СРАВНЕНИЕ ISO/IEC 27001:2005 И ISO/IEC 27001:2013

[1]Райкова Н.О., [1]Шахалов И.Ю.

[1] Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет информационных технологий, радиотехники и электроники» (МИРЭА), Москва, Россия (119454 Россия, г. Москва, проспект Вернадского, 78), e-mail: dtghmflysq@gmail.com

В данной статье производится сравнение новой и старой версии стандарта ISO/IEC 27001 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования». Детально рассматриваются изменения на уровне концепций и структуры стандарта. В заключении делается вывод о преимуществе изменений требований по сертификации системы менеджмента информационной безопасности.

Ключевые слова: система менеджмента информационной безопасности, СМИБ, сертификация, ISO/IEC 27001, международные стандарты.

COMPARISON OF ISO / IEC 27001: 2005 AND ISO / IEC 27001: 2013

[1]Raykova N.O., [1]Shahalov I.Y.

[1]Federal State Educational Institution of Higher Education «Moscow State University of Information Technologies, Radio Engineering and Electronics»(MIREA),Moscow, Russia (119454 Russia, Moscow, Vernadskogo avenu, 78), e-mail: dtghmflysq@gmail.com

This article compares the old and new version of ISO / IEC 27001 "Information technology. Methods of protection. Information security management system. Requirements. "Considered in detail the changes in the concepts and structure of the standard. In conclusion, the conclusion about the advantage of changes in requirements for certification of information security management system.

Keywords: Information Security Management System, ISMS certification, ISO / IEC 27001 international standards.

В конце прошлого года был принят новый международный стандарт - ISO/IEC 27001:2013 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования» [15]. Пересмотр стандарта готовился ещё с 2010 года, основываясь на следующих предпосылках:

- был разработан ряд вспомогательных стандартов серии ISO/IEC 27000;
- были обновлены стандарты, с которыми гармонизирован ISO/IEC 27001:2005;
- ISO/IEC 27001:2005 имеет ряд недостатков, например,избыточные требования, расплывчатость понятий ответственности руководства и так далее [10, 11, 13, 14].

В тоже время в нашей стране действует национальный стандарт ГОСТ ИСО/МЭК 27001:2006 «Информационные технологии. Методы защиты. Системы менеджмента защиты информации [1]. Требования», который копирует устаревший стандарт ISO/IEC 27001:2005, то есть существенно отличается выше названного как в плане учета современных угроз информационной безопасности, так и в плане этапов управления информационной безопасностью [4, 5]. Это создает предпосылки снижения уровня информационной безопасности в российских организациях в свете новых угроз информационной безопасности. Сравнению указанных стандартов посвящена данная статья.

1. Положения ISO/IEC 27001

Все изменения стандарта ISO/IEC 27001 можно разделить на несколько основных частей:

- обновленные концепции;
- изменения структуры стандарта;
- изменения в перечне механизмов контроля.

2. Обновленные концепции

При анализе концепции мы рассмотрим ее основные разделы: процессы, задачи информационной безопасности, заинтересованные стороны, обработку рисков, документации и др.

2.1. Процессы. В более ранней редакции стандарт следует модели PDCA [3]. В редакции 2013 года стандарт требует от процессной модели использования постоянного улучшения, но не настаивает на использовании определенной процессной модели. Для организаций с существующей СМИБ изменение требований насчёт модели PDCA является незначительным – цикл Деминга остается действующим. Так же подобные организации столкнутся с минимальными проблемами при желании построить процесс постоянного улучшения в других частях компании. Однако, организациям, которые внедряются новую СМИБ по стандарту ISO/IEC 27001:2013, должны определить лучший для своего бизнеса непрерывный процесс улучшения [4].

2.2. Задачи информационной безопасности (ИБ). Ранее требования о формулировании задач и планировании их выполнения содержались по разным разделам стандарта. В обновленном стандарте для них выделен отдельный раздел, называемый "Мониторинг, измерение, анализ и оценка". Данный раздел будет полезен и крайне необходим высшему руководству для оценки текущей ситуации и планирования дальнейших действий.

