УДК 006.3:004
ББК 72Ц
К – 59

Козлова Наталья Шумафовна, *кандидат философских наук, доцент кафедры организации и технологии защиты информации Майкопского государственного технологического университета, тел.: 89064381616.*

ИССЛЕДОВАНИЕ ПРОЦЕССА ВНЕДРЕНИЯ СТАНДАРТА CobiT

(рецензирована)

Построение эффективной системы обеспечения безопасности, управления и контроля над информационными технологиями решает не только внутренние проблемы, но и позволяет повысить привлекательность организации извне, позиционируя ее как преуспевающую, открытую, надежную и идущую в ногу со временем.

Ключевые слова: информационные технологии, стандарты CobiT и ITIL, система обеспечения безопасности, ИТ–процесс, информационная безопасность.

Kozlova Natalia Shumafovna*, Candidate of Philosophy, assistant professor of the department of organization and technology of information security, Maikop State Technological University, tel.: 89064381616.*

STUDYING OF THE IMPLEMENTATION OF THE STANDARD CobiT

Modeling of the effective security management system, management and control of information technology not only solves internal problems, but also enhances the attractiveness of the organization from the outside, positioning it as a prosperous, open, reliable, and up-to-date.

Keywords: information technology, standards CobiT and ITIL, security system, IT process, information security.

Эффективное управление информацией и смежными информационными технологиями (ИТ) является важным для выживания и успеха организации. Вследствие влияния таких факторов, как увеличивающаяся зависимость от информации и систем, предоставляющих эту информацию; размер и стоимость текущих и будущих инвестиций в информацию и информационные системы, а также создающий новые благоприятные возможности и снижающий стоимость их реализации в глобальном информационном сообществе, где информация передается через киберпространство без ограничений по времени, расстоянию и скорости, управление информационными технологиями возрастает.

Для многих организаций информация и поддерживающие ее технологии являются наиболее ценными активами. Более того, в современном быстроменяющемся бизнесе руководство требует от ИТ: повышения качества, функциональных возможностей, простоты использования, а также постоянного уменьшения времени обслуживания, улучшения уровня обслуживания при более низких затратах. Многие организации осознают потенциальные выгоды, которые могут привнести технологии. Успешные организации, напротив, понимают и управляют риском, связанным с внедрением новых технологий.

О полноправной интеграции стандартов обеспечения безопасности в сферу информационных технологий, свидетельствует определение ролей производителей, потребителей и экспертов по квалификации ИТ– продуктов и разделение функций в процессе создания защищенных систем обработки информации.

Развитие стандартов привело к отказу от единой шкалы ранжирований и критериев, замене ее множеством независимых частных показателей и введению частично упорядоченных шкал.

На основе современных стандартов складывается разделение ролей участников процесса создания и эксплуатации защищенных систем, применение соответствующих механизмов и технологий приводит к сбалансированному распределению ответственности между всеми участниками процесса. Стандарты носят на сегодняшний день гораздо более неформальный характер

и представляют собой скорее набор практических рекомендации по развертыванию и поддержанию системы управления информационной безопасностью.

Миссия стандарта CobiT (Разработан Ассоциацией Аудита и Контроля Информационных Систем (ISACA), название дословно расшифровывается как «Контрольные Цели (показатели) для Информационных и Смежных Технологий») состоит в исследовании, разработке, рекламе и продвижении международного набора авторитетных, отвечающих современным требованиям, общепризнанных задач управления (Control Objectives) ИТ для повседневного использования бизнес менеджерами и аудиторами [3].

