УДК 658.512+65.011.5+004.056.5

Гончар С.Ф.

В статті формулюються завдання з дослідження та розробки систем захисту інформації територіально розподілених автоматизованих систем управління технологічними процесами.

В статье формулируются задачи по исследованию и разработке систем защиты информации территориально распределенных автоматизированных систем управления технологическими процессами.

:

This article formulates the problem in the exploration and development of information security geographically distributed automated process control systems.

Специфика больших распределенных автоматизированных систем управления технологическим процессом (АСУ ТП) такова, что большинство систем, которые используются сегодня, были разработаны и спроектированы до появления компьютерных сетей и Интернета. Эти системы разрабатывались для обеспечения производительности, безопасности и гибкости. Поэтому до недавнего времени безопасность автоматизированных систем управления технологическим процессом подразумевала физический контроль доступа к инфраструктуре промышленного объекта [1].

Количество угроз и уязвимостей для систем АСУ ТП продолжает с каждым годом увеличиваться. Это связано с переходом от автоматизации отдельных установок до автоматизации в рамках всего предприятия. Создаются также и географически распределенные автоматизированные системы управления технологическим процессом, протяженность линий связи для которых может составлять тысячи километров.

Большое значение имеет использование стандартных технологий, которые имеют хорошо известные уязвимые места. Среди них надо назвать такие протоколы и стандарты, как IP, Ethernet, HTTP, XML, DCOM, .NET и т.д. Увеличивает область возможных атак и широкое распространение стандартных операционных систем, таких как Linux, Windows, а также коммуникационного оборудования: мультиплексоров, маршрутизаторов, коммутаторов и т.п.[2].

Все перечисленные уязвимые места, помноженные на значимость объектов, делают автоматизированные системы управления технологическим процессом весьма привлекательной целью как для недобросовестных конкурентов, так и для террористических организаций или недружественных стран.

Одним из первых средств для заражения промышленных объектов стал специализированный компьютерный вирус “Stuxnet”, который был обнаружен на компьютерах сотрудников иранской АЭС в Бушере и стал первой из вредоносных программ, способных инфицировать автоматизированные системы управления промышленных предприятий. Первые сообщения об обнаружении этого вируса появились в июне 2010 года [3]. Впервые в истории не только промышленного сектора, но и кибератак “Stuxnet” смог разрушить инфраструктуру промышленного объекта, существенно повысив риски техногенных катастроф. “Stuxnet” был только началом в разработке целого класса вирусного программного обеспечения. И если первоначально вирус был направлен против определенных объектов и физических устройств, то нынешние модификации вируса существенно расширили вектор атак, нацеленных на промышленный сектор.

Тот факт, что вирус может собирать различные сведения о новой “среде обитания” и обмениваться информацией с удаленным сервером, ранее приводил экспертов к выводу о том, что его главная цель – это промышленный шпионаж. Однако для осуществления основной миссии “Stuxnet” не нужен выход в Интернет, тем более что в закрытых внутренних сетях большинства предприятий, где существуют требования повышенной безопасности, доступ во всемирную сеть просто отсутствует. Вирус может действовать автономно – распространяться по внутренней сети и заражать съемные носители информации [3].

География распространения вируса также наводит на определенные мысли. Согласно отчету за август 2010 года словацкой компании “ESET”, работающей на рынке защиты информации и разработки антивирусов, на Иран приходится около 52% случаев заражения, около 17% – на Индонезию, около 12% – на Индию. По сообщению компании “Siemens”, вирус был обнаружен в компьютерных системах 14 промышленных предприятий Германии, но никакого вреда он не нанес и в производственный цикл не вмешивался [3].

Эксперты сходятся во мнении, что сам факт появления такой программы, даже если она пока не нанесла значительный ущерб, может стать угрозой для любого государства.

Угрозы для автоматизированных систем управления технологическим процессом разнообразные: от случайных действий некомпетентных сотрудников до умышленных действий террористических групп. Существующие угрозы для АСУ ТП возможно разделить на внешние, внутренние влияния и шпионаж.

К внешним воздействиям следует отнести целенаправленные атаки киберпреступников. Известны случаи, когда причиной атаки были соревнования между хакерами. Если десять лет назад для проведения подобной атаки была нужна серьезная подготовка и знание специфики строения промышленных сетей, то сегодня, с появлением “Stuxnet”, злоумышленники имеют готовые вредоносные скрипты и программы под специализированные протоколы. В ряде случаев внешним воздействием может стать не целевое проникновения в технологическую сеть, а просто массовое заражение.

Целью таких атак может стать нарушение работоспособности или шантаж компании.

Внутренние атаки опасны тем, что сотрудник внутри компании, даже не обладая специальными знаниями, имеет представление о специфике системы и принципе работы промышленной инфраструктуры. В роли такого сотрудника могут выступать как сотрудники организации, так и сотрудники компании-партнера, например, технический сотруд-

ник разработчика системы SCADA. Методами социальной инженерии злоумышленник имеет возможность попадать непосредственно внутрь сети, поскольку внутри компании всегда есть недовольные и обиженные, а также те, которые желают повысить уровень своего благосостояния. Используя сотрудников компании, можно распространять целевые вирусы на съемных носителях или дезинформировать сотрудников, которые имеют доступ к корпоративной сети в Интернет через средства обмена сообщениями.

