УДК 681.3

А.М. ФАЛЬ

СТАНДАРТИЗАЦИЯ В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Приведен обзор международных стандартов, которые разрабатываются в ПК 27 «Методы защиты ИТ» Объединенного технического комитета 1 ISO/IEC «Информационные технологии». Стандарты охватывают криптографические механизмы, оценку и тестирование продуктов и информационных систем, контрмеры и услуги безопасности. Рассмотрены как опубликованные стандарты, так и находящиеся в процессе разработки.

Ключевые слова: инцидент информационной безопасности, конфиденциальность, непрерывность бизнеса, оценка защищенности, управление ключами, функциональные услуги.

ВВЕДЕНИЕ

В апреле 2015 года исполнилось 25 лет со дня создания подкомитета по обеспечению безопасности информационных технологий объединенного технического комитета по информационным технологиям (JTC1/SC27 “IT Securities techniques”). В современном мире, который характеризуется внедрением информационных технологий во все сферы человеческой деятельности, защита информации, представленной в разных видах, является чрезвычайно важной задачей. Аналогичные проблемы исследовались и в 90-х годах прошлого столетия, когда был образован подкомитет. В начале его функционирования в состав подкомитета входило 18 стран — членов ISO. За 25 лет количество членов подкомитета увеличилось до 73, из них 52 — активные члены (P-members) и 21 — пассивные члены (O-members). За эти годы разработано более 150 международных стандартов и технических отчетов, охватывающих различные аспекты объектов стандартизации. Такую работу проведено с помощью более чем 300 экспертов из разных стран. Структура подкомитета сформирована из пяти рабочих групп, а именно:

— РГ1 «Системы менеджмента информационной безопасности»;

— РГ2 «Криптография и механизмы безопасности»;

— РГ3 «Оценка, тестирование и спецификация безопасности»;

— РГ4 «Контрмеры и услуги безопасности»;

— РГ5 «Менеджмент идентификационных данных и технологии обеспечения прайвеси».

В статье [1] приведен обзор стандартов в области менеджмента информационной безопасности, разработанных в РГ1. Настоящая работа посвящена стандартизации в рамках РГ2, РГ3 и РГ4. Ее содержание основано на документе [2], размещенном на сайте подкомитета www.jtc1sc27.din.de.

СТАНДАРТЫ, РАЗРАБОТАННЫЕ РГ2

Дорожная карта РГ2 определяет такие направления стандартизации:

— идентификация потребностей и требований к методам и механизмам обеспечения безопасности информационных технологий;

— разработка терминологии, общих моделей и стандартов для использования этих методов и механизмов в услугах безопасности.

Рассмотрим разработанные в РГ2 стандарты для различных областей применения.

Обеспечение конфиденциальности (confidentiality)

ISO/IEC 18033 (шесть частей). Алгоритмы шифрования (Encryption algorithms). Определяет симметричные шифры (блочные и поточные) и асимметричные шифры, включая шифры, основанные на идентификационных данных, и гомоморфные шифры.

ISO/IEC 29192 (шесть частей). Легкая криптография (Lightweight cryptography). Определяет криптографические механизмы, приспособленные для их использования в устройствах с ограниченными вычислительными ресурсами и ограниченной пропускной способностью.

ISO/IEC 29150. Шифрование с подписью (Signcryption). Определяет механизм одновременного подписывания и шифрования, в котором используются пары асимметричных ключей как отправителя, так и получателя.

ISO/IEC 19772. Шифрование с аутентификацией (Authenticated encryption). Определяет механизм для одновременных шифрования и аутентификации данных и отправителя.

ISO/IEC 10116. Режимы функционирования *n*-битового блочного шифра (Modes of operation for n-bit block cipher). Определяет режимы функционирования блочных шифров, а именно ECB, CBC, OFB, CFB и CTR.

Контролирование целостности данных с использованием аутентификации сообщений, хеш-функций, цифровых подписей

ISO/IEC 10118 (четыре части). Хеш-функции (Hash functions). Определяет несколько типов хеш-функций, которые отображают битовые строки произвольной длины в строки фиксированной длины.

ISO/IEC 9797 (три части). Коды аутентификации сообщений (MACs) (Message authentication codes (MACs)). Устанавливает алгоритмы вычисления кодов аутентификации сообщений для проверки целостности данных.

