МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПЕРЕХОД НА ISO 27001:2013

***Дорофеев Александр Владимирович**, CISSP, CISM, CISA*

Публикация завершает блок наших публикаций по менеджменту информационной безопасности в серии статей для специалистов по информационной безопасности, готовящихся сдать экзамен на получение статуса CISSP (Certified Information Systems Security Professional). В статье рассмотрена новая редакция стандарта ISO 27001:2013.

***Ключевые слова**: сертификация специалистов, CISSP, ISO 27001:2013, система менеджмента информационной безопасности (СМИБ), управление рисками информационной безопасности.*

INFORMATION SECURITY MANAGEMENT: TRANSITION TO ISO 27001:2013

***Alexander Dorofeev**, CISSP, CISM, CISA*

Publication finalizes the series of our publications devoted to management of information security as part of preparation for the CISSP (Certified Information Systems Security Professional) exam. New edition of ISO 27001:2013 is examined in the article.

***Keywords**: expert certification, CISSP, ISO 27001:2013, information security management system (ISMS), information security risk management.*

В предыдущих двух статьях нашей колонки по подготовке к сдаче экзамена CISSP мы рассмотрели основные понятия из области менеджмента информационной безопасности и подробно разобрали важнейшую составляющую системы менеджмента информационной безопасности (СМИБ) как управление рисками. Как вы помните, стандартом для построения системы менеджмента информационной безопасности де-факто является ISO 27001, последняя версия которого вышла совсем недавно: осенью 2013 года. Новый стандарт отличается от предыдущей редакции и по содержанию, и по форме. Сейчас многие эксперты выступают с докладами и статьями на тему изменений и, к сожалению, в своем анализе новой редакции стандарта допускают досадные ошибки, которые могут направить интересующихся специалистов в неверном направлении. Так как специалисту, стремящемуся получить статус CISSP необходимо глубоко разбираться в вопросах управления ИБ, то мы решили посвятить отдельную статью изменениям в стандарте на СМИБ.

Начнем с того, что разберемся, почему вообще стали менять стандарт ISO 27001:2005, ведь он был довольно качественно проработан. С 80-х годов прошлого века появилось множество стандартов по системам менеджмента (менеджмент качества, энергетический менеджмент, менеджмент безопасности питания и др.). Современные организации зачастую стоят перед необходимостью внедрения и поддержания в эффективном состоянии интегрированной системы менеджмента в соответствии с разными стандартами. Так как стандарты разрабатывались в разное время и специалистами из различных отраслей, накопилось множество расхождений, затрудняющих создание единой интегрированной системы менеджмента. Для унификации данных стандартов было принято Приложение SL (Annex SL) первой части директив ISO, в соответствии с которой должны разрабатываться новые стандарты менеджмента и обновляться существующие.

Стремление привести стандарт ISO 27001 к принятому единому формату для стандартов на системы менеджмента и послужило одной из основных причин ряда изменений.

Стоит отметить, что версии стандартов ГОСТ Р ИСО/МЭК 27001—2006 и ГОСТ Р ИСО/МЭК 27002—2012, принятые в России, являются переводами предыдущих версий стандартов (в редакции 2005 года).

К основным группам изменений в стандарте ISO 27001 можно отнести:

- изменение структуры;
- обобщение положений;
- появление новых понятий;
- уточнение роли руководства, важности коммуникаций;
- изменения в приложении А.

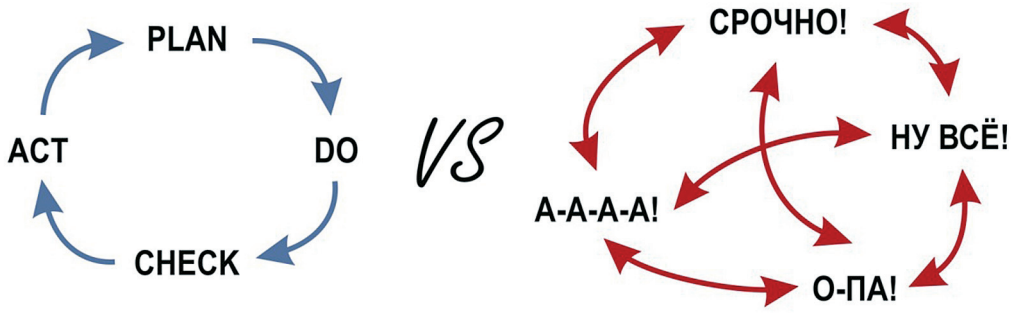

Рис. 1. *Модель Деминга и распространенная практика управления*

Изменение структуры

В подготовленном BSI (British Standards Institution) документе «Переход от ISO 27001:2005 к ISO 27001:2013»[1],приведено подробное сопоставление разделов предыдущей версии стандарта и версии 2013 года (структура изменена в соответствии с требованиями упомянутого выше Приложения SL). Проведя беглый анализ сопоставления, можно сразу придти к выводу, что суть стандарта не изменилась.