Целью таких атак является вредоносное влияние на сеть, например, с отложенным результатом нарушения трудоспособности или аварии.

Шпионаж. Большие и критические промышленные объекты являются важной частью инфраструктуры государства, и поэтому компании промышленного сектора могут стать целью для разведок других стран. Вирус “Stuxnet”, разработанный под промышленные объекты, по одной из версий, был создан именно при поддержке военных ведомств и разведки. Получение всей доступной информации является неотъемлемой частью работы разведывательных управлений всех стран мира. Информация же о промышленных объектах является ключевой на случай возможных военных конфликтов различного масштаба. Реалии современного мира диктуют новые правила конкурентной борьбы, где компании ведут настоящую охоту за “важной информацией”. Промышленный шпионаж с появлением аналогичных средств “Stuxnet” выводит вероятность кражи или подмены данных на очень высокий уровень.

Целью шпионажа может стать компрометация информации или ее кража с последующим деструктивным использованием, до полной остановки и банкротства промышленного объекта.

В классической инфраструктуре информационных технологий давно существуют способы и методы противодействия описанным угрозам. Относительно автоматизированных систем управления технологическим процессом решения по защите должны быть сильно изменены с учетом специфики промышленных предприятий. Вследствие этого для ряда задач, например, в процессах реального времени, часто требуется не просто доработки средств защиты, а их разработка с нуля с учетом новых требований.

Автоматизированные системы управления технологическим процессом имеют целый ряд отличий от традиционных систем информационных технологий (систем ИТ) [1]. Основными становятся риски для безопасности жизни людей, нарушения критической инфраструктуры и финансовые потери в случае прекращения производства. Требования, предъявляемые к защите информации, могут противоречить алгоритму работы автоматизированных систем управления технологическим процессом.

1. Системы ИТ обычно требуют высокую пропускную способность и не критичны к временным задержкам (например, перезагрузка компонента), в то же время, автоматизированные системы управления технологическим процессом работают в режиме реального времени с жестко заданными временными параметрами и не требуют высокой пропускной способности.

2. В системе ИТ первоочередной задачей является конфиденциальность данных и их целостность. Для автоматизированных систем управления технологическим процессом, наряду с информационной безопасностью, приоритетным есть безопасность обслужи-

вающего персонала, сохранность оборудования, предотвращение производственных потерь.

3. В системе ИТ при реализации киберзащиты отсутствует взаимосвязь с физическими событиями. В свою очередь, в автоматизированных системах управления технологическим процессом может быть очень сложная взаимосвязь киберзащиты с физическими процессами и последствиями в промышленном секторе. Поэтому, все функции безопасности, интегрированные в автоматизированные системы управления технологическим процессом, должны быть протестированы на предмет отсутствия угрозы штатному функционированию системы.

4. В автоматизированных системах управления технологическим процессом очень критично время реакции системы на воздействие оператора.

5. Системы ИТ создаются с достаточным запасом ресурсов для поддержки дополнительных приложений по обеспечению безопасности. В то же время, автоматизированные системы управления технологическим процессом создаются для обеспечения промышленных процессов и, зачастую, не хватает ресурсов для поддержки приложений по обеспечению безопасности.

6. Обновления программного обеспечения в системах ИТ осуществляются, как правило, своевременно и, зачастую, автоматически. Обновления программного обеспечения автоматизированных систем управления технологическим процессом не могут быть реализованы своевременно, поскольку они должны быть тщательно проверены конечным пользователем приложения перед внедрением, а отключения индустриальных систем управления должны планироваться заблаговременно (дни, недели). Кроме того, автоматизированная система управления технологическим процессом может потребовать повторной проверки как часть процесса обновления.

Исходя из вышеизложенного, исследование и разработка систем защиты информации территориально распределенных АСУ ТП является сложной и важной проблемой, поскольку слишком большие риски и последствия могут быть катастрофическими.

Таким образом, задачи по исследованию и разработке систем защиты информации территориально-распределенных АСУ ТП могут быть сформулированы следующим образом:

1) проведение критического анализа методов и средств обнаружения угроз и оценки их опасности для территориально-распределенных автоматизированных систем управления технологическими процессами;

2) разработка и исследование моделей оценки рисков развития вероятных сценариев развития ситуации;

3) разработка методов моделирования комплексных систем защиты и обеспечения безопасности территориально распределенных автоматизированных систем управления технологическими процессами, которые соответствуют современному уровню развития информационных технологий и минимизация участия персонала в настройке и эксплуатации программно-аппаратных средств, входящих в их состав;

4) разработка методов построения специализированных информационно-аналитических систем обеспечения безопасности территориально распределенных автоматизированных систем управления технологическими процессами;

5) разработка и внедрение образцов специализированных информационно-аналитических систем поддержки принятия решений для обеспечения безопасности территориально распределенных автоматизированных систем управления технологическими процессами.

1. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. Recommendations of the National Institute of Standards and Technology. – Gaithersburg: NIST, 2011. – 155 p.

2. Industrial communication networks – Network and system security: IEC 62443. – Part 1-1: Terminology, concepts and models. – [Valid from 2009-07-30]. – Geneva: IEC, 2009, 121 p. – (International standard).

3. Конухов Д. Новый вид информационного оружия испытан на иранской ядерной инфраструктуре [Электронный ресурс] / Д. Конухов. – Режим доступа: http://ceness-russia.org/data/doc/Konukhov-Stuxnet.pdf.