П. А. Демин

ПРОБЛЕМЫ РЕАЛИЗАЦИИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ОСНОВЕ СТАНДАРТИЗИРОВАННЫХ МОДЕЛЕЙ

Общая структура защиты информации включает в себя такие элементы, как люди, организационно-правовой аспект и технологии [1]. Для результативного обеспечения информационной безопасности (далее — ИБ) компании разрабатывают комплекс организационно-правовых мер, который реализуется через внедрение и сопровождение системы управления информационной безопасностью (далее — СУИБ). При этом все чаще при разработке структуры СУИБ компании обращаются к стандартизированным моделям, которые описаны в международных и отечественных стандартах.

На данный момент наиболее широко признанным стандартом в области управления ИБ является международный стандарт ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements», который имеет отечественный аналог ГОСТ Р ИСО/МЭК 27001. В основе стандарта лежат понятия: а) процессного подхода, подразумевающего представление деятельности в виде взаимосвязанных процессов, преобразующих входы в выходы, и б) цикла Деминга—Шухарта (или цикла PDCA), согласно которому в процессе управления и принятия решений существует четыре стадии: P (Plan) — идентификация и анализ проблемы, оценка возможностей, планирование необходимых действий; D (Do) — осуществление планов; C (Check) — проверка, оценка результатов, сопоставление результатов с ожиданиями на этапе планирования; A (Act) — принятие решения на основе оценки полученных результатов, реализация улучшений [2]. Эти же принципы заложены в Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения» [3].

Процессный подход является наиболее прогрессивным методом управления, который стал неотъемлемой частью управления в области ИБ. Однако в ходе внедрения и сопровождения СУИБ на основе стандартизированных моделей компании сталкиваются с рядом проблем, которые обусловлены историческим аспектом, управленческими ошибками, объективными факторами и недостатками самих стандартизированных моделей. В данной статье формулируется проблематика разработки и сопровождения СУИБ на основе стандартизированных моделей.

Роль исторического фактора в проблеме реализации СУИБ на основе стандартизированных моделей можно рассмотреть с двух сторон. С одной стороны, на отечественных предприятиях еще с советских времен сложилась административно-командная система управления функциональными единицами [4]. Построение сквозных бизнес-процессов и выделение цепочек предоставления ценности разрушают стены между подразделениями, что противоречит сложившейся системе управления. В итоге СУИБ, которая должна быть представлена как группа процессов, поддерживающих основные бизнес-процессы компании, становится лишь надстройкой над базисом бюрократизированной структуры, составленной из функциональных единиц, преследующих собственные цели.

С другой стороны, в области информационных технологий в целом и ИБ в частности долгое время сохранялось и продолжает сохраняться главенство технологий, что приводит к недостаточному организационному обеспечению ИБ и размежеванию целей ИБ и целей деловой деятельности. К тому же инженеры не очень охотно берут на себя роли, которые им назначают в рамках различных процессов СУИБ, а руководители нередко воспринимают ИТ-подразделение как «черный ящик».

Рассмотрение группы управленческих ошибок стоит начать с того, что многие руководители не понимают сути процессного подхода. Простая логика модели в данном случае играет с руководителями злую шутку, в итоге они занимаются внедрением процессного подхода,

тогда как требуется проведение существенной работы для понимания процессного подхода и специфики его применения в контексте компании. План внедрения, который рождается после полного осознания модели и выгоды, которую принесет ее применение для организации, должен содержать конкретные, четко сформулированные шаги по трансформации деятельности. Однако в большинстве случаев этап анализа контекста организации пропускается и в погоне за быстрыми «дивидендами» руководители составляют план внедрения.

Одна из причин такого положения дел — погоня за сертификатом, которая рождает «мертвые» системы, существующие только на бумаге. Еще в 2001 г. журнал European Quality, издаваемый Европейской организацией по качеству, опубликовал изложение книги Дж. Седдона «В поисках качества. Дело против ISO 9000» [5]. По мнению автора, внедрение процессного подхода в соответствии с ISO 9000 нанесло ущерб конкурентоспособности сотен тысяч компаний, а подготовка к процедуре сертификации не позволила организациям разглядеть реальные возможности для повышения качества. Желанный сертификат заслонил эти возможности и заставил руководителей думать, что все проблемы решены. Часто эта участь постигает компанию и при внедрении стандартов управления информационной безопасностью.

Так как предметная область процессного подхода — это область управления результатами, а не затратами на их достижение, критическим фактором успешной реализации модели процессного подхода является использование также и системного подхода, т. е. рассмотрение организации как совокупности взаимосвязанных элементов, в первую очередь процессов, но также подразделений, функций и методов. Деминг считал локальную оптимизацию — решение частной задачи по преобразованию вне связи с ее местом в системе — наиболее серьезной управленческой ошибкой [6]. Главной целью реализации процессного подхода является повышение качества продуктов и услуг для конечного потребителя при снижении издержек и дальнейшее непрерывное повышение эффективности, все более приближающее отношение качества к затратам к оптимальному значению. Поэтому только выделение всей цепочки предоставления ценности и формализация видов деятельности, обеспечивающих производство продуктов и предоставление услуг, может дать высокие результаты для всего бизнеса, а не для какой-то отдельной области. В рамках отдельной области, например в СУИБ, процессный подход не имеет никакого смысла, так как сами по себе процессы ИБ компании не представляют интереса для потребителей (только если услуги по ИБ не являются сферой деятельности компании) и могут быть определены как поддерживающие процессы для основных бизнес-процессов компании.

