Стандарты в области управления информационными рисками

написано Александр Астахов | 10 июня, 2023

Прародитель международных стандартов управления информационной безопасностью – британский стандарт BS 7799. Его первая часть – BS 7799-1 «Практические правила управления информационной безопасностью» – была разработана Британским Институтом стандартов (BSI) в 1995 г. по заказу правительства Великобритании. Как следует из названия, этот документ является практическим руководством по управлению информационной безопасностью в организации. Он описывает 10 областей и 127 механизмов контроля, необходимых для построения СУИБ, определенных на основе лучших примеров из мировой практики. В 1998 году появилась вторая часть этого британского стандарта – BS 7799-2 «Системы управления информационной безопасностью. Спецификация и руководство по применению», определившая общую модель построения СУИБ и набор обязательных требований для сертификации. С появлением второй части BS 7799, определившей, что должна из себя представлять СУИБ, началось активное развитие системы сертификации в области управления безопасностью. В 1999 году обе части BS 7799 были пересмотрены и гармонизированы с международными стандартами систем управления ISO 9001 и ISO 14001, а год спустя технический комитет ISO без изменений принял BS 7799-1 в качестве международного стандарта ISO 17799, который впоследствии был переименован в ISO 27002.

Вторая часть BS 7799 пересматривалась в 2002 г., а в конце 2005 г. была принята в качестве международного стандарта ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования». В это же время была обновлена и первая часть стандарта. С выходом ISO 27001 спецификации СУИБ

приобрели международный статус, и теперь роль и престижность СУИБ, сертифицированных по стандарту ISO 27001, значительно повысились.

BS 7799 и его международные редакции постепенно стали одними из наиболее важных стандартов для отрасли информационной безопасности. Однако, когда в августе 2000 г. в ISO обсуждалась первая редакция международного стандарта ISO 17799, с трудом удалось достичь консенсуса. Документ вызвал массу критических замечаний со стороны представителей ведущих ИТ держав, которые утверждали, что он не отвечает основным критериям, предъявляемым к международным стандартам. «Не было даже возможности сравнить этот документ со всеми остальными работами по безопасности, когда-либо рассматриваемыми в ISO», – говорит Жене Трой, представитель США в техническом комитете ISO.

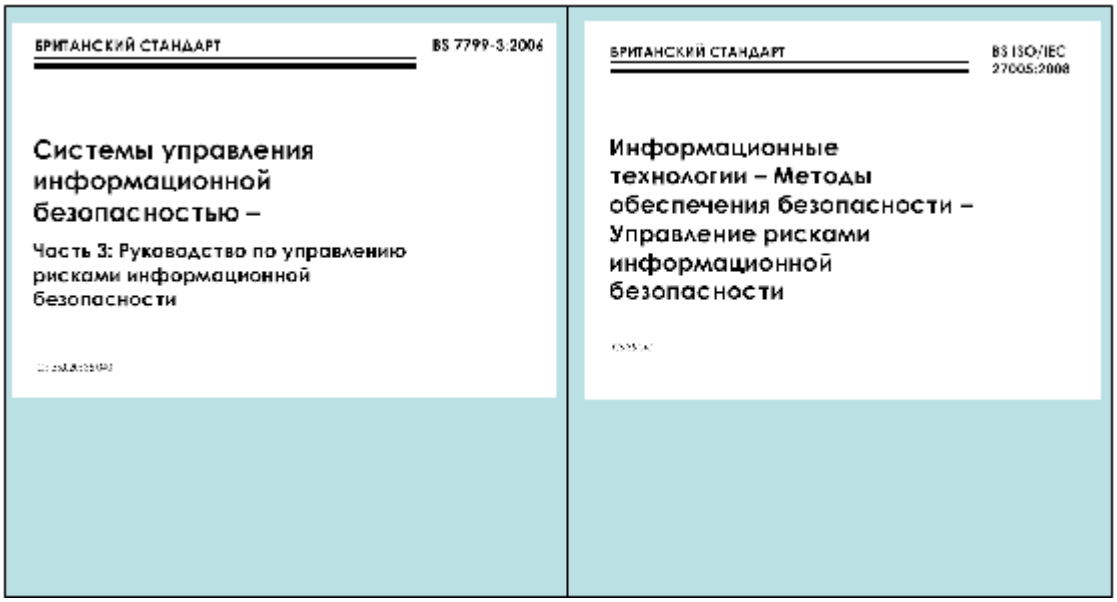
Сразу несколько государств, включая США, Канаду, Францию и Германию, выступили против принятия ISO 17799. По их мнению, этот документ хорош как набор рекомендаций, но не как стандарт. В США и европейских странах до 2000 г. уже была проделана огромная работа по стандартизации информационной безопасности. «Существует несколько различных подходов к ИТ безопасности. Мы считали, чтобы получить действительно приемлемый международный стандарт, все они должны быть приняты к рассмотрению, вместо того чтобы взять один из документов и ускоренно его согласовать, – говорит Жене Трой. – Главный стандарт безопасности был представлен как свершившийся факт, и просто не было возможности использовать результаты другой работы, проделанной в этой области».

