Леонид ДВОРКИН

ХОРОШИЕ СТАНДАРТЫ ПРИДУМАЛИ БРИТАНЦЫ

ИНТЕГРАЦИЯ BS 7799 В СИСТЕМЫ МЕНЕДЖМЕНТА

Информация и информационные технологии стремительно преобразуют мир. Открытость и доступность информации меняют представления о времени и пространстве, объединяют и вдохновляют людей. Использование собственных потенциалов и возможностей для развития информационной сферы актуально и для каждой организации, и для всей страны. В то же время соперничество людей и конкуренция в бизнесе обусловливают необходимость защиты ценной информации и сопутствующих активов. Этому посвящен новый стандарт системы менеджмента информационной безопасности.
Автор, квалифицированный аудитор по четырем системам менеджмента, рассказывает о стандарте с позиции встраивания защиты информации в общую систему управления организацией.

Многие британские стандарты успешно утверждаются как международные: BS 5750 популярен как ИСО 9001, BS 7750 известен как ИСО 14001, а BS 8800 стал основой для OHSAS 18001. Ценность стандартов в их бесспорности, добротной систематизации, универсальности и возможности неограниченной интерпретации. Единые базовые понятия, процессный подход и структура этих стандартов обусловливают внятную методику их интеграции в общую систему менеджмента организации.

Еще один стандарт, ориентированный на систему менеджмента, — BS 7799. Этот документ состоит из двух частей. Первая (бывший BS 7799-1:1999) принята как международный стандарт ИСО/МЭК 17799:2000 «Информационные технологии. Свод правил по управлению защитой информации» [1] и является набором апробированных и универсальных базовых рекомендаций по инициации, внедрению и обеспечению защиты информации. Вторая часть — BS 7799-2:2002 «Системы менеджмента информационной безопасности. Спецификации с руководством для применения» [2] — подготовлена как модель для налаживания и управления эффективной Системой менеджмента информационной безопасности (СМИБ).

Информация может создаваться и существовать в разных формах: на бумаге или в компьютерном файле, передаваться разными средствами — устно, обычной или электронной почтой. Информацию можно сохранять и перерабатывать, ее можно потерять, уничтожить, украсть. Ценность того, что создано не только руками, особенно значима для нашей страны, поскольку развитие информационной сферы — приоритетная задача, а многие интеллектуальные решения зачастую возвращаются в виде конкурентоспособных продуктов и услуг. Для каждой организации информация вместе с обеспечивающими процессами, системами, сетями является важным активом, условием конкурентного уровня, коммерческого имиджа, сохранения доходов, бесперебойной деятельности. Но и каждый человек, сведения о котором хранятся в различных базах данных, потребитель услуг банка, телефонного или интернет-провайдера вправе рассчитывать на гарантированность защиты информации о себе.

При этом все в большей мере увеличивается вероятность нарушений информационной безопасности и необходимость предотвращать или минимизировать ущерб от вандализма и шпионажа, отказов в работе, вирусов, хакерских атак, огня или наводнения и т.д. Убежденность в защищенности инфор-

мации необходима для государственных учреждений, организаций любых форм собственности и видов деятельности, всех заинтересованных сторон общества.

Информационная безопасность характеризуется в стандарте как сохранение:

- конфиденциальности — обеспечения доступа к информации только авторизованным пользователям;
- целостности — защищенности точности и полноты информации и методов работы с ней;
- доступности — обеспечения авторизованным пользователям возможности пользоваться информацией и сопутствующими активами, когда это требуется.

Стандарт ИСО 17799:2000 предлагает широкий, весьма полный, универсальный набор средств управления защитой информации. Каждая организация сама определяет свои требования к информационной безопасности, руководствуясь:

- оценкой рисков, благодаря которой выявляются опасности для активов, уязвимые места организации, вероятность наступления нежелательных явлений и предполагаемых последствий;
- законодательными, регулирующими, предписанными, контрактными и другими требованиями, которые обязаны соблюдать организации и их партнеры, подрядчики, провайдеры;
- специфическим набором принципов, целей и требований, установленных для информационных ресурсов и процессов, которые необходимы каждой конкретной организации для развития своей деятельности.

