Безопасность промышленных информационных систем

Часть 3

Стандарты по защите промышленных систем автоматизации

Мартин Нэдель, Дик Ойен

Во второй части данного руководства по информационной безопасности промышленных сетей были описаны различные типы вредоносного ПО и даны рекомендации по защите систем автоматизации.

Настоящая, заключительная, часть посвящена различным инициативам, посвященным созданию стандартов и других руководящих указаний по защите систем промышленной автоматизации, которые были инициированы за последние два года различными коллективами. Приведен обзор этих программ и результатов работы по ним, а также описание подхода рабочей группы МЭК TC65 WG10 к выработке технических проектов по защите систем управления в определенных ситуациях.

Учебное пособие

В настоящее время существует настоящий вал информации по безопасности информационных систем в целом. Кроме того, издан ряд официальных документов поставщиков решений в области автоматизации, в которых разъясняются различные аспекты защиты их систем. Однако наблюдается также и большой дефицит легкодоступной объективной рекомендательной информации о том, как обеспечить систематическую защиту систем управления и автоматизации от электронных атак.

Появление стандартов в этой области окажется очень полезным как для пользователей систем автоматизации, так и для их изготовителей, поскольку позволит им:

- оценивать объем работ по внедрению, сопровождению и эксплуатации механизмов и процедур обеспечения безопасности;
- формулировать задачи защиты на конкретном предприятии и определять функции и механизмы, которые должны предусмотреть поставщики и системные интеграторы;
- сравнивать полноту охвата различных видов угроз и стоимость предлагаемых решений по обеспечению безопасности;
- внедрять и эксплуатировать экономически эффективные механизмы защиты на группе предприятий или подразделений одного предприятия;
- контролировать соответствие систем защиты от информационных атак современному уровню.

Поставщики и системные интеграторы получат возможность:

- прогнозировать развитие требований к защите и разрабатывать соответствующие функции;
- создавать архитектуры средств обеспечения безопасности, пригодные для повторного использования в нескольких проектах; сократить за счет вышеуказанных факторов затраты на составление технических предложений, разработку и закупку устройств и приложений, поставляемых сторонними фирмами.

Основные инициативы в области стандартизации

Приведенный ниже обзор инициатив по стандартизации в области информационной безопасности промышленных систем составлен на основе [1] и [2].

ISA S99

Целью комитета SP99 Общества приборостроения, системотехники и автоматизации (ISA), носящего название «Защита технологических систем и систем управления» [1], является создание руководящих документов и стандарта (S99) по внедрению систем информационной безопасности в существующих промышленных системах управления и автоматизации.

Появление стандартов по обеспечению систематической защиты систем управления и автоматизации от электронных атак окажется очень полезным как для пользователей систем автоматизации, так и для их изготовителей.

ISA обладает правом на разработку стандартов для перерабатывающей промышленности, действующих в пределах США. Многие стандарты ISA применяются в рекомендательном порядке на международном уровне, а некоторые, такие как S88 и S95, утверждены в качестве международных стандартов.

Комитет SP99 начал работу в 2002 году. На первом этапе были разработаны два технических отчета, опубликованных весной 2004 года. Первый отчет, «Security Technologies for Manufacturing and Control Systems» («Технологии обеспечения безопасности для производственных систем и систем управления») [3], – это всестороннее исследование современного положения дел в технологиях и механизмах обеспечения безопасности с комментариями относительно их применимости на производстве. В нем рассмотрены следующие темы: аутентификация и авторизация; фильтрация/блокировка/ограничение доступа; шифрование и проверка корректности данных; аудит; измерения, контроль и обнаружение; операционные системы и программное обеспечение; физическая безопасность. Каждой технологии дается оценка по следующим показателям: уязвимые места, которые закрывает система; типовая схема развертывания; известные слабые места; применение в системах автоматизации; направления будущего развития; рекомендации; ссылки.

