КРАТКИЕ СООБЩЕНИЯ

А.М. ФАЛЬ

УДК 681.3

СТАНДАРТИЗАЦИЯ В СФЕРЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые слова: *информационная безопасность, модель систем менеджмента, стандарт, управление рисками, руководящие указания, процессная модель*.

ВВЕДЕНИЕ

В работе [1] описаны асимметричные криптографические алгоритмы, которые используются в современных системах электронного документооборота; отмечена также важность разработки и внедрения стандартов, относящихся к защите информации. Один из соавторов этой работы (А.И. Кочубинский) является создателем национального стандарта по цифровой подписи [2]. В данной статье отражено современное состояние стандартизации одного из важнейших направлений в защите информации — менеджмента информационной безопасности.

Для разработки стандартов в области безопасности информационных технологий учрежден подкомитет SC 27 Security techniques в рамках объединенного технического комитета ISO/IEC JTC 1 Information technology. Украинские специалисты принимают участие в разработке таких стандартов, а Украина, как активный член подкомитета, обязана участвовать в голосовании по проектам стандартов. Широкий спектр вопросов информационной безопасности, рассматриваемых специалистами, вовлеченными в деятельность SC 27, распределен между пятью рабочими группами, составляющими подкомитет. За каждой группой закреплено соответствующее направление.

Первая рабочая группа (РГ 1) Information Security Management Systems занимается разработкой стандартов и руководящих указаний по построению систем менеджмента информационной безопасности (ISMS).

Вторая рабочая группа (РГ 2) Cryptography and security mechanisms ориентирована на стандартизацию методов и механизмов обеспечения безопасности информационных технологий.

Третья рабочая группа (РГ 3) Security evaluation criteria разрабатывает стандарты для оценивания безопасности и сертификации информационных систем и их компонентов.

Четвертая рабочая группа (РГ 4) Security controls and services занимается разработкой и поддержкой стандартов и руководящих указаний, касающихся услуг и приложений, способствующих реализации мероприятий по защите информации, определенных в стандартах ISO/IEC 27001, 27002.

Пятая рабочая группа (РГ 5) Identity management and privacy technologies разрабатывает стандарты и руководящие указания, касающиеся управления идентификационными данными, биометрики и защиты персональных данных (privacy).

В своей деятельности рабочие группы следуют принципам и правилам, принятым в ISO и IEC. В частности, ими должны разрабатываться и через каждые шесть месяцев пересматриваться дорожные карты (road maps). Далее остановимся на содержании дорожной карты, принятой в РГ 1 в мае 2009 года.

Целью дорожной карты является:

а) точная идентификация стандартов, касающихся РГ 1, как уже опубликованных, так и разрабатываемых или готовящихся к разработке;

б) описание логических связей между разрабатываемыми в РГ 1 стандартами;

в) формулирование основных принципов, с помощью которых работа по созданию стандартов может быть скоординирована во избежание дублирования;

г) планирование работы по стандартизации в рамках РГ 1;

д) бóльшая координация между различными техническими комитетами ISO и IEC.

ТРЕБОВАНИЯ К РАЗРАБАТЫВАЕМЫМ СТАНДАРТАМ

Стандарты, разрабатываемые в РГ 1, касаются защиты информации, которая может существовать в различных видах (напечатанная или написанная на бумаге, хранимая на электронных или магнитных носителях, передаваемая по обычной или электронной почте, видеоинформация, речевая). Также в РГ 1 разрабатываются стандарты, касающиеся механизмов защиты, ограничивающих ущерб, нанесенный организации из-за ненадлежащей защиты информации (ошибочные финансовые отчеты, неправильные документы, выданные организацией, потеря репутации и престижа и т.п.).

Для эффективного решения вопросов информационной безопасности организации необходимо:

— систематически управлять деятельностью, связанной с информационной безопасностью;

— демонстрировать способность удовлетворить требования внутренних и внешних заинтересованных сторон.

Для того чтобы быть полезными различным организациям, стандарты, относящиеся к РГ 1, должны быть:

— согласованными (иметь общую модель систем менеджмента, общую структуру и общие элементы стандарта, согласованную терминологию);

— взаимосвязанными с другими стандартами ISO, такими как ISO 9000 (серия стандартов по системам менеджмента качества), ISO 14000 (система стандартов по менеджменту окружающей среды).

В настоящее время общепринятыми моделями являются:

- модель PDCA (планируй – делай – проверяй – действуй);
- процессная модель.

Стандарты РГ 1 должны следовать основополагающим принципам, применяемым к стандартам по системам менеджмента, для того чтобы помочь: пользователям реализовать системы менеджмента; разработчикам стандартов определить согласованную и логическую структуру.