Однако необходимо обратить внимание, на один важный момент, связанный со структурой новой редакции стандарта. Если в ISO 27001:2005 была представлена модель Деминга (PDCA или Plan-Do-Check-Act), то теперь ее в явном виде в стандарте нет, что дало почву для дискуссий на конференциях по информационной безопасности, так как ряд «экспертов» заявляют, что теперь отсутствует необходимость ей руководствоваться.

Если мы внимательно посмотрим на содержание ISO 27001:2013, то без труда увидим следующие разделы стандарта, расположенные последовательно друг за другом, отражающие последовательность цикла PDCA:

- Planning (Планирование);
- Operation (Функционирование);
- Performance evaluation (Оценка результативности);
- Improvement (Улучшение).

Таким образом, модель Деминга осталась в стандарте в самой его структуре и говорить о потере ее актуальности весьма преждевременно.

Стоит отметить, что данная модель отражает здравый смысл при управлении любой деятельностью: сначала думаем, что хотим сделать (Plan), затем делаем (Do), проверяем, что полученные результаты соответствуют ожиданиям (Check), вносим необходимые корректировки, улучшаем (Act). Согласитесь, что практика сначала что-то сделать, а потом подумать, является не самой эффективной, хотя и очень распространенной в нашей жизни.

Обобщение

Обобщение больше всего коснулось ядра СМИБ – процесса оценки рисков информационной безопасности. Если ранее в ISO 27001:2005 процесс был расписан довольно подробно и помимо прочего включал в себя такие шаги, как идентификация активов и их владельцев, а также уязвимостей, то в новой версии стандарта оставлены лишь основные этапы:

1. Определение критериев принятия рисков и критериев к процессу оценки рисков;
2. Идентификация рисков;
3. Анализ рисков (определение последствий, вероятности, определение уровней рисков)
4. Сопоставление оценок рисков с установленными критериями. Определение приоритетов по их обработке.

Теперь требования к процессу оценки рисков в ISO 27001:2013 соответствуют международному стандарту ISO 31000.

В явном виде из текста исчезло слово «asset» (актив), что также позволило «экспертам» говорить о том, что стандарт больше не требует идентификации активов для оценки рисков. Многие согласятся, что оценить риски не зная, какому активу и что именно угрожает, полностью дискредитирует саму идею риск-менеджмента. Неужели разработчики стандарта пошли на такой рискованный шаг?

Давайте посмотрим на текст стандарта в раздел 6.1.2 (c): «apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for *information* within the scope of the information security management system». Данную фразу можно перевести следующим образом: «применить

1 http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

процесс оценки рисков информационной безопасности, связанных с потерей конфиденциальности, целостности и доступности для информации, попадающей в границы СМИБ». Теперь нам потребуется разобраться, что подразумевается под термином информация (information) в данном контексте. В этом вопросе нам поможет стандарт ISO27000:2014, в котором дано определение терминов, используемых в линейке стандартов ISO 27000[2] . Кстати, мало кто знает, но данный стандарт можно бесплатно скачать с сайта ISO (см. сноску). В разделе 3.2.2 Information стандарта ISO27000:2014 можно почерпнуть, что информация является активом (как раз, используется знакомое нам слово asset), а также что данное понятие не ограничивается только данными в различной форме, но и включает в себя технологии передачи этих данных. Таким образом, на наш взгляд, корректным переводом понятия information в разделе 6.1.2 будет «информация и средства ее обработки». Соответственно, идентификация активов как была предусмотрена в ISO 27001:2005, так и осталась в ISO 27001:2013.

Еще к одному обобщению можно отнести тот факт, что из новой версии стандарта исчезла фраза с требованием не допустить того, чтобы аудиторы проверяли собственную работу. Если опять таки внимательно посмотреть на текст ISO 27001:2013, то можно увидеть раздел 9.2.e, в котором зафиксировано требование выбора аудиторов и проведения аудита таким образом, чтобы была обеспечена объективность и беспристрастность процесса аудита. О какой объективности может быть речь, если кто-либо будет проверять собственную работу? Авторы стандарта не убрали требование, а всего лишь убрали избыточный текст.

