# УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЙ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА В КОНТЕКСТЕ СТАНДАРТА ISO 27001:2013

**А.В. Суханов, доктор технических наук, доцент.**
**ЗАО «ЭВРИКА».**
**А.С. Смирнов, доктор технических наук, доцент.**
**Национальный центр управления в кризисных ситуациях МЧС России.**
**С.Б. Хитов.**
**Санкт-Петербургский университет ГПС МЧС России**

Рассмотрены основные изменения международного стандарта ISO/IEC 27001, являющегося основой построения систем менеджмента информационной безопасности в организациях, внесенные версией ISO/IEC 27001:2013 по сравнению с редакцией ISO/IEC 27001:2005.

*Ключевые слова:* ISO/IEC 27001:2013, информационная безопасность, система менеджмента информационной безопасностью

# MANAGEMENT OF DEFENSE INDUSTRY'S INFORMATION SECURITY IN THE CONTEXT OF THE ISO/IEC 27001:2013 STANDARD

A.V. Sukhanov. ZAO «EURICA».
A.S. Smirnov. National crisis management center of EMERCOM of Russia.
S.B. Khitov. Saint-Petersburg university of State fire service of EMERCOM of Russia

The main clauses of the new international standard for information security management – ISO/IEC 27001:2013, in comparing with ISO/IEC 27001:2005 are considered in the article. This standard is basis of creation an information security management system for any organization.

*Keywords:* ISO/IEC 27001:2013, information security, information security management system

С обострением международной обстановки, ростом глобального информационного противоборства, активностью террористических группировок особую остроту приобретает реализация угроз информационной безопасности (ИБ) посредством проведения компьютерных атак на государственные информационные системы и ресурсы [1]. При этом к одним из наиболее вероятных «мишеней» или объектов подобного рода атак можно в полной мере отнести предприятия и организации оборонно-промышленного комплекса (ОПК) страны, перед которыми, в данных условиях, приобретает особое значение обеспечение ИБ. В настоящее время данная проблема решается применением комплекса общих правовых, организационно-технических и экономических методов [1].

## Построение систем менеджмента ИБ как основы эффективного управления ИБ

Популярный в настоящее время процессный подход к управлению организациями, представляющий собой методологию, идентифицирующую процессы в организации таким образом, чтобы были понятны, видимы и измеримы их взаимосвязь, а итоговая совокупность процессов понималась как единая система целей деятельности организации, предполагает выделение в структуре системы обеспечения ИБ [2]:

– системы управления ИБ;

– инфраструктуры защиты информации, непосредственно реализующей процессы ИБ.

Кроме того, обеспечение ИБ путем реализации на предприятиях ОПК принципа управления рисками, профилактики и предупреждения крупномасштабных факторов, рисков и угроз ведет к необходимости создания в рамках общей системы обеспечения ИБ системы менеджмента ИБ (СМИБ), являющейся частью общей системы менеджмента организации, основанной на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению ИБ и отвечающей современным стандартам и требованиям [3, 4].

Требования, предъявляемые к СМИБ, даны в линейке международных стандартов ISO/IEC 27000, в которой определен понятийный аппарат, терминология, методология построения и деятельности СМИБ. Стандарты серии 27000 являются наиболее известными и широко используемыми при управлении ИБ.

Основными (обязательными) документами серии являются стандарты ISO/IEC 27001 и ISO/IEC 27006. Первый определяет назначение СМИБ, ее цели, понятия, а также требования, предъявляемые к системе, второй – требования к организациям, осуществляющим аудит и сертификацию СМИБ.

Согласно ISO/IEC 27001 целью СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон. Создание и эксплуатация СМИБ требует применения такого же подхода, как и любая другая система менеджмента. Обязательные процедуры стандарта управления качеством ISO 9001 требуются и стандартом ISO/IEC 27001.

Стандарт ISO/IEC 27001, являющийся совместной разработкой международной организации по стандартизации (ISO, в отечественной аббревиатуре ИСО) и международной электротехнической комиссии (IEC, МЭК), вышел в свет в конце 2005 г. Год спустя на основе аутентичного перевода ISO/IEC 27001 в нашей стране был принят в качестве государственного стандарта ГОСТ Р ИСО/МЭК 27001–2006 [5], который лег в основу построения отечественных СМИБ.

