**Стандартизация в области ИБ: зарубежный опыт**

Георгий Гарбузов

Как оценить качество какого-либо продукта или обеспечить его быструю замену, если он создавался по собственным, ни с кем не согласованным правилам?

Стандартизация устанавливает единые "правила игры", и в этом ее главная цель. Те, кто принимает эти правила, называются участниками стандартизации, а то, к чему предъявляются эти правила, – объектом стандартизации

ИСТОРИЯ стандартизации, как процесса установления единых требований, пригодных для многократного применения, насчитывает несколько тысячелетий – еще при строительстве пирамид в Древнем Египте использовались блоки стандартного размера, а специальные люди контролировали степень соответствия этому древнему стандарту. Сегодня стандартизация занимает прочное место практически во всех отраслях человеческой деятельности.

Стандартизация в области информационной безопасности Стандартизация в области информационной безопасности (ИБ) выгодна и профессионалам, и потребителям продуктов и услуг ИБ, так как позволяет установить оптимальный уровень упорядочения и унификации, обеспечить взаимозаменяемость продуктов ИБ, а также измеряемость и повторяемость результатов, полученных в разных странах и организациях. Для профессионалов – это экономия времени на поиск эффективных и зарекомендовавших себя решений, а для потребителя – гарантия получения результата ожидаемого качества.

Объектом стандартизации может являться любой продукт или услуга ИБ: метод оценки, функциональные возможности средств защиты и параметры настройки, свойства совместимости, процесс разработки и производства, системы менеджмента и т.д.

Стандартизация, в зависимости от состава участников, бывает международной, региональной или национальной, при этом международная стандартизация (наравне с официальными органами стандартизации, такими как ISO) включает в себя стандартизацию консорциумов (например, IEEE или SAE), а национальная стандартизация бывает государственной или отраслевой. Остановимся подробнее на некоторых востребованных сегодня зарубежных стандартах, так или иначе затрагивающих вопросы информационной безопасности.

Международные стандарты в области ИБ – зарубежный опыт Стандартизация в области ИБ за рубежом развивается уже не один десяток лет, и некоторые страны, например Великобритания, имеют огромный опыт в разработке стандартов – многие британские национальные стандарты, такие как BS7799-1/2, приобрели со временем статус международных. С них и начнем.

Международные стандарты ISO 27002 и ISO 27001 Пожалуй, на сегодня это самые востребованные стандарты в области ИБ.

ISO 27002 (прежде ISO 17799) содержит свод рекомендаций по эффективной организации систем управления ИБ на предприятии, затрагивая все ключевые области, в частности:

- формирование политики ИБ;

- безопасность, связанная с персоналом;

- безопасность коммуникаций;

- физическая безопасность;

- управление доступом;

- обработка инцидентов;

- обеспечение соответствия требованиям законодательства. Стандарт ISO 27001 является сборником критериев при проведении сертификации системы менеджмента, по результатам которой аккредитованным органом по сертификации выдается международный сертификат соответствия, включаемый в реестр.

Согласно реестру, в России в настоящее время зарегистрировано около полутора десятка компаний, имеющих такой сертификат, при общем числе сертификаций в мире более 5000. Подготовка к сертификации может осуществляться либо силами самой организации, либо консалтинговыми компаниями, причем практика показывает, что намного проще получить сертификат ISO 27001 компаниям, уже имеющим сертифицированную систему управления (например, качеством). Стандарты ISO 27001/27002 являются представителями новой серии стандартов, окончательное формирование которой еще не закончено: в разработке находятся стандарты 27000 (основные принципы и терминология), 27003 (руководство по внедрению системы управления ИБ), 27004 (измерение эффективности системы управления ИБ) и другие – всего в серии 27000 предполагается более 30 стандартов. Подробнее о составе серии и текущем состоянии ее разработки можно узнать на официальном сайте ISO (www.iso.org).

Международные стандарты ISO13335 и ISO 15408 Стандарт ISO 13335 является семейством стандартов безопасности информационных технологий, охватывающих вопросы управления ИТ-безопасностью, предлагая конкретные защитные меры и способы. В настоящее время происходит постепенное замещение серии 13335 более новой серией 27000. Стандарт ISO 15408 содержит единые критерии оценки безопасности ИТ-систем на программно-аппаратном уровне (подобно знаменитой Оранжевой книге, которая также известна как критерии оценки TCSEC, или европейские критерии ITSEC), которые позволяют сравнивать результаты, полученные в разных странах.

В целом данные стандарты, хотя и содержат лишь технологическую часть, могут использоваться как независимо, так и при построении систем управления ИБ в рамках, например, подготовки к сертификации на соответствие ISO 27001.