Актуальность задач, связанных с организацией, управлением и аудитом информационных и смежных технологий и их защитой довольно высока. Обусловлено это тем, что в настоящий момент в большинстве организаций как коммерческой, так и иной направленности наблюдается выдвижение ИТ–процессов на роль лидирующих и определяющих успешность иных производственных и бизнес–процессов. Построение эффективной системы обеспечения безопасности, управления и контроля над ИТ решает не только внутренние проблемы, но и позволяет повысить привлекательность организации извне, позиционируя ее как преуспевающую, открытую, надежную и идущую в ногу со временем [3]. Одно из решений подобной задачи – внедрение стандартов CobiT и ITIL, которые формализуют не только конкретные проекты в сфере ИТ, но и создают (на основе процессного подхода) то ядро управления и контроля ИТ, вокруг которого выстраиваются производственные процессы организации с максимально возможным уровнем эффективности.

В первую очередь начало процесса внедрения данных стандартов в организации предполагает переход от функционального построения деятельности ИТ–отдела к процессному подходу и для этого не потребуется коренной перестройки всей информационной системы. Несмотря на свои недостатки, эта система все же довольно эффективно выполняет возложенные на нее функции. Необходимо четкое понимание того, что достаточно отлаженную реально функционирующую сложную информационную систему не заменит собой никакой стандарт.

На практике применять абсолютно все требования и рекомендации стандартов, разрушая уже проверенные временем механизмы, необходимости нет и лишь в тех областях, где замечены существенные недостатки, применение положений рассматриваемых стандартов может реально повысить эффективность ИТ–сервисов.

Следует начать с выработки общего стратегического направления развития ИТ–сервисов в организации, совпадающего с задачами всей организации в целом и построения четкой иерархической системы целей функционирования информационной системы организации. Рассмотреть необходимо всю деятельность ИТ–отдела на уровне отдельных действий, а также транзакций в информационной системе, то есть произвести подробный анализ деятельности. Далее следует начинать группировку отдельных действий и транзакций в их связанные последовательности, каждая из которых направлена на достижение своей строго определенной цели. Каждая такая последовательность, которая задействует ресурсы и имеющая определенные показатели эффективности на выходе составляет процесс в понимании CobiT и ITIL. Иерархическая система целей и процессов позволит увидеть недостающие и лишние процессы, что в свою очередь позволит выработать конкретные рекомендации для оптимального распределения ресурсов и более эффективного достижения целей.

Начинать внедрение стандарта CobiT в деятельность организации следует поэтапно в соответствии с описанием:

1. Определение бизнес целей на основе Концептуального ядра CobiT относительно организации – объекта применения, главная цель функционирования ИТ–отдела – обеспечение стабильной работы информационной системы с заданными показателями безопасности и эффективности.
2. Выбор ИТ–процессов и механизмов управления с использованием высокоуровневых и детальных задач управления.
3. Согласование программы внедрения с бизнес планом.
4. Оценка существующих процедур и результатов внедрения механизмов управления при помощи «Руководства по аудиту».

5. Оценка текущего статуса организации, идентификация критичных действий, ведущих к успеху, и измерение производительности в достижении целей организации при помощи «Руководства по менеджменту».

Критические Факторы Успеха (Critical Success Factors) стандарта CobiT определяют наиболее важные ориентированные на руководство методы внедрения системы управления ИТ–процессами [3]. Это наиболее важные задачи, решение которых способствует достижению целей ИТ–процессов. К числу наиболее общих факторов успеха, применимых к любому ИТ–процессу, предлагается отнести: стандартизацию ИТ–процессов и их нацеленность на достижение целей бизнеса; определение групп пользователей ИТ–процессов; обеспечение масштабируемости ИТ–процессов и оптимального управления ресурсами в рамках этих процессов; качество персонала информационной системы; использование финансовых метрик для измерения производительности ИТ–процессов и премирование руководителей ИТ отделов на основании результатов этих измерений; наличие процедур контроля и повышения качества ИТ–процессов.

