COBIT: ДАВАЙТЕ РАЗБЕРЕМСЯ!

Лев Фисенко

В процессе наведения порядка в своей IT-системе компании нередко делают вполне закономерные ошибки. Чтобы не наступать на одни и те же грабли, следует лучше изучить мировой опыт, отраженный в различных стандартах и рекомендациях. Но как разобраться в многообразии стандартов? Что выбрать за основу? Не будем давать завуалированных советов, а рассмотрим один из самых известных стандартов - CobiT.

Проблема повышения эффективности управления не нова. С тех пор как люди организовались в социумы, их всегда заботил вопрос улучшения процесса управления. Будь то княжество, армия, племя, коммуна или компания. Сейчас же, в эпоху прогресса, вопрос вышел на новый уровень: требуется управлять информационными системами. Это привело к быстрому развитию целого ряда отраслевых, национальных и международных стандартов, рекомендаций по управлению IT и, как следствие, IT-безопасностью.

Интернациональным компаниям приходится вести свою деятельность, следуя положениям нормативных актов соответствующих стран. Бизнес сталкивается со все более ужесточающимися требованиями со стороны надзорных органов и общественности, которые предписывают компаниям должным образом использовать и защищать как корпоративную, так и персональную информацию. Эти нормативные документы касаются всех сфер, от безопасности до финансовой отчетности, и включают в себя американские законы SOX (Sarbanes-Oxley Act) и HIPAA, директивы Евросоюза и прочие.

Как правило, подход к управлению рисками IT-безопасности распределен по подразделениям компании. Вследствие этого часто функциональные обязанности и технические средства, необходимые для их выполнения, дублируются. Системы управления же частично перекрываются и противоречат друг другу. В результате администраторы не знают, насколько успешно они управляют сетевыми рисками.

Современный бизнес работает в бурном ритме, многие компании и организации не имеют временного ресурса для выработки собственных требований и стандартов. Поэтому активно используется чужой опыт и лучшие мировые практики, к которым относятся и стандарты. Стандарты управления и IT-безопасности были созданы на основе анализа методов, опробованных как большими группами профессионалов, так и множеством различных компаний и организаций. Как правило, стандарты подаются как рекомендации.

Кроме признанных международных стандартов управления и IT-безопасности, существует много национальных. Например, Control Objectives for Information and Related Technology (CobiT) наиболее часто используется для управления информационными системами в США и ряде других стран, а в Великобритании, Нидерландах и Австралии чаще используется IT Infrastructure Library (ITIL).

CobiT

CobiT — это сокращение от Control Objectives for Information and Related Technology («Задачи информационных и смежных технологий»).

CobiT представляет собой пакет открытых документов, около 40 международных и национальных стандартов и руководств в области управления IT, аудита и IT-безопасности. Создатели стандарта провели анализ и оценку и объединили лучшее из международных технических стандартов, стандартов управления качеством, аудиторской деятельности, а также из практических требований и опыта — все то, что так или иначе имело отношение к целям управления.

Задача CobiT заключается в ликвидации разрыва между руководством компании с их видением бизнес-целей и IT-департаментом, осуществляющим поддержку информационной инфраструктуры, которая должна способствовать достижению этих целей.

Нередко руководство компании в силу объективных причин не понимает IT-специалистов. По представлению руководства, сотрудники IT-подразделения разговаривают на каком-то птичьем языке. Те, в свою очередь, не понимают бизнес-терминов, на основании которых строятся распоряжения руководства. Это все приводит к росту издержек, выполнению лишней работы, что, конечно же, сказывается на эффективности деятельности компании.

CobiT, благодаря единой терминологии, служит своеобразной платформой-буфером для конструктивного диалога между всеми участниками бизнеса:

- топ-менеджерами;
- руководителями среднего звена (IT-директором, начальниками отделов);
- непосредственными исполнителями (инженерами, программистами и т. д.);
- аудиторами.

В CobiT детально описаны цели и принципы управления, объекты управления, четко определены все IT-процессы (задачи), протекающие в компании, и требования к ним, описан возможный инструментарий (практики) для их реализации. В описании IT-процессов также приведены практические рекомендации по управлению IT-безопасностью.