CobiT CobiT представляет собой набор из около 40 международных стандартов и руководств в области управления ИТ, аудита и безопасности и содержит описания соответствующих процессов и метрик. Основная цель CobiT заключается в нахождении общего языка между бизнесом, имеющим конкретные цели, и ИТ, способствующими их достижению, позволяя создавать адекватные планы развития информационных технологий организации. CobiT применяется для аудита и контроля системы управления ИТ организации и содержит подробные описания целей, принципов и объектов управления, возможных ИТ-процессов и процессов управления безопасностью. Полнота, понятные описания конкретных действий и инструментов, а также нацеленность на бизнес делают CobiT хорошим выбором при создании информационной инфраструктуры и системы управления ею.

В следующей части статьи мы рассмотрим некоторые интересные национальные и отраслевые зарубежные стандарты, такие как NIST SP 800, BS, BSI, PCI DSS, ISF, ITU и другие.

\*\*\*

Международный стандарт ISO 20000 Стандарт ISO 20000 заменил собой британский стандарт BS 15000. Он описывает сервисную модель ИТ, реализуя положения специализированной библиотеки ITIL (IT Infrastructure Library – библиотека инфраструктуры ИТ) и концепцию ITSM (IT Service Management – управление ИТ-услугами). Стандарт предъявляет требования к процессам управления ИТ-сервисами и устанавливает критерии оценки, пригодные для проведения сертификаций соответствия. Так же, как и в случае сертификации по ISO 27001, наличие у организации сертификата на какую-либо систему менеджмента упрощает процедуру подготовки к сертификации на соответствие ISO 20000. На сегодняшний день в России всего 6 организаций имеют сертификат ISO 20000.

\*\*\*

Международный стандарт ISO 18044 Стандарт ISO 18044 разработан в соответствии со стандартами ISO 13335-1 и ISO 17799 (ISO 27002) и описывает процесс управления инцидентами ИБ, а также усилия, которые должны быть предприняты на всех этапах жизненного цикла процесса управления инцидентами – от планирования и формирования команды реагирования до извлечения уроков и совершенствования. Он может применяться как при создании системы управления ИБ по ISO 27000, так и самостоятельно в рамках разработки единственного изолированного процесса.

\*\*\*

Комментарий эксперта

Алексей Плешков, начальник отдела защиты информационных технологий, Газпромбанк (Открытое акционерное общество)

Дополнительно к приведенному выше обзору международных стандартов хотелось бы обратить внимание на еще один регламентирующий документ по информационной безопасности, не распространенный на территории РФ. Одним из таких стандартов является документ из линейки методов EBIOS.

Проект EBIOS по разработке методов и инструментальных средств управления ИБ в информационных системах поддерживается правительством Франции и продвигается комиссией DCSSI при премьерминистре Франции на уровень общеевропейского. Назначение этого проекта – способствовать повышению безопасности информационных систем государственных или частных организаций (http://www.securiteinfo. com/conseils/ebios.shtml).

Текст комплекта документации на продукт автоматизации оценочных задач обеспечения ИБ "Методологические инструментальные средства достижения безопасности информационных систем EBIOS (определение потребностей и идентификация целей безопасности)" был опубликован на официальном сайте правительства Франции, посвященном вопросам обеспечения информационной безопасности автоматизированных систем в 2004 г. Метод EBIOS, предложенный Генеральным секретариатом министерства национальной обороны Франции и названный "Определение потребностей и идентификация целей безопасности" (EBIOS), был разработан с учетом международных стандартов, направленных на обеспечение ИБ. Он формализует подход к осуществлению оценки и обработки рисков в области безопасности информационных систем и применяется для оценки уровня ИБ в разрабатываемых и существующих системах.

Цель метода – позволить любой организации, находящейся под управлением государства, определить перечень действий по обеспечению безопасности, которые необходимо предпринять в первую очередь. Метод может быть реализован администраторами подразделения безопасности организации и может применяться на всех уровнях структуры разрабатываемой или существующей информационной системы (подсистемы, прикладные программы). Подход EBIOS учитывает три основных свойства ИБ: конфиденциальность, целостность и доступность как информации, так и систем, а также среды, в которой они находятся. В определенных случаях предлагается позаботиться об обеспечении потребностей неотказуемости, авторизации и аутентификации. Методология EBIOS напрямую связана с оценкой и обработкой рисков. Эти риски квалифицируются как операционные, поскольку они оказывают непосредственное влияние на бизнес-деятельность организации и управление организацией. Данный метод не так неизвестен, как представленные ранее международные стандарты, но все же его можно с уверенностью назвать международным стандартом. На территории Европейского союза применение методологии EBIOS достаточно востребовано. Ряд компаний специализируются на проведении консалтинговых работ в части приведения системы ИБ организации в соответствие требованиям подхода EBIOS.

В качестве справочного материала для знакомства с практикой международных стандартов в области защиты информации рекомендую использовать Интернет-ресурс http://www.iso27000.ru

Георгий Гарбузов, CISSP, MCSE:Security, дирекция информационной безопасности Страховой Группы "УРАЛСИБ"

**Список литературы**

Information Security №1, февраль-март 2009