УДК 681.237

АНАЛИЗ СТАНДАРТОВ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

А.К.Севастьянов
Институт кибернетики имени В.М. Глушкова НАН Украины
e-mail: aks@i.com.ua

1. Введение. Стандарт на систему менеджмента качеством (СМК) по ISO 9001:2008 – это минимальные требования на рынке. Особое место занимают системы информационной безопасностью. ISO/IEC 27000 - эта совокупность стандартов, которая должна решать проблемы информационной безопасностью и содействовать процессу принятия решений высшим руководством организации и мотивировать высшее руководство к освоению новых подходов к построению и развитию современной системы информационной безопасностью [1-8]. На Рис. 1. представлена модель PDCA, применительно к процессам СМИБ (СМЗИ), а в таблице 1 [4,6] приведены - сокращенное название, обозначение серии и название, обозначения стандартов. ISO/IEC 27001, как и стандарт ISO 9001, применяет широко известный цикл PDCA (см. Рисунок 1) для постоянного улучшения и адаптации системы менеджмента: **Plan** — разработайте СМИБ, которую затем установите, например, посредством утверждения и рассылки процедур и планов. **Do** — внедрите СМИБ и обеспечьте ее функционирование, например, посредством распределения полномочий и четкой постановки целей и задач. **Check** — регулярно проводите мониторинг и анализ СМИБ, например, через плановые и внеплановые аудиты, через анализы со стороны руководства. **Act** — при необходимости адаптируйте и улучшайте СМИБ, например, через корректирующие и предупреждающие действия.

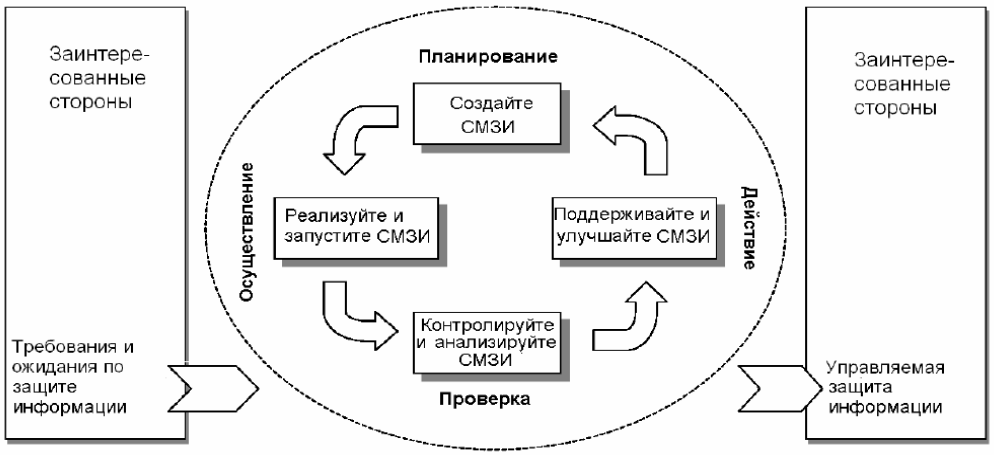

Рис. 1. Модель PDCA, применительно к процессам СМИБ (СМЗИ)

Табл.1.

Сокращенное название	Обозначение серии и название	Обозначения стандартов
СМИБ	Серия ISO/IEC 27000 Системы менеджмента информационной безопасностью	ISO/IEC 27001:2005; ISO/IEC 27000:2009 (словарь); ISO/IEC 27002:2005; ISO/IEC 27003:2010; ISO/IEC 27004:2009; ISO/IEC 27005:2008 (риски); ISO/IEC 27006:2007 (аккредитац.); ISO/IEC 27007 (аудит.); ISO/IEC 27008; ISO/IEC 27010; ISO/IEC 27011:2008 (телеком.); ISO/IEC 27013; ISO/IEC 27014; ISO/IEC 27015; ISO/IEC 27031; ISO/IEC 27032; ISO/IEC 27033:2009; ISO/IEC 27034; ISO/IEC 27035; ISO/IEC 27036; ISO/IEC 27037;

Сокращенное название	Обозначение серии и название	Обозначения стандартов
		ISO/IEC 27038; ISO 27799:2008; ISO/IEC Guide 83:2012;
CMP	Серия ISO 31000 Менеджмент рисками	ONR 49001:2010; ONR 49000:2010; ONR 49001:2010; ONR 49002-1:2010; ONR 49002-2:2010; ONR 49003:2010; ONORM S 2300; ONORM S 2310 (австрийские стандарты); ISO 31000:2009; ISO 31004 (проект); ISO/IEC 31010:2009; BS 31100:2008; AS/NZS 4360:2004; HB 436:2004 (австралийское руководство); BS 5760-7:1991 (IEC 61025:1990); CSA Q 850:1997; JIS Q 2001:2001; ISO/IEC Guide 73: 2002;

2. Предполагаемые изменения. На Рис. 2. представлены возможные изменения содержания основного стандарта [7].