Новая редакция стандарта богата новыми терминами и концепциями, основные из которых стоит внимательно рассмотреть:

Контекст организации

Важнейшим нововведением в ISO 27001:2013 является появление термина «контекст организации» (context). Профессионалы в области управления информационной безопасностью хорошо помнят, как совсем недавно компании успешно проходили сертификацию СМИБ по требованиям ISO 27001, заявляя довольно узкие границы (scope):один-два не очень критичных процесса, которые можно было защитить, внедрив систему минимальными усилиями. Теперь требования к обоснованию границ СМИБ (scope) стали жестче, так как они в соответствии с ISO 27001:2013 определяются исходя из контекста организации, т.е. из различных внешних и внутренних аспектов (issues), которые могут повлиять на то, как организация управляет рисками информационной безопасности. Организация должна четко определить заинтересованные стороны (interested parties) и их требования. Соответственно, на границы СМИБ напрямую влияют требования законодательства, регулирующих органов, контрактные обязательства и т.п. Конечно, границы СМИБ, как и в прошлой версии, стандарта должны быть оформлены в виде отдельного документа, включая описание контекста организации. Старый подход больше не сработает.

Владелец риска

Новая версия стандарта требует, чтобы для выявленных рисков информационной безопасности были идентифицированы владельцы рисков. В соответствии со словарем[3] по риск-менеджменту, опубликованным ISO владельцем риска является человек или организация, которая отвечает за управление риском и обладает необходимыми для этого полномочиями. Нам нельзя просто «повесить» все риски на менеджера по информационной безопасности и не дать ему никаких полномочий по их управлению, многие риски будут закреплены за руководителями соответствующих бизнес-подразделений.

Задачи информационной безопасности

В стандарте появился термин Information Security Objective, который очень легко неправильно перевести, так как английское слово «objective» имеет несколько значений, среди которых «цель» и «задача». В контексте менеджмента информационной безопасности подразумевается, на наш взгляд, значение именно «задачи», так как задачи в соответствии с требованиями стандарта должны определяться для соответствующих функций и уровней организации. ISO 27001:2013 требует четкого планирования задач, в ходе которого фиксируется:

- что должно быть сделано;
- какие ресурсы потребуются;
- кто отвечает;
- сроки;
- как будут оцениваться результаты выполнения задач.

Данное планирование оформляется документально.

Наверное, ни для кого не будет секретом, что в некоторых организациях системы менеджмен-

2 http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

3 ISO Guide 73 2009. Risk Management - Vocabulary.

та (качества, ИБ и другие) существуют только на бумаге – ответственные специалисты для целей сертификации генерируют бумагу в виде всевозможных процедур и отчетов, которой «кормят» аудиторов, выписывающих красивые сертификаты. Четкий формат управления задачами в рамках СМИБ, появившийся в новой редакции стандарта, на наш взгляд задачу подобной имитации деятельности усложнит на порядок.

Роль руководства

Любая система менеджмента должна быть необходима, прежде всего, топ-менеджменту компании, так как выстроенные процессы позволяют снизить зависимость от конкретных специалистов, сделать организацию лучше управляемой, обеспечить осмысленное планирование и т.п. Тем не менее, можно столкнуться с ситуацией, когда руководство организации больше заинтересовано в сертификате на систему менеджмента, а не в самой системе менеджмента. Мы не будем сейчас отвлекаться на тему хорошо это или плохо, так как однозначного ответа на данный вопрос нет. Так, например, хорошо выстроенная модель управления организации делает организацию отчасти уязвимой захвату извне. Обратим лишь внимание на то, что если к системе менеджмента нет должного отношения со стороны первого лица организации, то она работать не будет. По всей видимости, разработчики новой версии стандарта ISOISO 27001 этот момент хорошо прочувствовали, и теперь стандарт содержит подробное описание того, что должно предпринимать руководство, чтобы обеспечить результативное функционирование СМИБ. В частности, руководство должно обеспечивать:

- соответствие задач информационной безопасности стратегическому направлению движения организации;
- интеграцию ИБ в бизнес-процессы организации;
- обеспечение СМИБ необходимыми ресурсами;
- контроль достижения СМИБ запланированных целей;
- внедрение в организации политики информационной безопасности;
- необходимое распределение ответственности;
- и многое другое.