Наиболее серьезной ошибкой в управлении ИБ является нарушение цепочки «люди — процессы — технологии». ИБ-подразделения, как было сказано выше, чрезмерно ориентированы на технологии; это предсказуемо, так как в данной области работают преимущественно люди с техническим образованием, тяготеющие к решению задач с использованием программных и аппаратных средств. Однако значение технологий в общей системе управления крайне мало. Технологии работают там, где они поддерживают и автоматизируют процессы. Процессы должны работать и без технологий, но последние их ускоряют и автоматизируют часть функций. Люди при этом — ключевой компонент системы: те системы, где отлично формализованные процессы поддерживаются дорогими технологиями, но у сотрудников отсутствует приверженность политикам и регламентам СУИБ или принципы организации в отношении информационной безопасности не транслируются должным образом персоналу, являются неэффективными. Поэтому начинать нужно с людей (формирование культуры, мотивация, обучение), продолжать процессами, а заканчивать, если это необходимо, технологиями.

Сложности при реализации стандартизированных моделей также обусловлены объективными факторами. Рассмотрим пример. Модель, предложенная в ISO/IEC 27001:2005, подразумевает реализацию процессов управления конфигурациями и изменениями. Управление конфигурацией

заключается в документировании инфраструктуры в КБД (конфигурационная база данных). Однако с отображением реального мира в информационный связаны существенные проблемы. Во-первых, принципиальная невозможность точного задания атрибутов и описания объектов материального мира, во-вторых, неизменность информационных объектов во времени, что позволяет говорить о том, что время как сущность в информационном мире отсутствует и может поддерживаться только искусственным путем [7]. Таким образом, процесс управления конфигурациями — это поиск приемлемой детализации описания активов и их атрибутов, последующее хранение и предоставление по запросу информации об активах и атрибутах. По мнению многих экспертов, создание и сопровождение централизованной КБД — задача сродни внедрению эффективных и экономически оправданных ERP-систем, т. е. задача утопическая [8].

Процесс управления изменениями можно определить как попытку ввода в информационный мир такого понятия, как время, т. е. поддержания информации об активах и их атрибутах в актуальном состоянии. Проблемы управления изменениями связаны в первую очередь с тем, что изменение (например, замена сетевой платы в сервере) сначала проводится в материальном мире, а затем запускаются процедуры документирования в мире информационном. Таким образом, информационный мир всегда «бежит» за материальным. При этом операции с КБД в промежуток времени после изменения в материальном мире и до документирования этого изменения являются некорректными, так как информация об активе не обновлена и объекта с такими атрибутами в материальном мире уже не существует [7]. Помимо прочего, повышается риск того, что информационное представление вообще не будет актуализировано, если после изменения в материальном мире в силу, например, технического сбоя или человеческого фактора механизм документирования не будет запущен.

Сложнейшей задачей является понимание рисков ИБ в контексте общих рисков компании. Прямое отображение информационных рисков на общие риски организации крайне затруднительно, однако построение СУИБ должно начинаться с анализа идентифицированных рисков, угрожающих целям компании. Некорректно установленная связь рисков ИБ с общими рисками организации ставит под вопрос эффективность применения любых защитных мер в контексте принесения пользы компании. Ясно, что СУИБ не может считаться эффективной, если она не обеспечивает принятие надлежащих мер по защите информации, однако, согласно философии процессного подхода, эти меры не должны быть избыточными, иначе теряется эффективность для бизнеса, а значит, и существование самой СУИБ сомнительно.

Тенденции таковы, что значение информационной сферы и критичности операций, осуществляемых с информацией, постоянно растет, при этом задачи защиты конфиденциальности информации для многих компаний зачастую отходят на второй план, пропуская на первый необходимость противостояния сбоям, отказам, недоступности и падению производительности. Данные факторы заставляют специалистов по ИБ все чаще обращаться к теме управления непрерывностью бизнеса и рассматривать риски ИБ через призму рисков прерываний бизнес-процессов компании. В связи с этим со стороны бизнеса все чаще поступает запрос на модели и подходы, которые позволили бы установить взаимосвязи между информационной безопасностью, непрерывностью бизнеса, управлением рисками и общекорпоративным управлением и задали бы общую платформу для интегрированной системы управления.

СПИСОК ЛИТЕРАТУРЫ:

1. *Малюк А. А.* Информационная безопасность. Концептуальные и методологические основы защиты информации. Учебное пособие. М.: Горячая Линия — Телеком, 2004. — 280 с.
2. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

3. Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения».
4. *Червяков И. В.* «Священные коровы» и процессный подход. URL: http://quality.eup.ru/DOCUM6/sacred_cow.htm.
5. ФГУП РИА «Стандарты и качество». 10 аргументов против применения стандартов ИСО серии 9000. URL: http://quality.eup.ru/GOST/10arguments.htm.
6. *Григорьев Л. Ю., Кислова В. В.* Процессный подход и его роль в построении эффективной компании. URL: http://quality.eup.ru/DOCUM6/pp-rek.htm.
7. *Андрианов В. В., Зефиров С. Л.* Обеспечение информационной безопасности бизнеса. М.: ЦИПСиР — Альбина Паблишерз, 2011. — 373 с.
8. *Rob England*. Introdution to Real ITSM. CreateSpace, 2008. — 124 с.