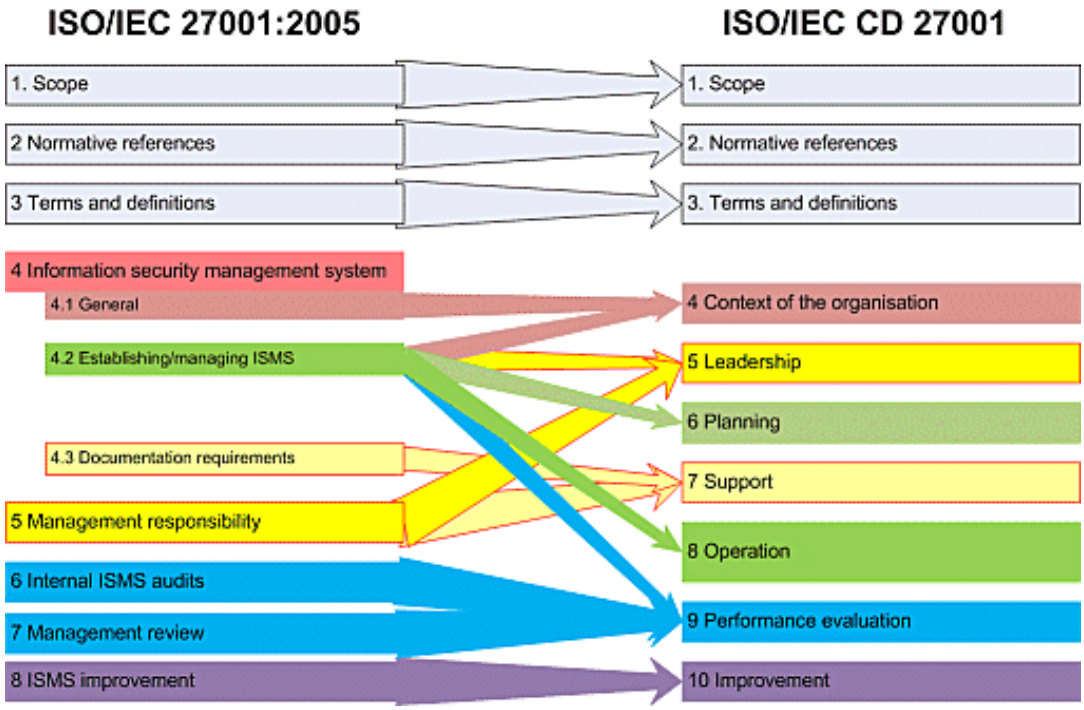

Рис. 2. Предполагаемые изменения в новой версии стандарта

3. Области применения. ISO/IEC 27001 применим для любых видов деятельности, для любых типов и размеров организаций. Наибольшей популярностью стандарт ISO/IEC 27001 пользуется в следующих отраслях [5]: (1) телекоммуникация; (2) банковская деятельность и финансы; (3) страхование; (4) информационные технологии; (5) здравоохранение; (6) государственные услуги; (7) коммунальные услуги; (8) розничная торговля; (9) образование; (10) службы по чрезвычайным ситуациям; (11) силовые структуры; (12) производство; (13) транспортные компании и (14) поставщики услуг.

Применение стандарта ISO/IEC 27001 позволяет получить следующий ряд преимуществ [5]: (1) демонстрация посредством сертификации на соответствие ISO/IEC 27001 того, что системы и процессы организации в достаточной степени обеспечивают безопасное обращение и пересылку информации; (2) обеспечение информационной безопасности для клиентов, что жизненно важно для ведения организацией успешного бизнеса, в частности,, для получения преимуществ в тендерах и конкурсах; (3) передача на аутсорсинг процессов без ущерба для информационной безопасности как организации, так м ее клиентов; (4) снижение рисков организации, связанных с вопросами информационной безопасности, что в целом способствует устойчивому развитию.

Организации, прошедшие сертификацию по ISO/IEC 27001, прежде всего, видят пользу от этой сертификации в расширении портфеля сертификатов, что непосредственно влияет на имидж организации как преуспевающей и современной.

Кроме стандартов ISO/IEC 27001 и ISO/IEC 27002 в серию стандартов по информационной безопасности уже вошли следующие стандарты [2,5]:

ISO/IEC 27000:2009 «Информационным» технологии — Методы обеспечения безопасности — Системы менеджмента информационной безопасности — Общие сведения и словарь». Данный стандарт содержит общие сведения и терминологию по информационной безопасности, также как стандарт ISO 9000 предоставляет общие положения и словарь для системы менеджмента качества.

ISO/IEC 27003:2010 «Информационные технологии - Методы обеспечения безопасности — Руководящие указания по внедрению системы менеджмента информационной безопасности». Данный стандарт содержит руководящие указания для внедрения СМИБ на основе стандартов серии ISO/IEC 27000.

ISO/IEC 27004:2009 «Информационные технологии - Методы обеспечения безопасности — Менеджмент информационной безопасности — Измерения» содержит рекомендации по показателям и измерениям в области информационной безопасности.

ISO/IEC 27005:2008 «Информационные технологии - Методы обеспечения безопасности — Управление рисками информационной безопасности». Как было отмечено выше, менеджмент рисками является ядром стандартов серии ИСО 27000, и поэтому был опубликован дополнительный стандарт касательно управления рисками безопасности.