ISO/IEC 9796 (две части). Схемы цифровой подписи, которые предоставляют раскрытие сообщения (Digital signature schemes giving message recovery). Определяет механизмы цифровой подписи, предоставляющие раскрытие всего сообщения или его части, способствующие уменьшению нагрузки, связанной с сохранением или передачей данных.

ISO/IEC 14888 (три части). Цифровые подписи с добавлением (Digital signatures with appendix). Определяет механизмы цифровой подписи, основанные на проблемах дискретного логарифмирования и факторизации целых чисел.

ISO/IEC 20008 (две части). Анонимные цифровые подписи (Anonymous digital signatures). Определяет механизмы анонимной цифровой подписи, в которых проверка подписи осуществляется с использованием открытого ключа группы пользователей.

ISO/IEC 18370 (две части). Слепые цифровые подписи (Blind digital signatures). Определяет механизмы слепой цифровой подписи, позволяющие получить цифровую подпись, не предоставляя подписанту информации об истинном сообщении и полученной цифровой подписи.

Аутентификация объектов (entity authentication)

ISO/IEC 9798 (шесть частей). Аутентификация объектов (Entity authentication). Определяет несколько типов механизмов аутентификации объектов, в которых объект (его достоверность проверяется) доказывает, что он знает некоторый секрет.

ISO/IEC 20009 (четыре части). Анонимная аутентификация объектов (Anonymous entity authentication). Определяет механизмы анонимной аутентифи-

кации объектов, в которых проверяющий использует схему групповой цифровой подписи, основанной на слепой цифровой подписи и слабых секретах.

Управление ключами с использованием генерирования случайных чисел и случайных простых чисел

ISO/IEC 11770 (шесть частей). Управление ключами (Key management). Описывает общие модели, на которых базируются механизмы управления ключами, определяет основные понятия управления ключами и несколько типов механизмов установления ключей.

ISO/IEC 18031. Генерирование случайных битов (Random bit generation). Определяет концептуальную модель для генераторов случайных битов, используемых в криптографических механизмах.

ISO/IEC 18032. Генерирование простых чисел (Prime number generation). Предоставляет методы генерирования простых чисел, применяемых в криптографических протоколах и алгоритмах.

ISO/IEC 15946 (две части). Криптографические методы, основанные на эллиптических кривых (Cryptographic techniques based on elliptic curves). Описывает математические основания эллиптических кривых и методы их генерирования.

ISO/IEC 19592 (две части). Распределение секрета (Secret sharing). Описывает криптографические схемы распределения секрета.

Обеспечение невозможности отказа от совершенных действий (non-repudiation)

ISO/IEC 13888 (три части). Обеспечение невозможности отказа (Non-reputation). Определяет предоставление услуг невозможности отказа. Целью услуги невозможности отказа является генерирование, сбор, поддержание доступности и проверка доказательств, касающихся заявленных событий или действий, применяемых для разрешения дискуссий о наличии либо отсутствии события или действия.

Услуги третьей доверенной стороны

ISO/IEC 18014 (четыре части). Услуги штемпелирования времени (Time-stamping services). Определяет услуги штемпелирования времени, которые предоставляются с помощью использования токенов штемпелей времени заинтересованными сторонами с дополнительным отслеживанием источников времени.

Подробный анализ стандартов в области криптографии приведен в работе [3].

СТАНДАРТЫ, РАЗРАБОТАННЫЕ РГ3

Областью применения РГ3 является разработка стандартов, касающихся спецификации, оценки, тестирования и сертификации информационных систем, компонентов и продуктов относительно безопасности ИТ, включая компьютерные сети, распределенные системы, биометрику и связанные с ними услуги приложений.

Разработаны стандарты, ориентированные на следующие аспекты области их применения.

Критерии оценки защищенности

ISO/IEC 15408 (три части). Критерии оценки защищенности ИТ (Evaluation criteria for IT security). Устанавливает общие понятия и принципы оценки защищенности ИТ и определяет общую модель оценки.

ISO/IEC 19790. Требования к безопасности криптографических модулей (Security requirements for cryptographic modules). Определяет требования к безопасности криптографических модулей, используемых для защиты информации в компьютерных и телекоммуникационных системах.