2.3. Руководство и управление. В стандарте появился раздел «Лидерство», в котором прописано то, как руководству компании следует показывать приверженность СМИБ. В прошлой версии стандарта, в разделе «Ответственность руководства» было уделено мало внимания этому вопросу. Хотя поддержка и приверженность руководства – основа для внедрения СМИБ.

2.4. Заинтересованные стороны. Обновленный стандарт учитывает интересы всех сторон, взаимодействующих с организацией (акционеров, регуляторов, клиентов, партнеров) и позволяет определить отдельные требования для каждого из них.

2.5. Обработка риска. Существует значительная разница между двумя подходами обработки риска. Для того, чтобы сделать переход к подходу, предусмотренному ISO 27001:2013, необходимо существенно изменить способ мышления. Принятие практики, описанной в ISO 31000, поможет сгладить переход к новому подходу [8, 12]. Наиболее важные изменения следующие:

– в преддверии оценки риска организация может определить и реализовать основополагающие контроли, базирующиеся на деловых, нормативных и договорных требованиях;

– оценка риска не основывается на активах;

– обработка риска и принятие остаточного риска осуществляется владельцем информации.

2.6. Контроли (средства управления).Многие контроли из версии стандарта 2005 года сохранены в новой, но не все контроли действуют для старых целей управления в новом стандарте. Вначале выбираются контроли для управления информационными рисками, а затем пересмотреть как выбранные контроли покрывают цели управления. Стоит отметить, что контроли выбираются, прежде чем обратиться к Приложению А, что позволяет организации выбрать из любого ресурса контроли, которые лучше всего подойдут для их процессов до заполнения остающихся пробелов с контролями Приложения А [11].

2.7. Несоответствия и корректирующие меры. Хотя превентивные меры и остались в Приложении А, но в явном виде более не упоминаются и не используются. Новый стандарт сосредотачивает внимание на существующих несоответствиях и корректирующих мерах, позволяющих их исправить.

2.8. Документация. Этоимеет незначительное влияние на внедренные СМИБ, особенно если организацияуже используетсистему менеджмента качества(СМК), таких как ISO/IEC 9001.Основное отличиемеждуизданиямив 2005 и2013в том, чтодокументы и

записине являются теперь обособленными, таким образом,процедурыбезопасности отвечают одинаковым требованиям [2].

2.9. Оценка эффективности. В то время как издание стандарта 2005 года требует от организации определить их собственные методы и практику для измерения эффективности СМИБ, новое издание приводит четкое руководство и указания [6, 9].

2.10. Сертификация. Так как сертификация по версии стандарта 2013 ещё не началась, у организаций есть выбор: начать изменять существующую СМИБ под требования нового издания стандарта или подождать с изменениями. Сертификация по ISO/IEC 27001:2005 производится в обычном порядке и будет действовать предположительно ещё три года.

2.11. Совместимость с другими стандартами. Касательно ISO/IEC 27001:2013 интеграция с другими стандартами систем менеджмента предполагается по обновленным версиям стандартов. Так как многие стандарты ISO перетерпели значительные изменения, совместимость со старыми версиями может быть затруднена [7].

2.12. Поддержка. В структуре выделен раздел Поддержка, в которомсделан акцент на предоставление ресурсов, наличию компетенций, повышение осведомленности и управление коммуникациями. Аналога управления коммуникациями ранее не было.

3. Изменения структуры стандарта

Структура стандарта, приведена в соответствие со стандартом ISO 22301:2012 "Требования к системам управления непрерывностью бизнеса" [14].

Описание структуры стандарта 2005 г. включает в себя 5 пунктов, которые относятся непосредственно к СМИБ, исходя из управленческой точки зрения. В 2013 г. включает себя 7 таких пунктов, которые необязательны к выполнению впорядке их перечисления. В обновленном стандарте выделяются следующие разделы, которых не было в предыдущей версии стандарта: «Лидерство», «Планирование», «Поддержка», «Эксплуатация» и «Измерение результативности». Несмотря на значительно измененную структуру стандарта, стандарт не перетерпел принципиальных изменений: требования были перенесены из одних разделов старой редакции в другие разделы новой, а также, были удалены дублирующийся требования. Стоит отметить, что обновленный стандарт имеет более удобную структуру.