Во втором отчете, «Integrating Electronic Security into the Manufacturing and Control Systems Environment» («Интеграция средств электронной безопасности в производственные системы и системы управления») [4], даны рекомендации по выбору архитектуры систем безопасности, описаны организационные проблемы и механизмы внедрения систем управления безопасностью на промышленных предприятиях. Подход, выбранный в данном отчете, опирается на стандарт ISO/IEC 17799 [5]. Он содержит разделы, посвященные разработке программ обеспечения безопасности, политикам, оценке рисков, аудиту и проверкам, разработке, отбору и поставке, контрмерам, а также примеры политик и форм.

С лета 2004 года комитет SP99 работает над стандартом S99. Этот стандарт, главным образом, посвящен следующим вопросам:

- модернизации механизмов обеспечения безопасности на действующих предприятиях с использованием представленных на рынке компонентов без строгого выбора конкретной архитектуры;
- административным процессам и процессам эксплуатации базовой системы организационного управления.

Фактические процессы и архитектура системы безопасности будут, вероятно, адаптироваться под конкретные предприятия.

IAONA

Альянс промышленной автоматизации на основе открытых сетей (IAONA) объединяет по интересам пользователей и разработчиков промышленных систем связи. Совместная техническая

Таблица 1. Инициативы в области безопасности.

CIDX (http://www. cidx. org/CyberSecurity/) разрабатывает рекомендации по процедурам обеспечения безопасности в химической промышленности. Работа ведется в согласовании с ISA SP99. Деятельность CIDX в основном осуществляется в Северной Америке.
NAMUR (http://www. namur. de/en/694.php) выдает рекомендации по безопасному применению сетевых технологий в перерабатывающих отраслях промышленности. NAMUR действует в основном в Европе, наиболее активно – в Германии.
NERC (http://www. nerc. com/) – это североамериканский орган саморегламентирования для электроэнергетических компаний. Соответствие стандарту NERC 1200 и последующим стандартам CIP 002...009 в отношении управления безопасности обязательно для энергетических компаний Северной Америки.
CIGRE (www. cigre. org), Международный совет по крупным электроэнергетическим системам, ведет работу над вопросами информационной безопасности в ряде рабочих групп.
PCSRF (http://www. isd. mel. nist. gov/projects/processcontrol/), Форум по вопросам безопасности систем АСУ ТП, содействует сертификации компонентов перспективных систем управления по уровню безопасности в соответствии с ISO/IEC 15408 («Общие критерии»). Он поддерживается Национальным институтом стандартов и технологий США (NIST), который является официальным органом сертификации по ISO/IEC 15408 в США.
PCSF (https://www. pcsforum. org/), Форум по АСУ ТП, был основан в 2004 году в качестве посреднической инициативы по обмену информацией между другими программами и инициативами, работающими в этой области.

группа по безопасности[2] (JTWG-SE) этого альянса разработала формуляр безопасности, предназначенный для использования в качестве шаблона поставщиками систем и приборов автоматизации при документировании функций связи и обеспечения безопасности, а также особых требований, связанных с их продукцией. Эта информация может послужить ценным исходным материалом для разработчика архитектуры безопасности системы автоматизации при проектировании и выборе конфигурации необходимых механизмов безопасности на предприятии. Плюсом такого формуляра является то, что в нем концентрируется сжатая информация, связанная с вопросами безопасности, которую зачастую нелегко извлечь из документации поставщика.

МЭК

В начале 2004 Технический подкомитет 65C по цифровой связи (Digital Communications) Международной электротехнической комиссии, а точнее его рабочая группа WG13 по информационной безопасности, начали в рамках стандарта IEC 61784 работу над проблемами безопасности промышленных шин и других систем промышленных сетей. Эти вопросы рассмотрены в новой, четвертой части, озаглавленной «Digital data communications for measurement and control – Profiles for secure communications in industrial networks» («Цифровые системы передачи данных для целей измерения и управления – Методы защиты связи в промышленных сетях»).

В этой работе стало очевидным, что проблемы безопасности в системах автоматизации не могут быть решены лишь путем защиты средств связи при ориентации только на устройства полевого уровня. Вместо этого рабочая группа начала определение современных безопасных способов реализации некоторых распространенных процедур, применяемых в сетях и системах автоматизации, например, удаленного доступа по коммутируемой линии. Такие определения, получившие название наборов требований (requirement sets), включают аппаратно-независимое описание технических механизмов в контексте передовой архитектуры обеспечения безопасности, а также рекомендации по выбору конфигурации и эксплуатации таких механизмов. Этот подход более подробно рассмотрен далее в статье.

