

УДК 621.322

## **Новейшие требования к системам менеджмента информационной безопасности**

***Райкова Н.О., студент***

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,  
кафедра «Информационная безопасность»*

*Научный руководитель: Шахалов И.Ю., доцент  
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,  
кафедра «Информационная безопасность»*

[v.a.matveev@bmstu.ru](mailto:v.a.matveev@bmstu.ru)

### **Введение**

В конце 2013 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/IEC 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.** Это имеет незначительное влияние на внедренные СМИБ, особенно если организация уже использует систему менеджмента качества (СМК), таких как ISO/IEC 9001. Основное отличие между изданиями в 2005 и 2013 в том, что документы и записи не являются теперь обособленными, таким образом, процедуры безопасности 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 котором сделан акцент на предоставление ресурсов, наличие компетенций, повышение осведомленности и управление коммуникациями. Аналога управления коммуникациями ранее не было (см. табл.1).

Таблица 1

Ключевые изменения стандарта ISO/IEC 27001

| ISO/IEC 27001:2005                                                                                                                                                                                                                                                                                                                                                                                               | ISO/IEC 27001:2013                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Процесс</b>                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| В стандарте однозначно прописано использование PDCA модели                                                                                                                                                                                                                                                                                                                                                       | Стандарт не определяет какую-либо конкретную модель процесса. Но устанавливает требование по использованию непрерывного процесса с постоянным улучшением                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Руководство и управление</b>                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Руководство организации играет значительную роль. Но взаимодействие руководства в СМИБ не разъяснено.                                                                                                                                                                                                                                                                                                            | Выделяются две роли: менеджер и топ-менеджер. Делается разделение между юридическим руководством организации и менеджером, ответственным за управление СМИБ.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Оценка риска</b>                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <ol style="list-style-type: none"> <li>1. Риск - сочетание вероятности события и последствий его возникновения;</li> <li>2. Риски идентифицируются в соответствии с активами;</li> <li>3. Владелец активов определяет как обрабатывать риск, принимая остаточный;</li> <li>4. Контроли берутся из Приложения А, которые не являются исчерпывающими;</li> <li>5. Используется понятие владелец актива.</li> </ol> | <ol style="list-style-type: none"> <li>1. Риск – эффект неопределенности целей, который может быть положительным или негативным;</li> <li>2. Процессы планирования оценки риска и его обработки приведены в соответствие со стандартом ISO 31000;</li> <li>3. Базовые контроли, основанные на деловых, нормативных и договорных обязательствах могут быть определены и реализованы до проведения оценки риска;</li> <li>4. Организация определяет риски для информации организации – оценка не должна производиться на основе активов;</li> <li>5. Владелец риска определяет как</li> </ol> |

|                                                                                                                                                                                                                             |                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                             | <p>обрабатывать риск, принимая остаточный;</p> <p>6. Контроли могут выбираться из любого ресурса и набора элементов управления;</p> <p>7. Выбранные контроли сопоставляются с Приложением А.</p> |
| <b>Контроли</b>                                                                                                                                                                                                             |                                                                                                                                                                                                  |
| Приложение А содержит 133 контроля и 11 категорий. Контроли из других источников используются для устранения пробелов, которые не покрыты контролями из Приложения А.                                                       | Приложение А содержит 114 контроля и 14 категорий. Прежде чем ссылаться на Приложение А, организацией определяются контроли (из любого ресурса).                                                 |
| <b>Документация</b>                                                                                                                                                                                                         |                                                                                                                                                                                                  |
| Стандарт признает две формы: документы и записи. Документы включают в себя политики, процедуры, диаграммы процессов и т.д. Записи отслеживают завершённую работу, расписание аудитов и т.д.                                 | Стандарт не делает различий между документами и записями. Они подлежат одинаковым требованиям контроля.                                                                                          |
| <b>Оценка эффективности</b>                                                                                                                                                                                                 |                                                                                                                                                                                                  |
| Существует требование необходимости определить способы измерения эффективности контролей и их оценивания. Организация должна идентифицировать свои измерения и режим мониторинга в целях доказательства эффективности СМИБ. | Стандарт требует процесс измерения эффективности СМИБ, его процессов и контролей. Стандарт так же устанавливает требования к процессу измерения и режима мониторинга.                            |
| <b>Сертификация</b>                                                                                                                                                                                                         |                                                                                                                                                                                                  |
| СМИБ может быть сертифицированы любой аккредитованной организацией по сертификации.                                                                                                                                         | Ещё нет аккредитованной программы сертификации.                                                                                                                                                  |
| <b>Совместимость с другими стандартами</b>                                                                                                                                                                                  |                                                                                                                                                                                                  |
| Стандарт предназначен для интеграции с другими стандартами ISO / IEC, хотя многие из них (14001 и 9001, например) с тех пор были обновлены.                                                                                 | Стандарт предназначен для лучшей интеграции с другими стандартами по системам управления. Термины и определения ISO / IEC стандартизированы по 27000 серии ISO.                                  |

### 3. Изменения структуры стандарта

Структура стандарта, как видно из таблицы 2, приведена в соответствие со стандартом ISO 22301:2012 "Требования к системам управления непрерывностью бизнеса" [14].

## Структура стандарта ISO/IEC 27001

| ISO/IEC 27001:2005                                | ISO/IEC 27001:2013           |
|---------------------------------------------------|------------------------------|
| 0 Введение                                        | 0 Введение                   |
| 1 Область применения                              | 1 Область применения         |
| 2 Нормативные ссылки                              | 2 Нормативные ссылки         |
| 3 Требования и определения                        | 3 Требования и определения   |
| 4 Система Менеджмента Информационной Безопасности | 4 Установление контекста     |
| 5 Обязательства руководства                       | 5 Лидерство                  |
| 6 Внутренние аудиты                               | 6 Планирование               |
| 7 Анализ системы менеджмента                      | 7 Поддержка                  |
| 8 Улучшение СМИБ                                  | 8 Эксплуатация               |
|                                                   | 9 Измерение результативности |
|                                                   | 10 Улучшение                 |

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 не обязательны к выполнению в порядке 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 дублирующие 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 (табл. 3);
- 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.