ТИПЫ СТАНДАРТОВ

Дорожная карта РГ 1 придерживается четырехуровневой модели, в рамках которой разрабатываются стандарты, относящиеся к РГ 1:

а) тип *A* — терминологический стандарт;

б) тип *B* — стандарт, касающийся требований;

в) тип *C* — стандарт, касающийся предоставления руководящих указаний (guidelines);

г) тип *D* — смежный стандарт.

Рассмотрим типы стандартов более детально.

Тип *A* — терминологический стандарт.

Стандарт предназначен для предоставления основной информации, включающей общую терминологию, которая согласованно используется во всей серии стандартов РГ 1.

Тип *B* — стандарт, определяющий требования по информационной безопасности.

Стандарт предназначен для формулирования спецификаций, относящихся к конкретной деятельности и позволяющих организациям демонстрировать способность удовлетворить внутренние и внешние требования по информационной безопасности.

Примерами стандартов типа *B* являются:

B-1: ISO/IEC 27001:2005. Системы менеджмента информационной безопасности — Требования;

B-2: ISO/IEC 27006:2007. Требования к органам, проводящим аудит и сертификацию систем менеджмента информационной безопасности.

Тип *C* — стандарт, включающий определенные руководства.

Стандарт предназначен для помощи организациям в реализации стандартов типа *B*.

Примерами стандартов типа *C* являются:

C-1: стандарты, содержащие руководства по удовлетворению требований к ISMS; стандарты, содержащие руководства по выбору и реализации мероприятий по информационной безопасности;

C-2: стандарты, включающие руководства по достижению требуемых результатов специфических процессов, связанных с менеджментом информационной безопасности (например, измерение эффективности мероприятий); стандарты, содержащие руководства по реализации конкретных мер/методов информационной безопасности (например, менеджмент инцидентов информационной безопасности);

C-3: стандарты, включающие руководства по реализации требований по информационной безопасности, учитывающих особенности отрасли (банковское дело, разработка программного обеспечения, здравоохранение, телекоммуникации).

Тип *D* — смежный стандарт.

Стандарт предназначен для предоставления дальнейшего руководства, касающегося конкретных сторон информационной безопасности или смежных методов поддержки. В общем случае эти стандарты разрабатываются на односторонней основе, без точных описаний, касающихся связей со стандартами типа *D* и/или типа *C*.

ЭЛЕМЕНТЫ СТАНДАРТОВ

В стандартах по системам менеджмента, разрабатываемым в ISO, существует ряд общих элементов. Эти элементы можно упорядочить по следующим основным темам: политика; планирование; реализация и эксплуатация; оценивание; улучшение; пересмотр руководством.

ОБЗОР СТАНДАРТОВ РГ 1

Рассмотрим состояние стандартов, разрабатываемых РГ 1.

ISO/IEC IS 27000 — Information security management systems — Overview and vocabulary (Published). Системы менеджмента информационной безопасности — Обзор и словарь (опубликован).

Для того чтобы облегчить гармонизацию стандартов, относящихся к РГ 1, и обеспечить единое и четкое их понимание, необходимо документировать в одном стандарте основные положения, систематический словарь и набор основных понятий и терминов, использующихся во всей серии этих стандартов.

Данный стандарт является ключевым документом для достижения эффективности разработки стандартов в РГ 1.

ISO/IEC 27000:2009 опубликован 30 апреля 2009 года.

ISO/IEC IS 27001:2005 — Information security management systems — Requirements (undergoing reviews). Системы менеджмента информационной безопасности — Требования (в стадии пересмотра).

Данный стандарт является «сердцевиной» семейства ISMS стандартов. Он определяет требования для установления, реализации, эксплуатации, мониторинга, пересмотра, поддержки документиро-

ванной ISMS в контексте общих деловых рисков организации. Этот стандарт также определяет требования к реализации мер безопасности, адаптированных к потребностям конкретных организаций или их подразделений. В соответствии с Резолюцией 11 37-го пленарного заседания РГ 1 в октябре 2008 года разработан план пересмотра стандартов ISO/IEC 27001:2005 и ISO/IEC 27002:2007.

В настоящее время существует рабочий проект (WD) пересматриваемого стандарта ISO/IEC 27001.

ISO/IEC IS 27006:2007 — Requirements for bodies providing audit and certification of information security management systems (published). Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности (опубликован).

Стандарт определяет требования и предоставляет руководство для органов, осуществляющих аудит и сертификацию систем менеджмента информационной безопасности, в дополнение к требованиям, содержащимся в стандартах ISO/IEC 17021 и ISO/IEC 27001.