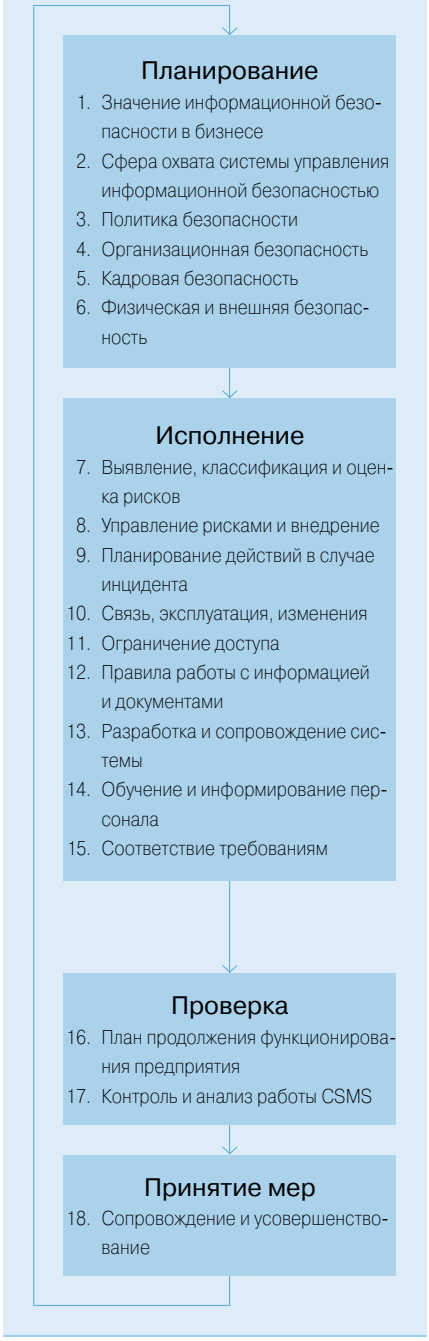
В дальнейшем работа группы была передана рабочей группе 10 технического комитета 65 (TC65 WG10) для оформления актуальной и необходимой деятельности в соответствии со структурой комитетов МЭК. Окончательная версия стандарта IEC 62443 под названием «Security for industrial process measurement and control – Network and system security» («Безопасность в промышленных системах измерения и управления – Безопасность сетей и систем») планируется к выходу в 2006 году. Последнее голосование относительно вступления в силу стандарта в качестве международного ожидается в первой половине 2007 года.

Некоторые другие инициативы в области безопасности кратко описаны в табл. 1.

Управление безопасностью на производстве согласно ISA S99

Технический отчет комитета SP99 общества ISA, TR99.00.01 «Security Technologies for Manufacturing and Control Systems» («Технологии обеспечения безопасности для производственных систем и систем управления») [3], содержит рекомендации по применимости широкого ряда технологий обеспечения безопасности. Рекомендации составлены на основе аккумулированного опыта специалистов в области безопасности, работающих как в компаниях-поставщиках решений, так и в компаниях-потребителях. Поскольку в отчете представлена аналитическая по своей природе информация, этот документ не является нормативным документом, соответствие которому можно определить количественно. Применимость информации в конкретной ситуации определяет читатель. Это превосходный документ как для тех, кто только начинает создавать механизмы безопасности, так и для тех, кто уже располагает опытом. Обновление отчета TR99.00.01 продолжается, однако содержащаяся в нем информация не войдет в состав стандартов S99.

1 Система управления информационной безопасностью CSMS.



В октябре 2005 года проекты двух из четырех частей стандарта S99 были уже почти готовы к общественному рассмотрению.