Методология применения критериев

ISO/IEC 18045. Методология оценки защищенности ИТ (Methodology for IT security evaluation). Определяет минимальные действия, которые следует совершить при оценке соответствия критериям, изложенным в стандарте ISO/IEC 15408.

ISO/IEC TR 19791. Оценивание безопасности действующих систем (Security assessment of operational systems). Технический отчет (TR) предоставляет руководство и критерии для оценки безопасности действующих систем.

ISO/IEC 19792. Оценка безопасности биометрических характеристик (Security evaluation of biometrics). Определяет объекты, которые нужно исследовать во время оценки безопасности биометрических систем.

Спецификация функциональных услуг и услуг гарантий информационных систем, компонентов и продуктов

ISO/IEC TR 15443 (две части). Общие положения гарантий безопасности ИТ (A framework for IT security assurance). Предоставляет руководство по выбору подходящего метода гарантирования при определении или внедрении услуги или продукта.

ISO/IEC TR 15446. Руководство по разработке профилей защиты и заданий по безопасности (Guide for the production of Protection Profiles and Security Targets). Предоставляет руководство, касающееся построения профилей защиты и заданий по защите, совместимых с требованиями стандарта ISO/IEC 15408.

ISO/IEC TR 19608. Руководство по разработке функциональных требований к безопасности и прайвеси, основанных на ISO/IEC 15408 (Guidance for developing security and privacy functional requirements based on ISO/IEC 15408). Технический отчет предоставляет руководство по разработке функциональных требований к обеспечению прайвеси, основанных на принципах обеспечения прайвеси, изложенных в ISO/IEC 29100, используя парадигму, описанную в ISO/IEC 15408-2.

ISO/IEC TR 19249. Каталог принципов, касающихся архитектуры и проектирования для защищенных продуктов, систем и приложений (Catalogue of architectural and design principles for secure products, systems and applications). Технический отчет предоставляет каталог указаний по принципам, касающимся архитектуры и проектирования при разработке защищенных продуктов, систем и приложений.

Методология тестирования для определения соответствия предоставляемых функциональных услуг и услуг гарантий

ISO/IEC 24759. Требования к тестированию криптографических модулей (Test requirements for cryptographic modules). Определяет методы, которые должны использоваться испытательными лабораториями для тестирования соответствия криптографических модулей требованиям стандарта ISO/IEC 19790.

ISO/IEC 17825. Методы тестирования противодействия классам неинвазивных атак на криптографические модули (Testing methods for the mitigation of non-invasive attack classes against cryptographic modules). Определяет метрики тестов на противодействие неинвазивным атакам для определения соответствия требованиям стандарта ISO/IEC 19790 относительно 3- и 4-го уровней безопасности.

ISO/IEC 18367. Тестирование соответствия криптографических алгоритмов и механизмов безопасности (Cryptographic algorithms and security mechanisms conformance testing). Целью данного стандарта является предоставление методов тестирования соответствия криптографических алгоритмов и механизмов безопасности, реализованных в криптографическом модуле.

ISO/IEC TR 20540. Руководящие указания по тестированию криптографических модулей в рабочей среде (Guidelines for testing cryptographic modules in their operational environment). Технический отчет предоставляет руководящие указания по аудиту того, что криптографический модуль должным образом инсталлирован, сконфигурирован или функционирует.

ISO/IEC 20543. Методы тестирования и анализа генераторов случайных битов в парадигме ISO/IEC 19790 и ISO/IEC 15408 (Test and analysis methods for random bit generators within ISO/IEC 19790 и ISO/IEC 15408). Определяет методы оценки и требования к тестированию генераторов случайных битов, приведенных в стандарте ISO/IEC 18031.

Административные процедуры для тестирования, оценки, сертификации и схем аккредитации

ISO/IEC 19896. Требования к компетентности тестировщиков и оценщиков информационной безопасности (Competence requirements for information security testers and evaluators). Предоставляет основополагающие понятия, касающиеся вопросов компетентности специалистов, отвечающих за проведение оценок ИТ-продуктов и тестирование соответствия.