ISO/IEC IS 27006:2007 опубликован 15 февраля 2007 года.

ISO/IEC IS 27002:2007 — Code of practice for information security management (undergoing review). Практические правила менеджмента информационной безопасности (в стадии пересмотра).

ISO/IEC 27002 опубликован как стандарт, предоставляющий всеохватывающее руководство по реализации мер информационной безопасности, и напрямую поддерживает стандарт ISO/IEC 27001.

Изменение нумерации ISO/IEC 17799 на ISO/IEC 27002 согласовано в SC 27 в апреле 2007 года в целях интеграции ISO/IEC 17799 в семейство ISMS стандартов. В связи с изменением нумерации никаких изменений в содержание этого документа не вносилось. В соответствии с Резолюцией 11 37-го пленарного заседания РГ 1 в октябре 2008 года разработан план пересмотра стандартов ISO/IEC 27001 и ISO/IEC 27002. В настоящее время имеется рабочий проект (WD) пересматриваемого стандарта ISO/IEC 27002.

ISO/IEC 27003 — Information security management systems implementation guidance (under development). Руководство по реализации систем менеджмента информационной безопасности (в стадии разработки).

Стандарт непосредственно поддерживает стандарт ISO/IEC 27001 и предоставляет материал по руководству, касающемуся реализации ISMS.

В настоящее время имеется окончательный проект международного стандарта (FDIS) ISO/IEC 27003.

ISO/IEC 27004 — Information security management measurements (under development). Измерения менеджмента информационной безопасности (в стадии разработки).

ISO/IEC 27004 предложен как стандарт по руководству, который предоставляет возможность измерять уровень эффективности реализованных в соответствии со стандартом ISO/IEC 27001 мероприятий и процессов.

Стандарт ISO/IEC 27004, чтобы быть эффективным, должен содержать ряд единиц измерений, включающих результативность мероприятий. Этот стандарт должен также предоставить инструментарий, который позволил бы эффективно измерять деятельность по информационной безопасности, осуществляемую для защиты информационных активов организации.

В настоящее время имеется окончательный проект международного стандарта (FDIS) ISO/IEC 27004.

ISO/IEC IS 27005:2008 — Information security risk management (published). Менеджмент рисков информационной безопасности (опубликован).

Стандарт содержит руководство по менеджменту рисков информационной безопасности и определяет принципы менеджмента рисков информационной безопасности, методы оценивания рисков, трактовку рисков, мониторинг и пересмотр рисков, предоставляя дополнительную информацию относительно выполнения требований стандарта ISO/IEC 27001.

ISO/IEC IS 27005:2008 опубликован 15 июня 2008 года.

ISO/IEC 27007 — Guidelines for information security management systems auditing (under development). Руководство по аудиту систем менеджмента информационной безопасности (в стадии разработки).

Стандарт ISO/IEC 27007 предложен как руководство по проведению аудитов ISMS и руководство по компетентности аудиторов систем менеджмента информационной безопасности в дополнение к руководству, содержащемуся в ISO 19011.

Стандарт включает также руководство, необходимое для аудитов ISMS в поддержку стандарта ISO/IEC 27006 и общего руководства для аудиторов, содержащегося в ISO 19011.

В настоящее время имеется 1-й проект комитета (CD) ISO/IEC 27007.

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (under development). Руководство для аудиторов мероприятий ISMS (в стадии разработки).

Данный технический отчет 2-го типа ориентирован на предоставление руководства по проверке доказательства и качества реализованных в ISMS мероприятий и тем самым поддерживает планирование и выполнение оценивания мероприятий ISMS.

В настоящее время имеется 2-й рабочий проект (WD) ISO/IEC 27008.

ISO/IEC 27013 — Guidance on the integrated implementation of 20000-1 and 27001 (under development). Руководство по интегрированной реализации стандартов ISO/IEC 20000-1 и ISO/IEC 27001 (в стадии разработки).

Стандарт предоставит руководство по реализации интегрированной системы менеджмента информационной безопасности и менеджмента услуг ИТ.

В настоящее время имеется предварительный рабочий проект (WD) ISO/IEC 27013, предлагающий структуру этого стандарта.

ISO/IEC 27014 — Information security governance framework (under development). Основные положения управления информационной безопасностью (в стадии разработки).

Стандарт сформулирует основные положения (framework) управления информационной безопасностью в поддержку требований к управлению корпорацией, которые предполагают эффективные внутренние меры по управлению организацией.

ISO/IEC 27010 — Information security management guidelines for inter-sector communications (under development). Руководство по менеджменту информационной безопасности для межотраслевых сообщений (в стадии разработки).