Оценка рисков на основе методических подходов является ключевой для идентификации требований по информационной безопасности, поскольку затраты на средства управления определяются с учетом возможных убытков от информационных потерь. В стандарте, как правило, указывается на необходимость использования метода оценки, а выбор и применение метода остается за разработчиком системы. Риск можно рассчитать статистически, оценив потери и повреждения информационных активов (кража, пожар, заражение вирусом и т.п.), вероятность наступления этих событий, а также степень уязвимости системы (недостатки защиты, обслуживания, компетентности, обучения, т.е. сопутствующих условий).

Вторая часть BS 7799 проходит стадии утверждения для принятия в качестве международного стандарта ИСО. Этот документ целенаправленно гармонизирован со стандартами ИСО 9001 и ИСО 14001 для обеспечения последовательности и единства при внедрении и функционировании систем менеджмента. Стандарт устанавливает модель PDCA как часть подхода, используемого в системах менеджмента для создания, реализации и улучшения системы информационной безопасности. Он также соответствует Руководящим принципам Организации экономического сотрудничества и развития [3]. BS 7799-2:2002 подчеркивает, что цели и средства управления, представленные в этом стандарте, являются производными и совпадают с приведенными в стандарте ИСО 17799:2000.

Такой подход и структура предопределяют возможность самостоятельного применения этого стандарта и встраивание в единые системы менеджмента.

Число сертификаций на соответствие стандарту BS 7799 по данным прошлого года составляло уже около 300 в Европе, более 400 — в Азии и Африке, несколько десятков в Америке.

Первая фаза цикла PDCA закладывает основы СМИБ и расписана по шагам.

1. Определение области действий системы менеджмента информационной безопасности, которая может охватывать всю или части организации, ее бизнеса, активов, мест размещения, процессов.

2. Разработка и документирование политики безопасности как основы для установления целей, принципов и общего направления.

3. Идентификация и оценка рисков, а также возможностей управления рисками. Необходимо определить активы информационных систем и их владельцев, возможные опасности (потери) и уязвимые места системы, а также их влияние на конфиденциальность, целостность и доступность системы. Оцениваются возможные потери из-за нарушений информационной системы, вероятность того, что это может произойти, уровень и критерии приемлемости рисков.

4. Управление риском. На основе результатов оценки и ранжирования рисков определяются методы управления рисками, возможности избегать и переводить риски (например, на страховые структуры или поставщиков).

5. Выбор подходящих требований безопасности и средств управления из общего набора для управления рисками.

6. Разработка и документирование заявления об ответственном применении — специального документа, где должны быть перечислены требования стандарта, применимые к соответствующим процессам системы, а исключения обоснованы. Предложенные остаточные риски, полномочия внедрять и поддерживать информационную систему в рабочем состоянии утверждаются руководством.

На второй фазе цикла — внедрения и реализации системы менеджмента информационной безопасности, которая расписана так же подробно, — организация формулирует и исполняет план действий, выделяет ресурсы и определяет приоритеты, распределяет ответственность и обучает сотрудников, внедряет процедуры для реагирования на информационные инциденты.

На третьей фазе проводится мониторинг и анализ СМИБ. Выявляются ошибки, нарушения, анализируется результативность предпринятых действий, оцениваются результаты обратной связи с заинтересованными сторонами, уровни допустимых рисков.

Четвертая фаза предусматривает улучшение СМИБ. Организация регулярно внедряет намеченные улучшения, пред-

принимает корректирующие и предупреждающие меры, сообщает о своих результатах заинтересованным сторонам, убеждается, что улучшения способствуют достижению намеченных целей.

Требования по документации определяют ряд обязательных документов, включая политику, цели, отчет об оценке риска, план управления рисками, заявление об ответственном применении, процедуры и записи, необходимые для планирования, реализации и контроля процессов информационной безопасности. По сравнению со стандартом ИСО 9001 данный стандарт вводит новые обязательные документы, в том числе: Отчет об оценке риска, План управления рисками и Заявление о применимости — специальный документ, где должны быть перечислены требования стандарта, применимые к соответствующим процессам системы, а исключения обоснованы.