ISO/IEC 19989. Оценка безопасности обнаружения атаки при предъявлении биометрических характеристик (Security evaluation of presentation attack detection for biometrics). Определяет дополнение к методике, изложенной в ISO/IEC 18045, для оценки обнаружения атаки при предъявлении биометрических характеристик.

ISO/IEC 29128. Верификация криптографических протоколов (Verification of cryptographic protocols). Устанавливает техническое основание для доказательства стойкости спецификации криптографических протоколов.

ISO/IEC 29147. Раскрытие уязвимостей (Vulnerability disclosure). Предоставляет руководящие указания по раскрытию потенциальных уязвимостей в продуктах и онлайновых сервисах.

ISO/IEC 30104. Атаки на физическую безопасность, методы противодействия и требования к безопасности (Physical security attacks, mitigations techniques and security requirements). Касается того, как гарантии безопасности могут быть сформулированы для продуктов, в которых среда требует поддержки механизмов физической защиты.

ISO/IEC 30111. Процессы обработки уязвимостей (Vulnerability handling processes). Предоставляет процессы обработки уязвимостей.

СТАНДАРТЫ, РАЗРАБОТАННЫЕ РГ4

Разработаны стандарты, ориентированные на следующие направления стандартизации.

Услуги третьей доверенной стороны

ISO/IEC TR 14516. Руководящие указания по использованию и менеджменту услуг третьей доверенной стороны (Guidelines for the use and management of Trusted Third Party services). Устанавливает четкое определение основных предоставляемых третьей доверенной стороной услуг и взаимные обязанности третьей доверенной стороны и потребителя ее услуг.

ISO/IEC 15945. Спецификация услуг третьей доверенной стороны (TTP) для поддержки применения цифровых подписей (Specification of TTP services to support the application of digital signatures). Определяет услуги, необходимые для поддержки применения цифровых подписей для невозможности отказа от факта создания документа.

ISO/IEC 29149. Лучшие практики предоставления и использования услуг штемпелирования времени (Best practice on the provision and use of time-stamping services). Объясняет, как генерировать, обновлять и проверять токены штемпелей времени.

Принципы готовности ИКТ для обеспечения непрерывности бизнеса

ISO/IEC 27031. Руководящие указания для готовности ИКТ при обеспечении непрерывности бизнеса (Guidelines for ICT readiness for business continuity). Описывает понятия и принципы готовности ИКТ для обеспечения непрерывности бизнеса.

Кибербезопасность

ISO/IEC 27032. Руководящие указания для кибербезопасности (Guidelines for cybersecurity). Предоставляет руководство по улучшению состояния кибербезопасности, а также базовые практики по обеспечению безопасности для заинтересованных сторон в киберпространстве.

Безопасность IT сетей

ISO/IEC 27033 (шесть частей). Безопасность сетей (Network security). Предоставляет обзор сетевой безопасности, описывает угрозы, методы проектирования и внедрения средств защиты для конкретных сценариев. Предоставляет руководство по выбору шлюзов безопасности, а также построению виртуальных защищенных соединений.

ISO/IEC 15816. Объекты информационной безопасности для управления доступом (Security information objects for access control). Предоставляет определение объектов информационной безопасности.

Безопасность приложений

ISO/IEC 27034 (семь частей). Безопасность приложений (Application security). Предоставляет руководство для оказания помощи организациям в интегрировании вопросов безопасности в процессы, используемые для управления приложениями. Вводит определения, понятия, принципы и процессы, вовлеченные в безопасность приложений.

Менеджмент инцидентов информационной безопасности

ISO/IEC 27035. Менеджмент инцидентов информационной безопасности (Information security incident management). Предоставляет структурированный подход к обнаружению, извещению и оцениванию инцидентов информационной безопасности, а также реагированию на них.

ISO/IEC 27037. Руководящие указания по идентификации, сбору, приобретению и сохранению цифровых улик (Guidelines for the identification, collection, acquisition and preservation of digital evidence). Предоставляет руководящие указания для деятельности, связанной с обработкой цифровых улик, имеющих юридическую значимость.

ISO/IEC 27041. Руководство по обеспечению приемлемости и адекватности методов расследования инцидентов (Guidance on assuring suitability and adequacy of incident investigative methods). Предоставляет руководство по приемлемости и адекватности используемых методов и процессов расследования инцидентов информационной безопасности.

