированных систем управления технологическими процессами на промышленных предприятиях никогда не стояла так остро, как в последние несколько лет.

Широкий интерес к проблеме безопасности промышленных систем возник после инцидентов с компьютерными вирусами Stuxnet [1], Duqu [2], Flame [3], атаковавшими иранские ядерные объекты, госучреждения и промышленные объекты Индии, Китая и других стран. До этих инцидентов считалось, что в работу АСУ ТП довольно трудно вмешаться. Такое представление базировалось на нескольких постулатах: программное обеспечение каждой АСУ ТП уникально и закрыто; локальная сеть АСУ ТП решает проблемы ограничения доступа; проникновение в АСУ ТП связано с большими интеллектуальными затратами, а денежное вознаграждение для злоумышленника не очевидно.

Изучение структуры и используемых программно-аппаратных средств современных АСУ ТП показало, что за последнее время произошли существенные изменения [4]. Повсеместно используется широко распространенное системное программное обеспечение (ПО): ОС Windows, TCP/IP протоколы и т. п., которое вместе со своими достоинствами принесло и свои недостатки — уязвимости. Нередко в сети АСУ ТП появляются компьютеры, имеющие доступ в Интернет.

Атаки на промышленные системы проводятся с помощью программных средств, разработанных не только хакерами-одиночками (внешними, а чаще внутренними пользователями систем), но и организованными группами высококвалифицированных специалистов. Так, специалисты по информационной безопасности, анализирующие Stuxnet [5], отмечают, что данный вирус содержал целевой код, удовлетворяющий целому ряду специфических требований и реализующий полноценную атаку на системы АСУ ТП производства компании Siemens. В частности, для реализации потенциала нападения вирус требовал наличия частотных конверторов производства двух компаний — Vacon (Финляндия) и Fararo Paya (Иран), работающих на частотах от 807 до 1210 Гц. Наличие подобных требований позволило большинству экспертов, исследовавших данный

*Работа частично поддержана РФФИ (грант 11-07-00561).

код, сделать вывод о том, что вирус предназначался для точечной атаки вполне определённого производства или ряда производств. Согласно анализу, проведённому специалистами компании Symantec, вредоносный код Stuxnet-а реализовывал атаку сразу на нескольких уровнях: на уровне операционных систем Windows, ПО управления АСУ ТП Siemens WinCC/PCS 7 и непосредственно программируемых логических контроллеров (ПЛК) Siemens S7-300, обслуживающих конверторы частоты (которые, в свою очередь, управляли скоростью вращения электромоторов).

По данным компании Siemens, из 15 случаев заражения вирусом в Германии ни в одном случае не было проникновения в ПЛК, так как не совпали параметры, в то время как на иранских объектах это удалось. Таким образом, атака была тщательно подготовлена специалистами, имеющими весьма специальные знания об объектах атаки. Это позволяет сделать предположение об организованной и спланированной акции, что непохоже на действия злоумышленников-одиночек.

Появился даже новый термин — "кибервойна" (cyberwarfare), упоминаемый в СМИ в связи проблемой защиты систем АСУ ТП на инфраструктурных объектах и опасных производствах. В ряде стран (например, в США и Китае) созданы специализированные подразделения для выведения из строя инфраструктуры на стороне потенциального противника. Так, в Ираке была дистанционно выведена из строя система радиолокационного обнаружения воздушных целей.

Таким образом, повсеместное использование компьютерного оборудования в управлении промышленными предприятиями выдвигает и повышенные требования к информационной безопасности (ИБ) таких систем.

Обзор состояния безопасности АСУ ТП, проведённый компанией Positive Technologies в 2012 г., показал довольно тревожную картину [6]. Резко увеличивается число обнаруженных уязвимостей. С 2010 по 2012 г. установлено в 20 раз больше уязвимостей, чем за предыдущие 5 лет. Каждая пятая уязвимость устраняется дольше месяца. 50 % уязвимостей позволяют хакеру запустить выполнение кода. Для 35 % уязвимостей есть эксплойты. Более 40 % доступных в Интернет систем могут взломать хакеры-любители. Больше всего уязвимостей обнаруживается у известных производителей: Siemens 42, Schneider Electric 30, Advantech/Broadwin 22, Invensys Wonderware 15, General Electric 15.

Что касается стран, то доли уязвимых АСУ ТП (обеспечивающих доступ к АСУ ТП из Интернет) составили: Швейцария 100 %, Чешская республика 86 %, Швеция 67 %, Великобритания 60 %, Россия 50 %, США 41 %, Германия 20 %.

Нельзя сказать, что разработчики АСУ ТП совсем не уделяют внимания информационной безопасности.

Основные проблемы информационной безопасности АСУТП, выделяемые экспертами [5, 7], проистекают:

— из слабой защиты от несанкционированного доступа (пароли);
— недекларированных возможностей SCADA;
— отсутствия контроля управляющих воздействий (совокупность параметров);
— использования беспроводных коммуникаций (некриптостойкое шифрование WiFi);
— отсутствия чётких границ между разными сегментами сети;
— несвоевременного или некорректного обновления программного обеспечения;
— дистанционных методов управления;
— Web-технологий, используемых на верхнем уровне АСУ ТП;

— отказа даже от минимальных мер безопасности (нередко ради удобства и производительности компании отказываются от установки не только, например, антивирусной, но и даже парольной защиты критически важных активов);
— распространения Windows в качестве основной операционной системы для рабочих станций и даже для серверов;
— разработки в расчёте на выполнение в доверенной среде закрытых индустриальных сетей;
— создания систем без учёта лучших практик разработки безопасного кода;
— человеческого фактора — слабой дисциплины сотрудников.