Таблица 3

Структура Приложения А стандарта ISO/IEC 27001

| ISO/IEC 27001:2005                                                | ISO/IEC 27001:2013                                                |
|-------------------------------------------------------------------|-------------------------------------------------------------------|
| A.5 Политика в области безопасности                               | A.5 Политика в области безопасности                               |
| A.6 Организация системы безопасности                              | A.6 Организация системы безопасности                              |
| A.7 Классификация активов и управление                            | A.7 Безопасность и персонал                                       |
| A.8 Безопасность и персонал                                       | A.8 Классификация активов и управление                            |
| A.9 Физическая и внешняя безопасность                             | A.9 Управление доступом к системе                                 |
| A.10 Управление коммуникациями и операциями                       | A.10 Криптография                                                 |
| A.11 Управление доступом к системе                                | A.11 Физическая и внешняя безопасность                            |
| A.12 Приобретение, разработка, обслуживание информационных систем | A.12 Безопасность операций                                        |
| A.13 Менеджмент инцидентов                                        | A.13 Безопасность коммуникаций                                    |
| A.14 Обеспечение непрерывности бизнеса                            | A.14 Приобретение, разработка, обслуживание информационных систем |
| A.15 Соответствие законодательству                                | A.15 Взаимоотношения с поставщиками                               |
|                                                                   | A.16 Менеджмент инцидентов                                        |
|                                                                   | A.17 Обеспечение непрерывности бизнеса                            |
|                                                                   | A.18 Соответствие законодательству                                |

В Приложении 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 меры можно подробно посмотреть на сайте BSI. Удаленные механизмы контроля и новые механизмы контроля приведены в таблице 4.

Таблица 4

Перечень удаленных и новых механизмов контроля

| Перечень удаленных механизмов контроля             | Перечень новых механизмов контроля                                 |
|----------------------------------------------------|--------------------------------------------------------------------|
| 6.1.1 Обязанности руководства по защите информации | A.6.1.5 Информационная безопасность в области управления проектами |

|                                                                                      |                                                                                   |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| 6.1.2 Координация защиты информации                                                  | A.12.6.2 Ограничение на установку программного обеспечения                        |
| 6.1.4 Процесс получения разрешения для средств, обрабатывающих информацию            | A.14.2.1 Политика безопасной разработки                                           |
| 6.2.1 Выявление рисков, связанных с внешними сторонами                               | A.14.2.5 Процедуры системы разработки                                             |
| 6.2.2 Решение вопросов безопасности при работе с клиентами                           | A.14.2.6 Среда безопасной разработки                                              |
| 10.7.4 Безопасность системы документации                                             | A.14.2.8 Тестирование безопасности системы                                        |
| 10.8.5 Системы деловой информации                                                    | A.15.1.1 Политика информационной безопасности в отношениях с поставщиками         |
| 11.4.2 Аутентификация пользователя для внешних соединений                            | A.15.1.3 Последовательность поставок информационных и коммуникационных технологий |
| 11.4.3 Идентификация оборудования в сетях                                            | A.16.1.4 Оценка и решение событий информационной безопасности                     |
| 11.4.4 Защита удаленного диагностирования и конфигурации портов                      | A.16.1.5 Реакция на инциденты информационной безопасности                         |
| 11.4.6 Управление подключением к сети                                                | A.17.2.1 Доступность средств информационной обработки                             |
| 11.4.7 Управление сетевой маршрутизацией                                             |                                                                                   |
| 12.2.1 Валидация вводимых данных                                                     |                                                                                   |
| 12.2.2 Управление внутренней обработки                                               |                                                                                   |
| 12.2.3 Целостность сообщений                                                         |                                                                                   |
| 12.2.4 Валидация выходных данных                                                     |                                                                                   |
| 11.6.2 Изоляция уязвимых систем                                                      |                                                                                   |
| 12.5.4 Утечка информации                                                             |                                                                                   |
| 15.1.5 Предотвращение неправильного использования средств, обрабатывающих информацию |                                                                                   |
| 15.3.2 Защита средств аудита информационных систем                                   |                                                                                   |

### **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 направлены 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: учебное 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: "Обчислювальна техніка та автоматизація". 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. Басараб М.А., Булатов В.В., Булдакова Т.И. и др. / под. ред. Матвеева В.А. Математические основы информационной безопасности. М.: НИИ РИЛТ МГТУ им. Н.Э.Баумана, 2013. 244 с.
10. Новое в ISO 27001. BSI. 2014. Режим доступа: [www.bsigroup.com/ru-RU/About-BSI/media-centre/BSI-CIS-News/news-2013/News-iso-27001/#.U8QmHaCGg3F](http://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.
14. Kosutic D. ISO 27001/ISO 22301 documents, presentation decks and implementation guidelines [ISO 27001 / ISO 22301 документы, презентация и рекомендации по реализации]. Режим доступа: <http://blog.iso27001standard.com/2013/09/30/list-of-mandatory-documents-required-by-iso-27001-2013-revision/> (дата обращения: 01.08.2014).
15. Information Security & ISO 27001 [Информационная безопасность и ИСО 27001]. IT Governance Ltd. 2014. Режим доступа: <http://www.itgovernance.co.uk/green-papers.aspx#.VXMp5FJA6o9> (дата обращения: 01.08.2014).