В части 1 дается определение терминов и описание моделей, применяемых при рассмотрении безопасности систем автоматизации. В части 2 даются рекомендации по созданию системы управления информационной безопасностью (cyber-security management system, CSMS). CSMS включает 18 основных элементов, которые организованы в виде постоянно повторяющегося жизненного цикла, включающего четыре этапа: планирование, исполнение, проверка, принятие мер. Система CSMS предоставлена консорциумом по обмену информацией в химической промышленности (Chemical Industry Data Exchange, CiDX) [7], в которой к системам автоматизации адаптированы четыре этапа из стандарта Великобритании BS 7799-2:2002 [6], а также определены 18 основных элементов. Система CMSM с ее составными элементами приведена на рис. 1. Ее циклическая структура явным образом определена на этапе 18, на котором сама программа обеспечения безопасности подвергается модификации на основе уроков, извлеченных в ходе осуществления предыдущих этапов.

Этап планирования (Plan):
Планирование программы обеспечения безопасности начинается с организации проекта на уровне предприятия, чтобы руководители высшего звена могли определить ясную политику верхнего уровня, санкционирующую внедрение программы.

Планируются меры организационной безопасности, при этом во внимание принимаются все отделы и сотрудники, имеющие дело с системой управления. На этой стадии определяются роли и ответственность в плане безопасности.

Безопасность связана с людьми: теми, кто обладает доступом к защищаемым объектам, теми, кто должен обеспечить защиту этих объектов, и теми, кто может подвергнуть их опасности. Кадровая безопасность определяет политику по работе с персоналом для оценки и поддержания благонадежности тех сотрудников, которые обладают существенными правами при доступе к объектам. Также необходимо спланировать меры физической и внешней безопасности. Разработка информационной безопасности ведется исходя из предположения, что предусмотрены мощные (но не абсолютные) преграды против физического воздействия.

На этапе планирования производится выявление, классификация и оценка рисков. Подробные методические указания по этим операциям даны в стандарте S99 и литературе, на которую в стандарте даны ссылки.

Этап исполнения (Do):
Оценка рисков приводит напрямую к этапу исполнения. На основе результатов оценки рисков ресурсы, выделенные на обеспечение безопасности, могут быть оптимальным образом применены для защиты действительно уязвимых мест.

Создаются процедуры, представляющие собой план действий в случае потенциальных инцидентов. При планировании действий должен быть определен момент, с которого возникает необходимость уведомления государственных органов о значительной угрозе населению.

Разрабатываются общие организационные политики и процедуры, охватывающие вопросы связи, эксплуатации системы и организации изменений.