Типичная АСУ ТП имеет от двух до трёх уровней сетевой архитектуры. На современных предприятиях всё чаще реализуется единая среда управления в корпоративной ЛВС, в которой размещены компьютеры и системы, посредством которых осуществляется управление организационной и финансовой деятельностью. Часть компьютеров этой сети может иметь доступ к серверам АСУ ТП, содержащим накапливаемую о технологическом процессе информацию.

Сеть собственно 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. Всё 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 ещё 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.

Приведём 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, удалённое изменение пароля и т. д.);
— атаки на инфраструктуру и оперативную систему (вирусы, троянские программы, черви, DoS- и DDos-атаки, ARP-спуфинг — перехват трафика после объявления себя маршрутизатором);
— атаки на протоколы, уязвимость протоколов (OPC — переполнение буфера, нестойкий пароль — 2011 г.);
— 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).

Среди всех типов уязвимых компонентов АСУ ТП лидируют SCADA — 87 %, далее следуют системы, обеспечивающие человеко-машинные интерфейсы, — 49 %, реже обнаруживаются уязвимости в программируемых контроллерах — 20 % и совсем редко в используемых протоколах — 1 %.

Доли уязвимостей по типам распределились следующим образом: переполнение буфера 36 %, аутентификация/управление ключами 22.86 %, уязвимости Web-приложений (сервер 10.86 %, клиент 9.14 %), удаленное исполнение кода 13.14 %.

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 учётом 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 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 защищённости, 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 трёх уровней. Базовый уровень включает механизмы, традиционные для большинства информационных систем. Средний уровень предполагает выполнение начальных тактических 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. Для иллюстрации разных уровней второй группы мер рассмотрим сервис обеспечения безопасного межсетевого взаимодействия.

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 [8].

Зона ЛВС АСУ ТП (уровень 0 — уровень 3) отделяет критичные системы АСУ ТП и состоит из нескольких функциональных минизон. Нулевой уровнь — датчики сбора данных и исполнительные механизмы. Первый уровнь — 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 минизон 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 (ControlSystems, SCADA) в настоящий момент существует целый ряд стандартов и рекомендаций [7, 9, 10]. Их можно классифицировать следующим образом:

1) отраслевые решения:
— стандарты NERC для систем управления электрическими сетями,
— стандарты ChemITC для химической индустрии,
— Cisco SAFE for PCN — стандарты Газпрома;
2) рекомендации общего уровня (стандарты NIST, ISA и др.):
— ISA S99 — Комитет общества приборостроения, системотехники и автоматизации (ISA),
— NIST PCSRF Security Capabilities Profile for Industrial Control Systems,
— IEC 61784-4,
— КСИИ ФСТЭК.

При этом каких-либо обязательных требований к соответствию определенным критериям безопасности для коммерческих компаний не предъявляется.

Процесс с выпуском российских стандартов по информационной безопасности АСУ ТП явно затягивается, и, таким образом, сохраняется некоторая неопределённость для интеграторов и ИТ структур, обеспечивающих безопасность АСУ ТП. Однако перед научным сообществом в документе “Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации” [11] поставлены определённые и серьёзные задачи в области развития фундаментальной и прикладной науки, технологий и средств обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры.

Список литературы

[1] Symantec. W32.Stuxnet.
URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=2 (дата обращения: 02.07.13)

[2] Duqu: следующий Stuxnet. Symantec.
URL: http://www.symantec.com/ru/ru/outbreak/?id=stuxnet (дата обращения: 20.07.13)

[3] Gostev A. The Flame: Questions and Answers. SECURELIST.
URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers (дата обращения: 20.07.12)

[4] Аникеенко В. Безопасность АСУ ТП и контроль привилегированных пользователей. URL: http://www.anti-malware.ru/node/11899 (дата обращения: 20.07.13)

[5] Воронцов А. Автоматизированные системы управления технологическими процессами // Вопр. безопасности: информ. бюл. комп. "Инфосистемы Джет". Информационная безопасность промышленных объектов.
URL: http://www.jetinfo.ru/jetinfo_arhiv/informatsionnaya-bezopasnost-promyshlennykh-obektov/2011/?nid=77f3dbdaa8dfb77077c0888a712a3e1a (дата обращения: 20.07.13)

[6] Грицай Г., Тиморин А., Гольцев Ю. и др. Безопасность промышленных систем в цифрах v2.1*. URL: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (дата обращения: 10.07.13)

[7] Лукацкий А. Стандарты безопасности АСУ ТП.
URL: http://www.slideshare.net/CiscoRu/ss-8690963 (дата обращения: 20.06.13)

[8] Cisco Inc. Архитектура и стратегия информационной безопасности Cisco // Информационный бюллетень.
URL: http://www.cisco.com/web/RU/downloads/Cisco_Security_Architecture.pdf (дата обращения: 20.07.13)

[9] Лукацкий А. Обзор мировых стандартов ИБ АСУ ТП и советы по их применимости в российских условиях. URL: http://www.slideshare.net/lukatsky/ss-14591209 (дата обращения: 20.06.13)

[10] Безопасность АСУ ТП: от слов к делу. URL: http://www.slideshare.net/lukatsky/ss-14279925 (дата обращения: 20.06.13)

[11] Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. URL: http://www.scrf.gov.ru/documents/6/113.html (дата обращения: 29.07.13)

Поступила в редакцию 29 ноября 2013 г.