В ответственность руководства также по аналогии с базовым стандартом входят: обязательства подтверждать свою руководящую роль в том, что система установлена, внедрена, действует, отслеживается, анализируется, поддерживается и улучшается, необходимые ресурсы определены и обеспечены, а также утверждение уровней допустимых рисков, полномочия внедрять и поддерживать информационную систему в рабочем состоянии. Руководство отвечает и за обучение, осведомленность и компетентность персонала.

Общие требования к анализу СМИБ руководством организации аналогичны требованиям стандарта ИСО 9001. Специфика СМИБ — в регулярном анализе опасностей и уязвимых мест, которые могли быть неадекватно отражены в предыдущей оценке риска. В выходные данные анализа, помимо улучшения эффективности системы и ресурсных нужд, входит модификация процедур для реагирования на внешние и внутренние факторы, потребности бизнеса и процессов, нормирующие требования, а также уровни риска, значимые для системы и их приемлемость.

Требования к внутренним аудитам привычны для тех, кто использует этот инструмент в системах менеджмента. Аудиты должны проводиться регулярно для установления того, что контрольные цели, средства управления, процессы и процедуры отвечают требованиям стандарта и системы, законодательным и регулирующим требованиям, эффективно внедрены и функционируют.

Последний раздел основного текста стандарта завершают общие положения по улучшению СМИБ. Подход к улучшению также соответствует общим требованиям единых систем менеджмента: применение политики и целей, результаты аудитов, анализ результатов мониторинга, корректирующие и предупреждающие действия.

В приложении А (нормативном) стандарта BS 7799-2:2000 помещен весь набор средств управления информационной безопасностью с оговоркой, что он не является исчерпывающим, и организации могут дополнять его при необходимости.

Приложение А включает 12 разделов, начиная с введения. Во втором разделе указано, что советы по внедрению и указания по наилучшему применению, включенные в разделы 3—12 стандарта ИСО 17799:2000, приведены в виде нормативных требований в соответствующих разделах А3—А12 стандарта BS 7799-2:2000. Здесь разделы оформлены в виде таблиц, содержащих соответствующий набор требований, каждая из которых начинается с формулировки цели управления. Это логично и очень удобно.

В раздел А3 включены требования, касающиеся Политики безопасности. Цель — обеспечить стратегию и поддержку менеджмента в области информационной безопасности.

В раздел А4 входят общеорганизационные требования. Они многочисленны и разбиты на подгруппы. Первый подраздел предназначен для создания инфраструктуры информационной безопасности. Цель — управлять безопасностью в организации. Второй регулирует безопасность доступа третьих сторон. Цель — управлять безопасностью информационных ресурсов, к которым имеют доступ сторонние организации. Третий подраздел нацелен на обеспечение безопасности при передаче информационных процессов внешним организациям (при аутсорсинге).

В раздел А5 включены требования к классификации активов и средствам управления ими. В цели двух подразделов включено обеспечение безопасности активов в соответствии со степенью их защиты: составление перечня активов, обращение с ними и маркировка.

Раздел А6 касается безопасности персонала. В первую очередь предусматривается снижение рисков от человеческих ошибок, обманов, краж и неправильного использования оборудования путем определения обязанностей в должностных инструкциях, отбора персонала и соблюдения конфиденциальности. Обучение предусматривается как для персонала, так и для пользователей третьей стороны. Здесь же предусмотрены меры реагирования на инциденты в области информационной безопасности в виде отчетности, изучения причин и дисциплинарного процесса.

Требования раздела А7 направлены на обеспечение физической безопасности и безопасности окружающей среды. Здесь три подраздела: безопасность территории в пределах физического периметра (охраняемое помещение, изолированный склад); безопасность оборудования для предупреждения его утери, перебоев в питании, плохого обслуживания, выноса за пределы территории без удаления информации и т.п.; общие меры, включая политику чистого рабочего стола и экрана, уничтожение активов специальным разрешением. Все цели этого раздела являются превентивными.