ISO/IEC 27006:2007 «Информационные технологии — Обеспечение безопасности - Требования к органам, осуществляющим аудит и сертификацию систем информационной безопасности». Данный стандарт необходим аккредитованным органам для предоставления услуг по аудиту и сертификации систем информационной безопасности.

Следует также опираться на стандарт ISO/IEC 17021:2006 «Оценка соответствия - Общие требования для органов, выполняющих аудит и сертификацию систем менеджмента» и ISO 19011:2002 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента».

4. Сертификация. Как и при применении ISO 9001, применяя ISO/IEC 27001, организация может разработать, внедрить и сертифицировать свою систему менеджмента на соответствие международного стандарта. На конец 2007 года согласно официальным данным ISO во всем мире по ISO/IEC 27001 сертифицировались 7732 организации [2,5] из 70 стран. Абсолютный лидер — Япония, где сертификацию по ISO/IEC 63 % от общего объема сертификации! В этой стране бизнес всегда уделял первостепенное внимание информации и знаниям, считая их основой успеха в международной конкуренции. Общая динамика роста сертификатов по ISO/IEC 27001 свидетельствует о том, что данный стандарт является настоящим бестселлером. Несомненно, кроме жизненной необходимости в защите информации, этому способствует все большее преобладание в деятельности нематериальных активов над материальными, т.е. информационной над физической составляющей продукции. Текущий финансовый кризис еще раз подтвердил значимость информации в наше время и тяжесть последствий от ошибок в области информационной безопасности.

5. Выводы. Системы менеджмента являются важным инструментом достижения целей организации. Особое значение занимает информационная поддержка при развитии системы менеджмента. Обобщение и систематизация новых знаний содействует обоснованному и эффективному принятию решений высшим руководством при развитии системы менеджмента в организации. Представленная обширная информация по новым стандартам, говорит о необходимости проведения постоянного мониторинга в этой

области для своевременного принятия решений для усиления конкурентных преимуществ организации. Для сокращения времени внедрения новых подходов и новых видов менеджмента целесообразно пользоваться международными и национальными стандартами развитых стран. Это позволит организациям Украины повысить их конкурентоспособность. Многообразие стандартов в области систем менеджмента делает актуальной задачу разработки стандарта для выбора стандартов или методологического указания для принятия решений при выборе стандартов для конкретных организаций. В Украине уже несколько организаций внедрили или внедряют систему менеджмента информационной безопасностью на основе международного стандарта ISO/IEC 27001. Это объясняется не столько популярностью стандартов ISO, сколько насущной потребностью организаций в защите их нематериальных активов.

Литература

1. Севастьянов А.К., Международные стандарты систем менеджмента для решения проблем безопасности и устойчивого развития (International standards for management systems for solving the security and sustainable development) // Стандартизація, сертифікація, якість. – Харьков. – 2012. - №4. – С.41-49.

2. Севастьянов А.К., Анализ стандартов для систем менеджмента в телекоммуникациях. – Шоста міжнародна науково-технічна конференція та Четверта студентська науково-технічна конференція «Проблеми телекомунікацій» присвячені Дню науки і Всесвітньому дню телекомунікацій, 24-27 квітня 2012 року, Матеріали конференції. - Київ: НТУУ «КПІ», 2012. - С.138-140.

3. Севастьянов А.К., Информационная поддержка для принятия решений в современных системах менеджмента. – Четвертая дистанционная научно-практическая конференция с международным участием «Системы поддержки принятия решений. Теория и практика. СППР 2008». – Киев: Академия технологических наук Украины, Институт проблем математических машин и систем НАН Украины. – 2008. – С.178-183.

4. Севастьянов А. К., Развитие системы информационной поддержки для принятия решений в современных системах менеджмента. – Седьмая дистанционная научно-практическая конференция с международным участием «Системы поддержки принятия решений. Теория и практика. СППР 2011». – Киев: Академия технологических наук Украины, Институт проблем математических машин и систем НАН Украины. – 2011. – С.134-137.

5. Есмуханов Е. Информационная безопасность на основе международного стандарта ISO/IEC 27001. – УСПЕХ- SUCCESS. – Сентябрь-Октябрь 2010. – С.20-24.

6. Севастьянов А.К., Менеджмент рисками – новое задание руководству. – Восьмая дистанционная научно-практическая конференция с международным участием «Системы поддержки принятия решений. Теория и практика. СППР 2012». – Киев: Академия технологических наук Украины, Институт проблем математических машин и систем НАН Украины. – 2012. – С.111-114.

7. DRAFT ISO GUIDE 83, Secretariat: TMB, Voting begins on Voting terminates on 2011-05-06, 2011-09-06. - High level structure and identical text for management system standards and common core management system terms and definitions. - Structure à niveau élevé et texte identique pour les normes de système de management et termes et définitions principaux communs de système de management.

8. Севастьянов А.К., Мотивация в системах менеджмента: высказывания успешных людей. – Киев: Освита Украины. – 2011. – 212 с.