Кроме того, CobiT вводит целый ряд показателей (метрик) для оценки эффективности реализации системы управления IT, которые часто используются аудиторами IT-систем. В их число входят показатели качества и стоимости обработки информации, характеристики ее доставки получателю, показатели, относящиеся к субъективным аспектам обработки информации (например стиль, удобство интерфейсов). Оцениваются показатели, описывающие соответствие компьютерной IT-системы принятым стандартам и требованиям, достоверность обрабатываемой в системе информации, ее действенность, общепринятые показатели информационной безопасности — конфиденциальность, целостность и доступность обрабатываемой в системе информации.

В CobiT вводится понятие модели зрелости процесса, показывающей, как процесс может быть улучшен. Если обобщить, то управление IT по CobiT можно представить в следующем ступенчатом виде (по порядку реализации):

- Стратегии (выстраивание IT-процесса по бизнес-целям, постановка задачи, цели и создание концепции IT-процесса; ответственные: руководство бизнес-подразделений).
- Политики (методы достижения целей в рамках стратегий, например: «длина пароля регламентируется»; ответственные: руководство IT-подразделений).
- Стандарты (метрики для политик-методов, например: «длина пароля должна составлять не менее 8 символов»; ответственные: руководство IT-подразделений).
- Процедуры (регламенты работ для применения политик-методов с использованием стандартов-метрик, рабочие инструкции для исполнителей; ответственные: руководство IT-подразделений).

Стандарт отвечает всем потребностям практики, сохраняя независимость от конкретных производителей, технологий и платформ. При разработке стандарта была заложена возможность использования его как для проведения аудита IT-системы компании, так и для проектирования IT-системы. В первом случае CobiT позволяет определить степень соответствия исследуемой системы лучшим образцам, а во втором — спроектировать систему, почти идеальную по своим характеристикам.

История CobiT

Первая версия стандарта была выпущена в 1996 году Организацией аудита и контроля информационных систем (Information Systems Audit and Control Foundation, ISACF) с целью обеспечения методов оценки и контроля, которые пригодились бы и IT-персоналу, и аудиторам, и клиентам. Она включала концептуальное ядро, определяющее набор основополагающих принципов и понятий в области управления IT, описание задач управления и руководство по аудиту. Вторая, переработанная версия CobiT была опубликована в 1998 году.

Третья редакция была выпущена уже в 2000 году Институтом управления информационными технологиями (IT Governance Institute), учрежденным Ассоциацией аудита и контроля информационных систем (Information Systems Audit and Control Association, ISACA) совместно с ISACF с целью развития и популяризации принципов управления IT (в настоящее время названный институт и является основным разработчиком CobiT). Проект подготовки третьей редакции CobiT включал разработку принципов управления и переработку второго издания с использованием новых и пересмотренных международных источников. Кроме того, концепция CobiT была пересмотрена и расширена, с тем чтобы предусмотреть усиленный административный контроль, ввести управление производительностью и развить управление IT.

Новая редакция — CobiT 4.0

Институт управления IT постоянно совершенствует CobiT. С этой целью в течение последних нескольких лет институт организовал детальные исследования по ряду аспектов целей и принципов управления.

Год назад был принят CobiT 4.0 — расширение 3-й редакции. Введение 4-й редакции дало возможность улучшить управление и средства контроля:

- Анализ положений CobiT и практик ведущих компаний мира выявил пробелы, которые были ликвидированы посредством изменения названий некоторых IT-процессов и добавления новых целей управления.
- В CobiT включена таблица, показывающая связь между бизнес-задачами, IT-целями и определенными в CobiT IT-процессами.
- Для облегчения интеграции CobiT с другими, более детальными, руководствами (ITIL, ISO 17799 и прочими) была проведена унификация используемых терминов и принципов.
- Из-за большого количества рекомендаций по оценке эффективности, предназначенных в основном для аудита, в CobiT всегда делался большой акцент на управление рисками. В CobiT 4.0 достигнут компромисс между рисками и возвратом инвестиций.
- CobiT 4.0 содержит диаграммы, показывающие, кто несет ответственность, кто подотчетен, с кем необходимо консультироваться и кого необходимо проинформировать для описания ролей и ответственности за каждый IT-процесс.