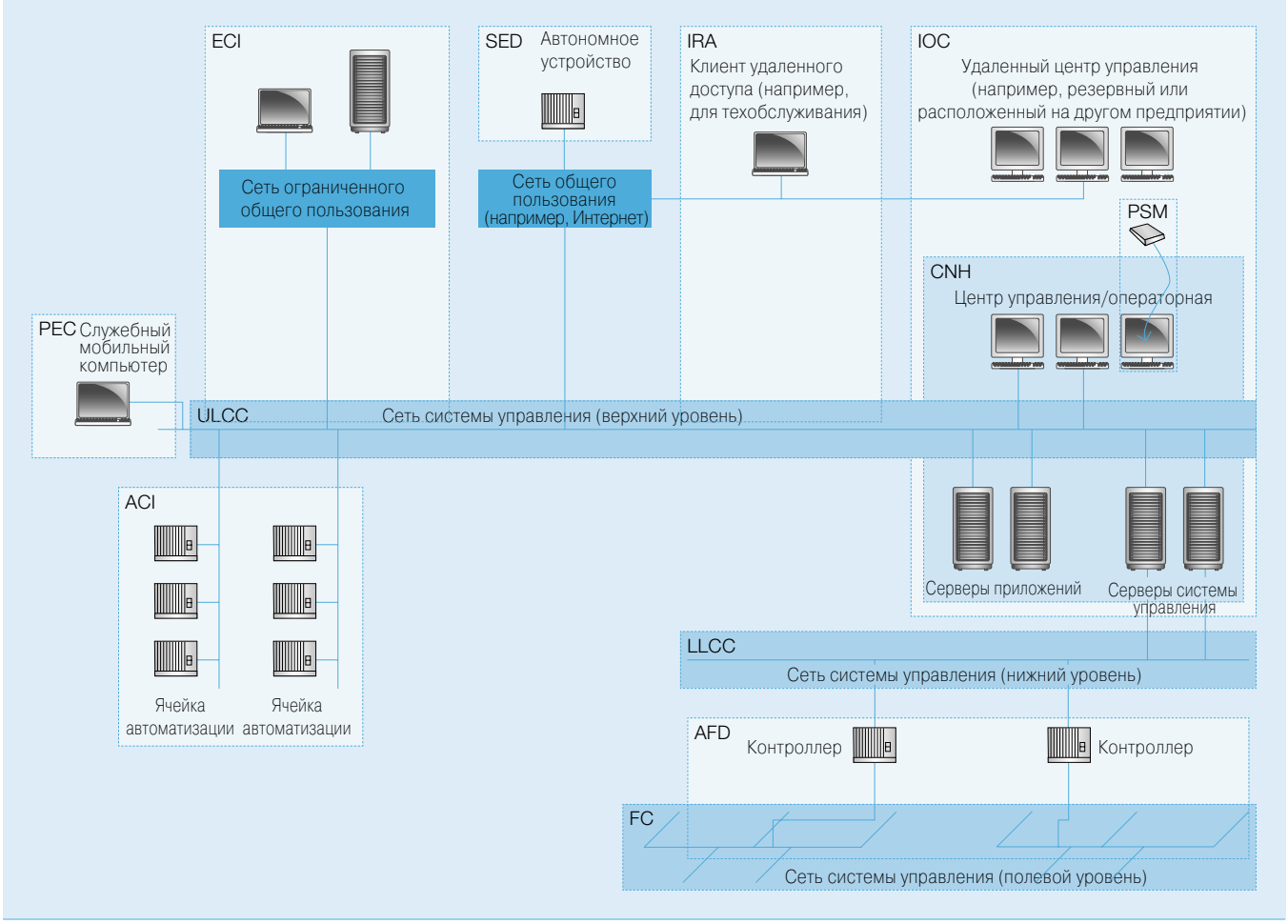
Ограничение доступа связано с определением привилегий, соответствующих различным ролям. На этой стадии также определяются процедуры ограничения прав доступа сотрудников по отношению к операциям и информации, не предусмотренных их привилегиями. Разрабатываются средства аутентификации, гарантирующие, что конкретный пользователь (сотрудник или программа) имеют соответствующие права доступа.

В правилах работы с информацией и документами задается классификация данных в отношении безопасности и определяются меры защиты. Вопросы безопасности, связанные с разработкой и сопровождением системы, также должны быть описаны политикой и процедурами.

Персонал должен пройти обучение соответствующим процедурам обеспечения безопасности, при этом все сотрудники обязаны проходить регулярные курсы переподготовки по общим вопросам безопасности. Соблюдение политик и процедур безопасности в различных отделах и каждым сотрудником должно постоянно контролироваться посредством текущего контроля и периодически – посредством аудита. При проверке соблюдения политик также должны учитываться внешние требования, такие как требования заказчиков, партнеров по договорным отношениям и регулирующих органов.

Этап проверки (Check):
Этап проверки включает разработку «Плана продолжения функционирования предприятия» и следование ему. Такой план определяет, как компания будет действовать в случае инцидентов, повлекших за собой крупный ущерб, остановку производства или катастрофические последствия для населения. На этапе проверки рассматриваются уроки, полученные при выполнении предыдущих пунктов программы.

2 Модульная архитектура безопасности. Каждый модуль может быть поставлен в соответствие определенным компонентам системы автоматизации и входящей в ее состав сети.



Этап принятия мер (Act):

Поскольку система CSMS предусматривает цикличность процесса, программа обеспечения безопасности подвергается пересмотру в соответствии с результатами этапа проверки. В части 2 стандарта S99 приведены более подробные рекомендации, а также 19 этапов создания системы CSMS. Задачей части 3 является выдача рекомендаций по эксплуатации системы CSMS.