Раздел А8 можно считать техническим, он посвящен менеджменту операционной деятельности и коммуникаций. Дифференцированные цели по семи подразделам, которые можно кратко охарактеризовать как стремление к безопасному функционированию компьютеров и сетей, предусматривают:

- обеспечение операционных процедур и обязанностей;
- планирование и приемку систем;

- защиту от злонамеренных программ;
- повседневное обслуживание;
- администрирование сетей;
- безопасное обращение с носителями, удаленный доступ;
- обмен данными и программами с другими организациями.

Технические аспекты и средства не конкретизированы, поскольку концепция этой пары стандартов — реализация целей менеджмента.

Раздел А9 «Управление доступом» содержит самую многочисленную группу требований. Общая цель: управлять доступом к информации, предотвращая несанкционированное использование. Девять подразделов включают:

- производственные требования к управлению доступом;
- управление доступом пользователей;
- обязанности пользователей;
- управление доступом к сетям;
- управление доступом средствами операционных систем;
- управление доступом приложениями;
- слежение за доступом и использованием сетей;
- использование мобильных компьютеров и удаленного доступа.

Раздел А10 «Разработка и сопровождение систем», по сути, охватывает весь жизненный цикл систем. Интегральная цель пяти подразделов — обеспечить выполнение требований безопасности, сохранение конфиденциальности и целостности в процессах анализа, разработки и развития информационной системы организации, поддержание безопасности прикладных систем, средств криптографии, системных файлов.

Раздел А11 посвящен аспектам бесперебойной работы организации. Цель раздела — предотвращение перерывов в деятельности организации и защита критически важных бизнес-процессов от последствий крупных аварий и отказов.

Раздел А12 «Соответствие» — последний раздел нормативного приложения. Общая цель раздела — избежать нарушений законодательных, нормативных, контрактных и других требований по безопасности, включая законы об авторских правах и защите данных, обеспечить соответствие политике безопасности и стандартам организации, максимизировать действенность аудита и минимизировать помехи от этого процесса и вмешательство в него.

Рис. 1. Общие элементы стандартизации систем менеджмента

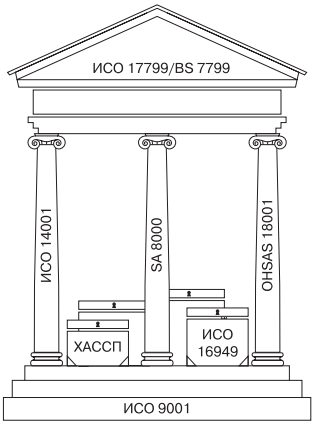

Рис. 2. Храм менеджмента

Приложение В (информативное) является руководством к использованию стандарта и подробно описывает применение фаз цикла PDCA в разработке и поддержании СМИБ.

Пересечение фигур на рис. 1 иллюстрирует общие элементы стандартизации четырех систем менеджмента: область применения, политика, планирование, включая оценку рисков, ответственность руководства, документация и записи, ресурсы, обучение и обмен информацией, операционная деятельность, аудиты, улучшение, корректирующие и предупреждающие действия.

Здесь уместно согласиться с [4], что эта схема пригодна для аудиторов, которые (на основе выборочных наблюдений) проводят оценку соответствия требованиям каждого стандарта. Прекрасная процессно-функциональная трехмерная модель интегральной системы менеджмента, приведенная там же, подтверждает и неограниченный потенциал международных стандартов, и неисчерпаемую изобретательность отечественных консультантов, упорно продвигающих внедрение цельных работоспособных систем в реальное управление деятельностью организаций.

Вдохновляющие концепции и созидательные возможности стандартизованных систем менеджмента ведут к возведению сооружения, начальный эскизный проект которого предлагается на рис. 2.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. BS ISO/IEC 17799:2000. Information Technology — Code of practice for information security management.
2. BS 7799-2:2002. Information security management systems — specification with guidance for use.
3. OECD Guidelines for the Security of Information Systems and Network — Towards a Culture of Security. — Paris: OECD, July 2002.
4. **Василевская С.В.** TQM — основа интегральной системы менеджмента // Методы менеджмента качества. — 2005. — № 1.

Леонид Семенович ДВОРКИН —
кандидат технических наук,
ведущий аудитор систем менеджмента качества