Коммуникации в области ИБ

Наверное, многим знакомы организации, в которых службы информационной безопасности возглавляются бывшими сотрудниками спецслужб, которые любят работать в стиле проведения «секретной спецоперации». В таких компаниях, как правило, сотрудники ничего не знают про информационную безопасность и только иногда догадываются, что «большой брат» следит за ними: прослушиваются телефонные переговоры, просматривается электронная почта и т.п. С таким подходом эффективную СМИБ внедрить очень сложно, так как важно, чтобы каждый сотрудник организации хорошо понимал, что такое ИБ, и что от него требуется в разных ситуациях, а для этого, как известно хорошо подходят методы пропаганды, которые сейчас по-научному называются методами коммуникаций. В новой версии стандарта появился отдельный подраздел 7.4, посвященный данному вопросу. ISO 27001:2013 требует планирования внешних и внутренних коммуникаций по вопросам информационной безопасности: мы должны определить что, кто, кому и когда будет коммуницировать в организации и за ее пределами относительно соблюдения правил ИБ.

Изменения в приложении А

Не избежал изменений и перечень контролей, приведенный в приложении А. Как мы с вами помним, по предыдущим статьям [2,3] контроль представляет собой способ минимизации риска информационной безопасности. По сути ISO 27001 представляет собой описание механизма выбора контролей на основе оценки рисков и содержит в приложении А перечень контролей, представляющий некий минимум, на основе которого и строится система.

В новой версии стандарта имеется 114 контролей, разделенных на 14 следующих доменов:

- политики информационной безопасности;
- организационные вопросы ИБ;
- вопросы ИБ, связанные с персоналом;
- управление активами;
- управление доступом;
- криптография;
- физическая безопасность и защита от угроз окружающей среды;
- операционные вопросы ИБ;
- безопасность коммуникаций;
- приемка, разработка и поддержка информационных систем;
- взаимодействие с поставщиками;
- Управление инцидентами ИБ;
- Вопросы ИБ при обеспечении непрерывности бизнеса;
- Выполнение требований.

В предыдущей редакции контроли были раз-

биты на одиннадцать доменов, 20 контролей были удалены, 11 добавлено, в некоторых улучшены формулировки.

Стоит напомнить, что вместе с ISO 27001 был обновлен и сопутствующий ISO27002. Подробное сопоставление приложений А нового и предыдущего стандарта приведены в соответствующей публикации[4] BSI.

Заключение

Рассмотренные нами основные изменения ISO 27001 и определяют те области СМИБ в организации, которые требуют основного внимания при переходе на новую версию стандарта. С одной стороны ISO 27001 стал жестче и конкретнее (требования к руководству, задачи ИБ) с другой стороны из него исчезли некоторые детали (нюансы оценки рисков, внутреннего аудита), которые безусловно сохраняются на практике. Организациям, которые серьезно подошли к вопросам внедрения СМИБ, не составит труда привести систему в соответствие новым требованиям. Тем же, кто руководствовался стратегией внедрения «малой кровью» придется очень серьезно постараться. В свою очередь, специалистам, готовящимся сдать экзамен CISSP настоятельно советуем ознакомиться с последней версией стандарта ISO 27001:2013, чтобы быть в курсе последних тенденций в области построения систем менеджмента информационной безопасности.

Литература

1) Дорофеев А.В. Статус CISSP: как получить и не потерять? //Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2) Дорофеев А.В. Марков А.С. Менеджмент ИБ: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С.67-73.
3) Дорофеев А.В. Менеджмент ИБ: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С.66-73.
4) Марков А.С., Цирлов В.Л. Управление рисками – нормативный вакуум информационной безопасности// Открытые системы. СУБД. 2007. № С. 63-67.
5) Douglas J.Landoll. The security risk assessment handbook, Second Edition. – CRC Press, 2011. 474 p.

References

1) Dorofeyev A.V. Status CISSP: kak poluchit i ne poteryat? Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 65-68.
2) Dorofeyev A.V., Markov A.S. Menedzhment informacionnoj bezopasnosti: osnovnye koncepcii // Voprosy kiberbezopasnosti, 2014, No 1(2). pp. 67-73
3) Dorofeyev A.V. Menedzhment informacionnoj bezopasnosti: upravlenie riskami // Voprosy kiberbezopasnosti, 2014, No 2(3). pp 66-73
4) Markov A.S., Tsirlov V.L. Upravlenie riskami – normativnyy vacuum informatsionnoy bezopasnosti, Otkrytyye sistemy. SUBD, 2007, No 8, pp.63-67.
5) Douglas J.Landoll. The security risk assessment handbook, Second Edition. – CRC Press, 2011. 474 p.

4 http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO 27001-mapping-guide-UK-EN.pdf