4. Изменения в перечне механизмов контроля

Структура разделов Приложения А и соответствующего ему стандарта ISO/IEC 27002:2013 также претерпела некоторые изменения:

- изменен порядок разделов;
- раздел "Управление коммуникациями и операциями" в обновленной версии стандарта разделен на два самостоятельных раздела: "Безопасность операций" и "Безопасность коммуникаций";
- выделены два новых раздела: "Криптография" и "Взаимодействие с поставщиками".

Требования данных разделов ранее были распределены по другим разделам приложения и стандарта.

В Приложения А стандарта значительно уменьшилось количество мер обеспечения безопасности с 133 мер в старой версии стандарта по 114 меры в обновленной версии ISO/IEC 27001. Большинство мер не изменились, однако многие из них были перенесены в другие разделы приложения, которых теперь 14 (в ISO/IEC 27001:2005 11 разделов). Перенесенные и удаленные меры можно подробно посмотреть на сайте BSI.

Выводы

В целом стандарт ISO/IEC 27001 и вспомогательный ISO/IEC 27002 перетерпели изменения к лучшему:

1. Стандарт ISO/IEC 27001 гармонизирован с современными стандартами, выпущенными Международной организацией по стандартизации;

2. Появились нововведения в соответствии со стандартом ISO 22301:2012 «Социальная безопасность. Системы менеджмента непрерывного бизнеса. Требования» (структура и содержание текстовой части стандарта);
3. Обновленный стандарт конкретизирует способы по эффективному взаимодействию топ-менеджменту и лиц, ответственных за информационную безопасность, а также способствует большему вовлечению в процессы управления СМИБ руководства;
4. Произведена оптимизация требований и перечня механизмов контролей, с помощью выделения новых разделов, удалений лишних контролей, добавления недостающих контролей;
5. Изменения требований ISO/IEC 27001 направленны на либерализацию и послабление, что обеспечивает организации большую гибкость в выборе методик и защитных мер.

Список литературы

1. Акулов О.А., Баданин Д.Н., Жук Е.И., Медведев Н.В., Квасов П.М., Троицкий И.И. Основы информационной безопасности: Учеб. пособие. М.:Изд-во МГТУ им. Н.Э. Баумана, 2008. 161 с.
2. Барабанов А.В. Стандартизация процесса разработки безопасных программных средств // Вопросы кибербезопасности. 2013. № 1(1). С.37-41.
3. Воропаева В.Я., Щербов И.Л., Хаустова Е.Д. Управление информационной безопасностью информационно-телекоммуникационных систем на базе модели «Plan-Do-Check-Act» // Наукові праці Донецького національного технічного університету. Серія: "Обчислювальнатехнікатаавтоматизація". 2013. № 2 (25). С. 104-110.
4. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2 (3). С. 66-73.
5. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С.67-73.
6. Лившиц И.И. Оценка систем менеджмента информационной безопасности // Менеджмент качества. 2013. № 1. С. 22-34.
7. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С.28-35.
8. Марков А.С., Цирлов В.Л.. Управление рисками - нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. №8. С. 63-67.
9. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под. ред. В.А.Матвеева. М.: НИИ РиЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.
10. Новое в ISO 27001. BSI. 2014. URL: www.bsigroup.com/ru-RU/About-BSI/media-centre/BSI-CIS-News/news-2013/News-iso-27001/#.U8QmHaCGg3F (Дата обращения: 01.08.2014)
11. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4-14.
12. Шрайнер Ю.С., Безруков А.А., Азарьева В.В. Исследование подходов к менеджменту риска на основе стандартизации // Известия СПбГЭТУ "ЛЭТИ". 2014. Т. 4. С. 93-99.
13. Матвеев В.А., Цирлов В.Л. Состояние и перспективы развития индустрии информационной безопасности Российской Федерации в 2014 г. // Вопросы кибербезопасности. 2013. № 1(1). С.61-64.