УДК 330.47

Методология управления информационной безопасностью на базе международных стандартов

Нартов Павел Юрьевич, преподаватель, Университет Нархоз, Алматы, Казахстан

В статье рассматриваются вопросы определения и классификации существующих стандартов управления информационной безопасностью с точки зрения дальнейшего методологического сопровождения повышения уровня информационной безопасности различных организаций.

Ключевые слова: *информационная безопасность, менеджмент*

In this article the questions of identification and classification of modern standards of information security management are examined in the context of further methodological maintenance of the upgrading of the level of information security of different organizations.

Key-words: *information security, management*

Современное общество все больше сталкивается с проблемой обеспечения информационной безопасности. И если раньше внедрение компьютеризированных систем рассматривалось исключительно как благо, снижающее трудозатраты и повышающее оперативность принятия решений, то на текущем этапе общественного развития экономическая сфера жизни общества сталкивается с ростом угроз действующим информационным системам. В частности, российская экономика стала постоянно сталкиваться с обозначенной проблематикой: так, по итогам 2016 года зафиксировано свыше 70 млн. т.н. хакерских атак на российские информационные ресурсы, а также несколько крупных попыток дестабилизировать финансовый сектор страны [1].

В связи с этим, внимание академических исследователей должно обратиться к поиску методологических основ и предпосылок по формированию более устойчивой системы управления информационной безопасностью в рамках развития общей теории управления. В данной связи, на первом этапе методологического сопровождения будущих теорий целесообразно рассмотреть существующие практические модели поддержания информационной безопасности. К основным стандартам, разработанным в западных странах и широко применяющимся во всем мире, относятся следующие серии документов: ITIL, ISO, COBIT.

Стандарт ISO относится к группе международных документов, связанных с универсальной стандартизацией аспектов человеческой деятельности. В том числе данный стандарт регламентирует вопросы поддержания и обеспечения информационной безопасности (ISO 27001, 2013 г.). ISO 27001 базируется на модели Deming cycle (взаимосвязанные элементы которой заключаются в следующих действиях: планирование, реализация, аудит, исправление).

Общие рекомендации стандарта таковы:

1-ый этап. Разработка политики управления ИТ-безопасностью, содержащей определение «слабых мест» информационных систем, а также основных групп информационных рисков (в том числе рисков физического уничтожения баз данных).

2-ой этап. Разработка программы совершенствования и развития ИТ-систем на основании политики.

3-ий этап. Оптимизация / модернизация программного обеспечения в соответствии с политикой и программой.

4-ый этап. Аудит (систематический) информационных систем на предмет реализации потенциальных рисков информационной безопасности.

5-ый этап. Постоянное обновление и актуализация как документарной, так и аппаратной части системы обеспечения информационной безопасности.

Основное достоинство представленного стандарта ISO заключается в унификации принципов управления безопасностью и общей инфраструктурой информационных систем, однако же, за счет этого снижаются адаптационные возможности при внедрении стандарта на различных предприятиях и/или в организациях.

Документы серии ITIL (библиотека инфраструктуры информационных технологий) развивают системный подход стандарта ISO к вопросам информационной безопасности. Основными направлениями для достижения более безопасных форм управления информационными технологиями признаются имплементация информационной безопасности в процессы разработки уровней качества информационных услуг на предприятии, а также формирование оптимального уровня информационной безопасности в соответствии с имеющимися ресурсами (людскими, финансовыми и проч.).

За счет более широких возможностей согласования общеэкономических и информационных аспектов и приоритетов деятельности организации, ITIL является гораздо более «подвижным» стандартом, по сравнению с ISO 27001. Его дополнительным преимуществом является также возможность модульного внедрения, исходя из существующих условий (возможностей и угроз) внешней среды. В свою очередь, основные регламентирующие условия для внедрения ITIL заключаются в следующем:

* Возможность комплексного внедрения принципов управления информационными системами в соответствии с обозначенными условиями и требованиями, а также информирование всех участников организационной системы о заданных условиях и принципах.

* Возможность постоянного отслеживания функционирования информационных систем на предмет реализации инцидентов (проблем) с информационной безопасностью и иными угрозами.

С учетом данных ограничений, внедрение ITIL, даже с учетом модульной реализации, является крайне затратным мероприятием, предполагающим де-

тальное обучение сотрудников организации принципам функционирования стандарта.

Стандарт COBIT, впервые разработанный в США, в отличие от двух предшествующих систем документов, концентрируется на четко определенном перечне информационных процессов (включая процесс обеспечения и поддержания информационной безопасности). COBIT оперирует понятием «уровень зрелости процесса», каждый из которых предполагает качественное поддержание исполнения каждого процесса на определенной ступени (начиная от «0» - отсутствие процесса, до «5» - процесс достиг возможности самооптимизации).

В вопросах информационной безопасности COBIT предполагает исполнение следующего плана действий:

1. Определение ведущих / ключевых задач обеспечения информационной безопасности.

2. Обозначение приемлемого уровня риска информационной безопасности (в соответствии со стратегией развития информационных систем).

3. Разработка плана минимизации возможных рисков (угроз) безопасности.

4. Поддержание и развитие компетенций управления информационной безопасностью.

Важным дополнительным отличием COBIT от ITIL является возможность внедрения (и последующего поддержания) процесса управления информационной безопасностью на заданном уровне, без внедрения и необходимости одновременного развития каких-либо связанных модулей, что значительно снижает нагрузку на бюджет организаций. Вместе с тем, данный стандарт крайне специализирован с точки зрения использования специальной терминологии и требует относительно высокого базового уровня понимания информационных процессов (при этом, в COBIT отсутствует широкая детализация действий с пояснениями для менеджеров по сравнению с ISO и ITIL).

Итак, подводя итог данной работе, мы можем констатировать необходимость дальнейшего всестороннего изучения существующей методологической

базы управления информационной безопасностью в рамках освоения накопленного зарубежными организациями опыта. Промежуточная классификация существующих стандартов для последующего развития отечественного опыта (как в аспекте теории, так и практики) представлена в таблице 1.

Таблица 1

Трехуровневая классификация стандартов управления информационной безопасностью

Стандарт	**Сильная сторона**	**Слабая сторона**	**Применимо в…**
ISO	Универсальная модель в основе	Низкая адаптируемость	Крупных и транснациональных компаниях
ITIL	Возможность модульного внедрения	Дорогостоящее комплексное внедрение	Финансово обеспеченных компаниях
COBIT	Наибольшая гибкость	Избыточность регуляторных аспектов	Молодых компаниях и стартапах

Список используемых источников:

1. ФСБ: более 70 млн. атак совершено в прошлом году на российские информресурсы. Финмаркет [Электронный ресурс]. Режим доступа: http://www.finmarket.ru/news/4459144, свободный.