Представители BSI возражали, что работы, о которых идет речь, касаются в основном технических аспектов, а BS 7799 никогда не рассматривался как технический стандарт. В отличие от других стандартов безопасности, таких как Commonly Accepted Security Practices and Regulations (CASPR) или ISO 15408/Common Criteria, он определяет основные не технические аспекты защиты информации, представленной в любой форме. «Он должен быть

таким, так как предназначается для любых видов организаций и внешних окружений, – говорит представитель BSI Стив Тайлер (Steve Tyler). – Это документ по управлению информационной безопасностью, а не каталог ИТ продуктов».

Несмотря на все возражения, авторитет BSI (являющегося основателем ISO, основным разработчиком международных стандартов и главным органом по сертификации в мире) перевесил. Была запущена процедура ускоренного согласования, и стандарт вскоре был принят.Основным достоинством ISO 17799 и родственных ему стандартов является их гибкость и универсальность. Описанный в нем набор лучших практик применим практически к любой организации, независимо от формы собственности, вида деятельности, размера и внешних условий. Он нейтрален в технологическом плане и всегда оставляет возможность выбора технологий. Когда возникают вопросы: «С чего начать?», «Как управлять ИБ?», «На соответствие каким критериям следует проводить аудит?» – этот стандарт поможет определить верное направление и не упустить из виду существенные моменты. Его также можно использовать как авторитетный источник и один из инструментов для «продажи» безопасности руководству организации, определения критериев и обоснования затрат на ИБ.

В стандартах серии ISO 27000 нашло отражение все, что требуется для управления информационными рисками. Речь идет прежде всего о выпущенном в 2008 году международном стандарте ISO/IEC 27005:2008, а также о его предшественнике – британском стандарте BS 7799-3:2006, увидевшим свет в 2006 году. Эти стандарты во многих вещах взаимно перекликаются, а в некоторых вопросах дополняют друг друга. Они служат фундаментом для излагаемой в настоящей книге методологии управления рисками и широко цитируются при последующем изложении материала.



Заслуживает также упоминания американский стандарт в области управления рисками NIST 800-30, который, в свою очередь, опирается на ISO Guide 73, ISO 16085, AS/NZS 4360. Основные положения этого стандарта были учтены при разработке ISO 27005.

Вопреки ожиданиям, ISO 27005 вовсе не является международной версией BS 7799-3, в отличие от своих предшественников ISO 27001 и ISO 27002, которые, как известно, являются международными версиями британских стандартов BS 7799-2 и BS 7799-1 соответственно. ISO 27005 пришел на смену международным стандартам ISO 13335-3 и ISO 13335-4, действие которых теперь отменено. Это свидетельствует о позитивном процессе замещения уже слегка устаревшей серии стандартов ИТ безопасности ISO 13335 относительно новой серией стандартов в области управления информационной безопасностью – ISO 27000. В результате данного процесса стандартов становится меньше, а их качество заметно улучшается.

Сопоставляя стандарты BS 7799-3 и ISO 27005, мы обнаруживаем, что они определяют все наиболее важные моменты, связанные с рисками, сходным образом. Это касается процессной модели, элементов управления рисками, подходов к анализу рисков и способам их обработки, а также вопросов коммуникации рисков. Оба стандарта содержат в виде приложений примеры типовых угроз, уязвимостей и требований безопасности.

BS 7799-3 и ISO 27005 определяют:

- *основные элементы процесса управления рисками;*
- *процессную модель;*
- *общий подход к управлению рисками;*
- *процессы анализа и оценивания рисков;*
- *способы качественного определения величины рисков;*
- *способы обработки рисков;*
- *процесс коммуникации рисков;*
- *примеры рисков, угроз, уязвимостей, активов, ущербов, требований законодательства и нормативной базы.*

Однако разные источники разработки обусловили и ряд различий между британским и международным стандартами управления рисками. ISO 27005 более подробно описывает критерии и подходы к оценке рисков, контекст управления рисками, область и границы оценки, а также ограничения, влияющие на уменьшение риска. В то же время BS 7799-3 более тесно связан с ISO 27001 и непосредственным образом отображает процессы управления рисками на процессы жизненного цикла СУИБ. Он также определяет требования к эксперту по оценке рисков и риск-менеджеру и включает в себя рекомендации по выбору инструментария для оценки рисков. BS 7799-3 также содержит примеры законодательных и нормативных требований применительно к США и странам Европы.

Различия стандартов управления рисками информационной безопасности:

ISO 27005

- *заменяет ISO 13335-3 и ISO 13335-4;*

- *определяет основные критерии для оценки рисков:*

- *область действия и границы;*
- *подходы к оценке рисков;*
- *ограничения, влияющие на уменьшение риска.*

BS 7799-3

- *отображает процессы управления рисками на модель жизненного цикла СУИБ согласно ISO 27001;*
- *определяет требования к эксперту по оценке рисков и к риск-менеджеру;*
- *содержит примеры соответствия требованиям законодательства и нормативной базы;*
- *содержит рекомендации по выбору инструментов для управления рисками.*

Подробная сравнительная таблица стандартов ISO 27001, ISO 27005 и BS 7799-3 приведена в Приложении № 1. Сведения о лицензионных русских переводах этих стандартов приведены в Приложении № 12.