Техническая архитектура безопасности на основе IEC 62443

Стандарт IEC 62443, главным образом, посвящен техническим (на системном уровне) аспектам архитектуры безопасности и тем самым дополняет аппаратно и программно-ориентированные инициативы, такие как IAONA, и процедурные рекомендации SP99 и NERC.

Благодаря непрекращающейся работе по стандартизации механизмов и архитектур в области безопасности промышленных информационных систем, руководители предприятий получают реальную возможность внедрить современную и экономически эффективную систему защиты.

Главной идеей, лежащей в основе подхода МЭК, является идея модульной архитектуры обеспечения безопасности. Каждый модуль соответствует определенному способу использования системы или методу связи и может быть поставлен в соответствие определенным компонентам системы автоматизации и входящей в ее состав сети (рис. 2). Каждый модуль представлен набором требований, описанным в стандарте. Некоторые из требований, а также физические или логические компоненты, к которым они привязаны, являются общими для нескольких модулей. Архитектурные модули могут и должны комбинироваться в соответствии с индивидуальными условиями применения и набором угроз в конкретной системе автоматизации. В стандарте предусмотрены руководящие указания по расстановке приоритетов между модулями в тех ситуациях, когда полная реализация стандарта оказывается невозможной в силу ограничений бюджета, выделенного на начальное внедрение или текущее сопровождение.

Требования будут сформулированы таким образом, чтобы их можно было использовать в основе запросов на коммерческие предложения к поставщикам (RFP) или в основе предложений, а также при проведении проверок безопасности. В то же время, они должны допускать возможность применения различных технических решений. Поставлена цель сделать так, чтобы требования стандарта могли быть удовлетворены с использованием изделий и технологий, представленных на рынке уже сейчас. Требования могут также быть применены к ныне эксплуатируемым системам и к системам, выпущенным ранее, а также скорректированы для тех систем, где анализ показывает наличие невысокого риска для предприятия и населения.

Рабочая группа предусматривает следующие модули:

Связь между сетью предприятия и сетью системы управления (ECI). Модуль ECI (Enterprise-control net interconnect) определяет архитектуру безопасности для потоков информационного обмена между сетью системы управления и корпоративной сетью не в реальном времени, предпочтительно одностороннего – только из системы управления.

Интерактивный удаленный доступ (IRA). Модуль IRA (Interactive remote access) описывает архитектуру безопасности, необходимую для организации удаленного доступа к элементам системы управления (например, по телефонной линии или Интернету) для целей разработки, экспертной диагностики и т. п.

Связь между центрами управления (ICC). Модуль ICC (Inter control center connect) описывает методы обеспечения безопасности связи между стационарными центрами управления по общедоступным сетям.

Автономное встроенное устройство (SED). Модуль SED (Stand-alone embedded device) задает требования к безопасности устройства автоматизации, расположенного за пределами безопасной зоны, для которого создание полномасштабного периметра защиты оказывается слишком дорогим, например, мачтового интеллектуального электронного прибора (IED, intelligent electronic device).

Мобильный компьютер разработчика (PEC). Модуль PEC (Portable engineering computer) предусматривает меры защиты системы от угроз, вызванных переносными компьютерами, которые могут попеременно быть подключены то к общедоступным сетям, то к сети системы управления.

Переносные носители информации (PSM). Система автоматизации может быть подвергнута заражению вредоносным ПО через носители информации, такие как «флэш» -накопители или компакт-диски. В модуле PSM (Portable Storage Media) описано, как этого можно избежать.

Связь между ячейками автоматизации (ACI). В модуле ACI (Automation cell interconnect) описана архитектура безопасности, необходимая для организации защищенной связи между ячейками автоматизации в сети системы управления.

Центр управления верхнего уровня (ULCC). Часть сети управления связана с рабочими станциями оператора, программами регистрации и ведения журналов, серверами приложений и связи. В модуле ULCC (Upper level control center) подробно рассмотрены сетевые механизмы обеспечения безопасности для этой части сети.

Центр управления нижнего уровня (LLCC). В модуле LLCC (Lower level control center) рассмотрены сетевые механизмы, связанные с защитой части сети, подключенной к микроконтроллерам и ПЛК.