Стандарт будет содержать руководство по менеджменту информационной безопасности сообщений и сотрудничеству между открытыми и/или закрытыми секторами.

В настоящее время имеется текст, предоставленный редакторами этого стандарта.

ITU X.1051|ISO/IEC 27011: 2008 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. Руководство по менеджменту информационной безопасности для телекоммуникационных организаций на основе ISO/IEC 27002.

Данный стандарт:

а) определяет руководящие указания и общие принципы для инициирования, реализации, поддержки и улучшения менеджмента информационной безопасности в телекоммуникационных организациях на основе ISO/IEC 27002;

б) формулирует основные рекомендации для реализации менеджмента информационной безопасности в телекоммуникационных организациях для обеспечения конфиденциальности, целостности и доступности телекоммуникационных средств и услуг.

ISO/IEC IS 27011 опубликован 15 декабря 2008 года.

ISO/IEC 27015 — Information security management guidelines for financial and insurance services (under development). Руководящие указания по менеджменту информационной безопасности для финансовых услуг и услуг страхования (в стадии разработки).

Стандарт устанавливает требования и руководящие указания для инициирования, реализации, поддержки и улучшения менеджмента информационной безопасности, специфические для организаций, предоставляющих финансовые услуги и услуги страхования. Требования этого стандарта дополняют требования стандарта ISO/IEC 27001, которые также должны выполняться.

Руководящие указания в контексте оказания финансовых услуг и услуг страхования являются дополняющими общее руководство по реализации менеджмента информационной безопасности, предоставляемое стандартом ISO/IEC 27002. В настоящее время имеется рабочий проект (WD) этого стандарта.

ISO/IEC 27031 — Guidelines for ICT readiness for business continuity (under development). Руководство по обеспечению готовности информационно-коммуникационных технологий (ИКТ) по поддержанию непрерывности бизнеса (в стадии разработки).

Стандарт описывает концепцию и принципы обеспечения готовности ИКТ по поддержанию непрерывности бизнеса для любой организации независимо от ее размера, а также спецификации всех аспектов улучшения готовности ИКТ по обеспечению непрерывности бизнеса. Область действия этого стандарта охватывает все события и инциденты, которые могут иметь влияние на системы и инфраструктуру ИКТ. Она включает и расширяет практические правила рассмотрения инцидентов, связанных с безопасностью, и менеджмент планирования поддержания готовности ИКТ.

В настоящее время имеется проект комитета (CD) этого стандарта.

ISO/IEC 27033 — Network security (all parts) (under development). Безопасность сетей (все части) (в стадии разработки).

Стандарт предоставит детальное руководство по аспектам безопасности, касающимся управления, эксплуатации и использования сетей информационных систем и их связей.

ISO/IEC 27034 — Application security (all parts) (under development). Безопасность приложений (все части) (в стадии разработки).

Различные части этого стандарта предоставят руководящие указания для разработчиков программного обеспечения, администраторов безопасности, пользователей программного обеспечения, аудиторов, менеджеров по определению, разработке в случае необходимости, реализации, поддержке и замене приложений с точки зрения информационной безопасности.

ISO/IEC 27035 — Information security incident management (under development). Менеджмент инцидентов информационной безопасности (в стадии разработки).

Стандарт предоставит руководство по менеджменту инцидентов информационной безопасности для администраторов безопасности, администраторов информационных систем, сетей как для больших, так и для малых организаций.

ISO/IEC 27036 — Guidelines for security of outsourcing (under development). Руководящие указания по безопасности аутсорсинга (в стадии разработки).

Стандарт предоставит руководство по оцениванию рисков, исходящих от приобретения и использования услуг аутсорсинга, в поддержку стандарта ISO/IEC 27001 и мероприятий, связанных с аутсорсингом, стандарта ISO/IEC 27002.

ISO/IEC 27037 — Guidelines for identification, collection and/or acquisition and preservation of digital evidence (under development). Руководящие указания для идентификации, сбора и/или приобретения и сохранения цифровых доказательств (в стадии разработки).

Стандарт включает детальное руководство, описывающее процесс обнаружения, идентификации, сбора и/или приобретения и сохранения цифровых данных, которые могут содержать информацию, имеющую потенциальное доказательное значение.

СПИСОК ЛИТЕРАТУРЫ

1. Коваленко И.Н., Кочубинский А.И. Асимметричные криптографические алгоритмы // Кибернетика и системный анализ. — 2003. — **39**, № 4. — С. 95–102.
2. ДСТУ 4145 — 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. — Увед. 28.12.2002. — К.: Держспоживстандарт України, 2002. — 37 с.

Поступила 05.11.2009