Ключевые Индикаторы Целей (Key Goal Indicators) CobiT определяют критерии для оценки достижения бизнес целей при помощи ИТ–процессов. Основными общими целями совокупности ИТ–процессов в организации, в соответствии со стандартом, можно выделить следующие [3]:

1. Улучшение управления производительностью и затратами.
2. Увеличение отдачи от вложений дополнительных ресурсов в ИТ.
3. Сокращение времени запуска в эксплуатацию нового продукта, услуги.
4. Улучшение управления качеством, новшествами и рисками.
5. Соответствующая интеграция и стандартизация бизнес–процессов.
6. Положительные отзывы от клиентов информационной системы.
7. Выполнение требований и ожиданий клиента по качеству и времени.
8. Соответствие законам, инструкциям, промышленным стандартам и договорным обязательствам.
9. Полное осознание меры принимаемого риска, а также соответствие уровню риска, приемлемого для данной организации.
10. Эталонное тестирование зрелости управления ИТ.

Ключевые Индикаторы Производительности (Key Performance Indicators) CobiT определяют критерии для оценки производительности ИТ процессов в достижении ими бизнес целей организации. Примерами наиболее общих индикаторов производительности должны служить [3]:

11. Увеличение рентабельности ИТ–процессов.
12. Улучшение работы и планирования действий по совершенствованию ИТ–процессов.
13. Увеличение нагрузки на ИТ–инфраструктуру.
14. Повышение степени удовлетворения пользователей.
15. Улучшение взаимодействия и коммуникаций между руководителями ИТ и руководством организации.
16. Повышение производительности сотрудников.

Использование описанных показателей (индикаторов) позволяет реализовать стандартизированные, управляемые и измеряемые ИТ–процессы. Например, по отношению к ИТ–процессу «Обеспечение антивирусной защиты корпоративной сети» в качестве ключевых индикаторов целей выступают минимизация количества заражений вирусами компьютеров, подключенных к сети и минимизация последствий таких заражений.

Перекрытие всех возможных каналов распространения компьютерных вирусов, регулярность обновлений антивирусных баз данных и оптимальность настроек антивирусного программного обеспечения являются критическими факторами успеха. Ключевыми показателями эффективности данного ИТ–процесса являются количество обнаруживаемых и успешно обезвреживаемых вирусов, а также скорость и качество реагирования на инциденты, связанные с заражением компьютерными вирусами.

Исходя из проведенного исследования, можно сделать вывод о том, что адекватное применение процессного подхода, реализованного в стандартах CobiT и ITIL, а также выполнение требований и рекомендаций данных стандартов могут значительно улучшить ИТ–сферу организации, и вывести ее на современный уровень при оптимизации расходования ресурсов. Данные стандарты не ориентированы на то, чтобы пересмотреть все устоявшиеся правила, нормы и

требования. Конечно, при необходимости, в них можно найти довольно детализированные действия и примеры, касающиеся ИТ–сервисов и мер обеспечения ИТ–безопасности. Но их главная ценность в том, что они направлены на упорядочивание и организацию контроля уже осуществляемой деятельности по ИТ и ЗИ, причем большинство обычных действий и транзакций останутся без изменения. CobiT и ITIL позволяют проанализировать и по–другому взглянуть на ИТ в целом не как на набор часто бессвязных функциональных требований, а как на совокупность взаимосвязанных процессов с четко поставленными целями, временем, задействованными ресурсами.

На основании стандартов, информационная безопасность рассматривается как процесс защиты информационных активов организации от различного рода угроз. CobiT и ITIL являются бесценным источником оптимальных и заведомо эффективных решений, а поэтому их использование во многих случаях может чрезвычайно упростить практическую деятельность специалиста в области информационной безопасности.

Литература:

1. Зегжда Д.П., Иващенко А.М. Основы безопасности информационных систем. М.: Горячая линия – Телеком, 2000.;
2. Киберев А.Е. ITIL набирает популярность // КомпьютерПресс. 2007. №9;
3. CobiT 3rd Edition, Released by the CobiT Steering Committee and the IT Governance Institute, July 2000;
4. Version 1.1. Technical Report CMU/SEI-93-TR-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, February 1993;
5. KPMG. Global Information Security Survey, 2002.