Фундамент безопасности АСУ ТП:
от правовых основ до особых методик

Виктор ГАВРИЛОВ,
ведущий научный сотрудник – главный специалист по безопасности информации, ИПИ РАН

При подготовке к международному экономическому форуму в Женеве международная группа экспертов, определяя глобальные риски 2013 г., выделила среди них угрозу возникновения «цифровых пожаров», имея в виду как рост компьютерной преступности (на 30% в 2012 г.), так и использование ИТ-технологий для неконтролируемого вирусного распространения информации провокационного или экстремистского характера. Озабоченность экспертного сообщества вызывает активное внедрение информационных технологий для нужд государственного и военного управления, управления технологическими и иными процессами реального времени, в том числе на критически важных объектах информационной инфраструктуры, не подкрепляемое адекватными мерами защиты. При этом для информационно-аналитических систем, обрабатывающих информацию ограниченного доступа, вопросы защиты в достаточной мере проработаны, а реализация установленных требований зависит в большей мере от правовой культуры и финансового состояния владельца системы.

Проблемы защиты информации в системах управления реального времени, в том числе автоматизированных системах управления технологическими процессами (АСУ ТП), долгое время находились вне зоны внимания специалистов по информационной безопасности. Определенным толчком, пробудившим интерес к данной тематике, послужила широко обсуждавшаяся в печати вирусная атака Stucksnet. По сути, был поставлен масштабный натурный эксперимент, показавший, к каким катастрофическим последствиям может привести, казалось бы, невинное отступление от правил эксплуатации защищенной автоматизированной системы, а также невысокую эффективность распространенных систем защиты, построенных на идеологии защиты периметра.

Проведенные по результатам этого и других менее значимых происшествий исследования [8, 9] показали крайне низкий уровень информационной безопасности АСУ ТП. Так, с 2010 г. в 20 раз возросло количество обнаруженных уязвимостей используемого программного обеспечения, только в 2012 г. их выявлено больше, чем за весь предшествующий период. При этом половина уязвимостей дает возможность хакеру запускать произвольный исполняемый код (для 35% уязвимостей есть эксплойты, что позволяет взломать защиту даже малоквалифицированному нарушителю). Более чем 90% уязвимостей имеют средний либо высокий уровень опасности, а в 9% случаев их использование не вызывает трудностей. В трети проверенных систем недостатки в системе безопасности связаны с ошибками конфигурации, использованием стандартных технологических паролей и т. п., что свидетельствует о безответственности обслуживающего персонала.

Осознание сложившегося положения привело к появлению целого ряда документов органов государственной власти России. Советом Безопасности Российской Федерации в 2005 г. принята «Система признаков критически важных объектов…» [1], на основании которой распоряжением Правительства РФ утвержден перечень таких объектов [2]. ФСТЭК России разработан пакет нормативных документов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры [3–6], включающий методику определения актуальных угроз и базовую модель угроз безопасности, а также общие требования и рекомендации по обеспечению безопасности информации. Наконец, Советом Безопасности разработаны и в феврале 2012 г. утверждены Президентом Российской Федерации «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации [7]. Указанный документ определяет факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем

управления критически важных объектов, ее основные принципы и направления, а также основные механизмы и этапы ее реализации. Координация деятельности федеральных органов исполнительной власти по реализации «Основных направлений…» возложена на федеральный орган исполнительной власти в области обеспечения безопасности. В январе 2013 г. Указом Президента РФ [8] на Федеральную службу безопасности возложена задача создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, что предусмотрено «Основными направлениями…» [7]. В настоящее время проходит согласование проект Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [8], разработанный Федеральной службой безопасности Российской Федерации во исполнение положений «Основных направлений…». Проектом определяются цели и принципы обеспечения безопасности критической информационной инфраструктуры Российской Федерации, полномочия органов государственной власти в этой сфере, порядок категорирования объектов критической информационной инфраструктуры и оценки их защищенности, источники финансирования мероприятий по обеспечению безопасности. Таким образом, к настоящему времени заложена определенная правовая база для организации деятельности по защите информации АСУ ТП.

Вместе с тем разработка средств и систем защиты информации в АСУ ТП потребует подготовки целого ряда нормативных и методических документов. Одной из первоочередных задач в этом направлении является установление соответствия между категориями критически важных объектов и существующими классами систем защиты информации либо введение новой классификации систем защиты для таких объектов. Второй подход представляется предпочтительным, поскольку существующая классификация систем защиты привязана к степени конфиденциальности информации, но в АСУ ТП критически важных объектов даже высокой категории опасности может отсутствовать информация ограниченного доступа. Уровень защиты такого объекта, очевидно, должен быть достаточно высоким. Система защиты информации АСУ ТП и иных систем реального времени имеет специфические особенности, основная из которых заключается в том, что на первый план выходит обеспечение функциональной безопасности и таких традиционных характеристик безопасности, как целостность и доступность ресурсов системы. Под функциональной безопасностью здесь подразумевается состояние АСУ ТП, при котором риск наступления нежелательных (потенциально опасных) событий в системе снижен до приемлемого уровня. Действующие нормативные и методические документы по защите информации ориентированы в основном на обеспечение конфиденциальности информации, а такие характеристики безопасности, как целостность и доступность, играют вспомогательную роль. Однако в АСУ ТП нарушение доступности отдельных ресурсов или целостности критически важных параметров технологического процесса зачастую может привести к катастрофическим последствиям. Функциональная безопасность в литературе нередко отождествляется с надежностью функционирования системы в условиях как случайных сбоев и неисправностей, так и преднамеренных действий потенциального нарушителя. Но в случае ошибок реализации алгоритма технологических процессов либо в его описании даже надежная работа программно-технических средств системы не спасает от негативных последствий. Таким образом, важными элементами в обеспечении информационной безопасности АСУ ТП являются анализ алгоритма функционирования АСУ и верификация реализующего его программного обеспечения. Решение первой из указанных задач невозможно без активного участия профильных министерств и ведомств, а также владельца критически важного объекта. В целях удешевления и ускорения проведения соответствующих работ по безопасности информации необходима разработка отраслевых стандартов и типовых решений АСУ ТП. Проблема верификации современного программного обеспечения с учетом высокой трудоемкости этой работы требует научного разрешения и разработки соответствующих методических рекомендаций.

Проблема обеспечения безопасности информации в АСУ ТП носит межведомственный, комплексный характер, требует разработки целого ряда документов федерального и отраслевых уровней правового, нормативного и методического характера, а также типовых программно-технических решений. ■

Литература

1. Совет Безопасности 08.11.2005. Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий.
2. Распоряжение Правительства Российской Федерации № 411 от 23. 03. 2006 г. «Об утверждении предварительного перечня ключевых систем информационной инфраструктуры Российской Федерации».
3. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).
4. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).
5. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).
6. Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 19.11.2007).
7. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом Российской Федерации 03.02.2012).
8. *Грицай Г., Тиморин А., Ильин Р., Гордейчик С., Карпин А.* Безопасность промышленных систем в цифрах. V. 2.1. 2012.
9. Отчет NSS Labs' Vulnerability Threat Report 2013 г.