Источники совершенствования: ITIL и CobiT

Преимущество стандартов в их разнообразии и множестве: в этом случае повышается вероятность того, что один из них подойдет в конкретной ситуации. Если CobiT не подходит, можно применить ITIL. Но есть ли взаимосвязь или взаимозависимость между CobiT и ITIL?

ITIL — библиотека лучшего практического опыта в части управления IT-услугами, а CobiT специализируется и на управлении, и на аудите IT. Необходимо отметить, что и к процессам ITIL могут быть применены принципы контроля и управления CobiT. Посредством использования CobiT руководители IT-подразделений преобразуют задачи бизнеса в четкие и понятные планы развития IT. Методология ITIL применяется для

оптимизации процесса обслуживания информационных систем с точки зрения управления.

Стандарт CobiT и библиотека ITIL не являются противоречащими друг другу подходами (наборами передового опыта), они дополняют друг друга, охватывая разные сферы деятельности и разные уровни управления. Оба стандарта оказываются более полезными именно тогда, когда используются вместе, а не по отдельности.

CobiT помогает понять, что следует делать для решения поставленной задачи, а ITIL показывает, как этого достичь.

ITIL & CobiT позволяют повысить производительность и эффективность операционных процессов IT-подразделения. Они могут продуктивно использоваться совместно для контроля и построения структуры качественного управления IT. CobiT и ITIL вместе образуют ценную комбинацию ресурсов, помогающих организации управлять IT исходя из бизнесзадач.

Достоинства использования

Плюсы использования стандартов состоят в отсутствии необходимости тратить финансовые, человеческие и прочие ресурсы на разработку стратегии управления. Намного удобнее и выгоднее использовать чужой опыт.

Но никакой стандарт не сможет охватить весь объект управления в деталях. Поэтому необходимо иметь представление обо всех основных стандартах. Их содержание и идеи должны быть готовы к использованию в подходящей ситуации.

Допустим, ISO 17799 говорит нам о важности аудита IT-безопасности, но не содержит никакой информации о том, как его осуществлять.

А вот здесь пригодятся принципы аудита CobiT. Процесс управления IT-безопасностью описан в BS 7799, а оперативная составляющая управления IT-безопасностью описана в специальном разделе ITIL. То есть построение системы управления должно быть основано на лучшем из соответствующих стандартов.

Организация, решившая применить стандарты, сталкивается с множеством проблем. Во-первых, чтобы убедить каждого сотрудника работать в соответствии со стандартами, потребуется время. Об этом, так же, как о стоимости процесса перехода от старого способа работы к новому, часто забывают. Стандарт не всегда будет соответствовать текущим условиям. Его адаптация к ним, если она вообще возможна, вызывает дополнительные затраты. Вследст вие формальной природы стандартов их внедрение поможет сделать процессы менее гибкими, более статичными.

Иногда это может привести к серьезным проблемам: динамика сегодняшних бизнес-процессов порой требует гибкости.

Особенности национальной стандартизации

Все эти стандарты, рекомендации и требования, безусловно, хороши. Но все-таки они основаны, хоть и на лучших, но зарубежных практиках. Фраза об особенностях российского менталитета и практики ведения бизнеса уже набила оскомину. Но, как ни крути, уйти от нашей российской действительности не получится. Внедряя стандарты и требования, придется делать поправки. Может быть, некоторые, достаточно замкнутые в плане общения с внешним для компании миром подразделения смогут с успехом перенять весь зарубежный опыт, заключенный в различных рекомендациях, требованиях, правилах и т. д. Но для компании в целом перейти на зарубежные стандарты будет сложно и в большинстве случаев этот переход будет только декларируемым и формальным. Этому есть несколько причин. Во-первых, надо признать, что во всем цивилизованном мире уже давно формализовано все и вся. Существует огромное количество инструкций, требований и прочего. Главное — они все четко выполняются. Нашим цивилизованным соседям по планете не привыкать жить и работать таким образом. Мы же только учимся этому (хотя надо ли нам это делать?). Во-вторых, деятельность абсолютного большинства

компаний тесно связана или контролируется государственными структурами, имеющими свои собственные требования. И они будут иметь приоритет для выполнения, так как несоответствие им может повлечь неприятности для компании или, того хуже, прямые санкции.

На нынешний день российским компаниям приходится проявлять чудеса гибкости и изворотливости, лавируя между отечественными и зарубежными рекомендациями и стандартами.