Управление полевыми устройствами (FC). В модуле FC (Field control) рассмотрены сетевые механизмы, связанные с защитой части сети, подключенной к полевым устройствам.

Компьютеры сети системы управления (CNH). Модуль CNH (Control network host) определяет методы защиты рабочих станций и серверов, используемых для эксплуатации или доработки системы, например, от инсайдерских атак или вредоносного ПО.

Полевое устройство автоматизации (AFD). Модуль AFD (Automation field device) определяет методы защиты полевых устройств и встроенных контроллеров.

В каждом модуле приводится описание ситуаций, в которых он может быть применен; угроз, защита от которых предусмотрена или, наоборот, не предусмотрена; исходных допущений; требований. Кроме того, указана сторона (поставщик средств автоматизации, системный интегратор или владелец предприятия), ответственная за выполнение каждого из требований. Центральной частью каждого модуля является набор требований, содержащий, в зависимости от модуля, от 20 до 50 требований.

Каждое требование состоит из нормативного высказывания, необязательного «ослабленного» варианта, обоснования, а также, во многих случаях – одного или нескольких примечаний прикладного характера. Обоснование является обязательным элементом, поскольку оно позволяет читателю принять информированное решение о важности или применимости требования. В примечаниях даются технические рекомендации по возможным способам технической реализации требования.

Стандарт IEC 62443 отвечает на вопросы «что необходимо сделать?» и «почему?», связанные с архитектурой системы безопасности, тогда как ответ на вопрос «как?» индивидуален для конкретного предприятия или системы и поэтому ос-

Сноски

1) http://www. isa. org/MSTemplate. cfm?MicrositeID=988&CommitteeID=6821

2) http://www. iaona. org/home/jtwg-se. php

Учебное пособие

тавлен на усмотрение специалистов предприятия и интегратора систем автоматизации.

Заключение

Благодаря непрекращающейся работе по стандартизации механизмов и архитектур в области безопасности промышленных информационных систем, а именно систем управления и автоматизации, руководители предприятий получают реальную возможность внедрить современную и экономически эффективную систему защиты.

Инициативы по стандартизации, рассмотренные в данной статье, позволяют сделать общий вывод – промышленность нуждается в прагматических решениях, а также в конструктивном сотрудничестве между поставщиками и потребителями средств автоматизации.

Компания АББ принимает активное участие в различных инициативах по стандартизации в области безопасности. Компания предлагает изделия и решения, соответствующие появляющимся стандартам, и обеспечивает своих заказчиков поддержкой по применению этих стандартов на практике, на производстве и в новых проектах.

Мартин Нэдель
ABB Switzerland, Corporate Research
martin. naedele@ch. abb. com

Дик Ойен
ABB US, Corporate Research
dick. oyen@us. abb. com

Литература

[1] Naedele, M.: Standardizing Industrial IT Security – A First Look at the IEC approach, 10-я международная конференция IEEE по новым технологиям и автоматизации производства (ETFA 05), Катания, сентябрь 2005 г.

[2] Dzung, D., Naedele, M., von Hoff, T., Crevatin, M.: Security for industrial communication systems, Труды IEEE, Том 93 (6), июнь 2005 г., с. 1152-1177

[3] ISA SP99: Security Technologies for Manufacturing and Control Systems, Instrumentation, Systems, and Automation Society, ISA-TR99.00.01-2004, март 2004 г.

[4] ISA SP99: Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems, and Automation Society, ISA-TR99.00.02-2004, апрель 2004 г.

[5] ISO: Information technology – Code of practice for information security management, ISO/IEC 17799:2000, декабрь 2000 г.

[6] British Standards Organization: Information security management systems – Specification with guidance for use, BS 7799-2:2002, сентябрь 2002 г.

[7] Chemical Industry Data Exchange (CiDX): Guidance for Addressing Cybersecurity in the Chemical Sector, версия 2.0, декабрь 2004 г.

Указатель статей за 2005 год

1/2005: Дух новаторства

3/2005: Устойчивое развитие

2/2005: Сотрудничество промышленных предприятий с университетами

4/2005: Инновации – генетическая основа бизнеса