ISO/IEC 27042. Руководящие указания по анализу и интерпретации цифровой улики (Guidelines for the analysis and interpretation of digital evidence). Предоставляет руководство по анализу и интерпретации цифровой улики.

ISO/IEC 27043. Принципы и процессы расследования инцидента (Incident investigation principles and processes). Предоставляет руководящие указания по внедрению процессов в различные сценарии расследования инцидента, использующие цифровые улики.

Безопасность аутсорсинга

ISO/IEC 27036 (четыре части). Информационная безопасность во взаимоотношениях с поставщиками (Information security for supplier relationships). Предоставляет обзор руководства по обеспечению безопасности информации и информационных систем в контексте взаимоотношений с поставщиками и, в частности, поставщиками услуг облачных вычислений.

Системы обнаружения и предотвращения вторжений

ISO/IEC 27039. Выбор, внедрение и функционирование систем обнаружения и предотвращения вторжений (Selection, deployment and operation of intrusion, detection and prevention systems). Предоставляет руководящие указания, касающиеся помощи организациям по подготовке к внедрению системы обнаружения и предотвращения вторжений.

Услуги восстановления после стихийных бедствий

ISO/IEC 27040. Безопасность хранения (Storage security). Предоставляет технические указания организациям, касающиеся планирования, проектирования, документирования и реализации безопасности хранения данных.

ISO/IEC 27038. Спецификация для цифрового редактирования (Specification for digital redaction). Определяет характеристики методов для осуществления цифрового редактирования цифровых документов, а также требования к программным средствам редактирования.

ISO/IEC 27050. Электронное раскрытие (Electronic discovery). Предоставляет требования и руководство, касающиеся деятельности, связанной с электронным раскрытием, включая идентификацию, сохранение, сбор, обработку, анализ информации, хранимой на электронных носителях.

ЗАКЛЮЧЕНИЕ

В настоящее время отмечается возрастающая важность разработки стандартов, учитывающих новейшие достижения в научных исследованиях и технологиях. Особенно актуальным является наличие современных стандартов в области безопасности информационных технологий, так как они способствуют повышению доверия к устройствам и системам, реализующим требования и рекомендации, сформулированные в этих стандартах. Обзор опубликованных и разрабатываемых в профильном подкомитете технического комитета по информационным технологиям стандартов отражает текущее состояние и тенденции стандартизации процессов обеспечения безопасности информационных технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Фаль А.М. Стандартизация в сфере менеджмента информационной безопасности. *Кибернетика и системный анализ*. 2010. Т. 46, № 3. С. 181–184.

2. ISO/IEC JTC 1/SC 27 Standing Document 11 — Overview of the Work of SC27. 61 p.

3. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації. Частина 1. Методи побудування та аналізу, стандартизація та застосування криптографічних систем. Харків: Форт, 2015. 959 с.

Надійшла до редакції 25.04.2016

О.М. Фаль

СТАНДАРТИЗАЦІЯ У СФЕРІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Анотація. Наведено огляд міжнародних стандартів, які розробляються у ПК 27 «Методи захисту ІТ» Об'єднаного технічного комітету 1 ISO/IEC «Інформаційні технології». Стандарти охоплюють криптографічні механізми, оцінку та тестування захищеності продуктів та інформаційних систем, контрзаходи і послуги безпеки. Розглянуто як опубліковані стандарти, так і ті, що перебувають у процесі розроблення.

Ключові слова: інцидент інформаційної безпеки, керування ключами, конфіденційність, неперервність бізнесу, оцінка захищеності, функціональні послуги.

O.M. Fal'

STANDARDIZATION IN INFORMATION TECHNOLOGY SECURITY

Abstract. The author overviews the international standards developed by SC 27 "IT Security techniques" of the ISO/IEC Joint technical committee 1 "Information technology". The standards include cryptographic mechanisms, evaluation and testing of products and information systems, countermeasures and security services. Both published standards and those under development are considered.

Keywords: business continuity, confidentiality, information security incident, functional services, key management, security assessment.

Фаль Алексей Михайлович,
кандидат физ.-мат. наук, ведущий научный сотрудник Института кибернетики имени В.М. Глушкова НАН Украины, Киев, e-mail: amfall@bigmir.net.