Стандартом ISO/IEC 27001:2005, а также ГОСТ Р ИСО/МЭК 27001–2006 на основе процессного подхода применительно к менеджменту ИБ реализовывалась циклическая модель управления качеством PDCA (Plan-Do-Check-Act–Планирование-Осуществление-Проверка-Действие), представленная на рисунке.

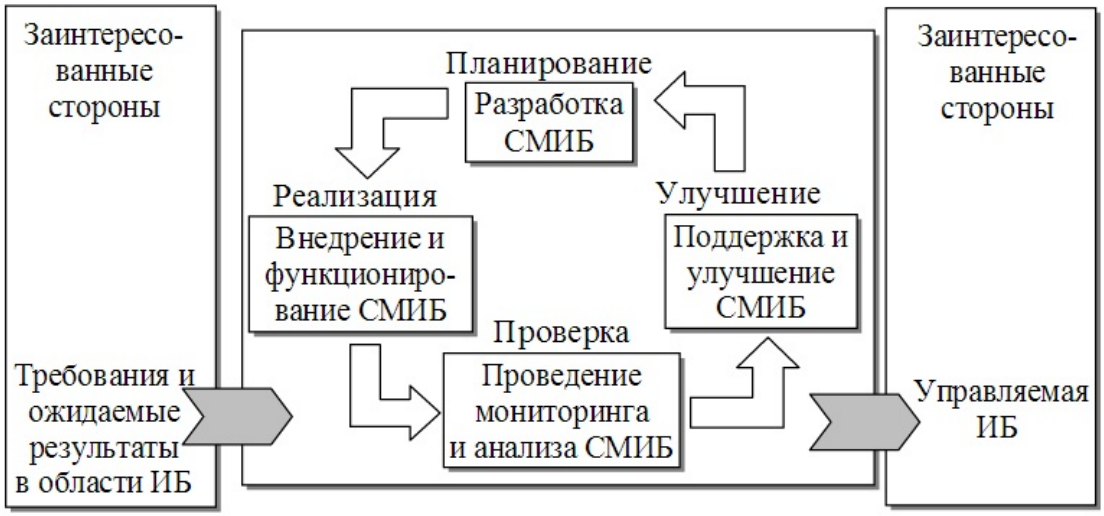


Рис. **Цикл PDCA для СМИБ в соответствии с ISO/IEC 27001:2005**

Из рисунка видно, что СМИБ, используя в качестве входных данных требования ИБ и ожидания заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения ИБ, которые соответствуют этим требованиям и ожидаемым результатам [5].

В соответствии с моделью PDCA построение СМИБ начинается с этапа «Планирование», в котором проводится оценка состояния ИБ с учетом угроз и уязвимостей, связанных с информационными активами организации. Проводится выбор необходимых мер и средств контроля и управления ИБ, определяются цели их применения, а также цели применения мер и средств контроля и управления для обработки рисков. Разрабатываемые и реализуемые политики и процедуры должны охватывать следующие ключевые процессы:

– управление активами;
– управление рисками;
– управление мерами контроля;
– управление персоналом;
– управление документацией и записями СМИБ;
– управление инцидентами;
– управление эффективностью системы;
– управление изменениями (пересмотр и модернизация системы);
– управление непрерывностью бизнеса и восстановление после прерываний.

На этапе «Внедрение» проводится внедрение выбранных мер и средств управления и контроля для достижения целей ИБ, определяется способ измерения результативности СМИБ, проводятся измерения мер и средств управления и контроля.

На этапе «Проверка» осуществляется анализ результативности СМИБ, производится пересмотр оценки рисков, с учетом результативности СМИБ, производится подтверждение эффективности СМИБ с учетом результатов предыдущих аудитов, определяются направления совершенствования СМИБ, формируются исходные данные для принятия решения по усовершенствованию СМИБ, развитию способов оценивания результативности мер и средств управления и контроля.

На последнем этапе «Действие» проводится реализация принятых решений по улучшению СМИБ.

## Переход к ISO/IEC 27001:2013

Международный «старший брат» ISO/IEC 27001 в 2013 г. претерпел изменения, коснувшиеся как формы, так и содержания по сравнению с версией 2005 г. Одной из причин подобного обновления можно отметить появление Приложения SL (AnnexSL) первой части директив ИСО, унифицирующего многочисленные стандарты на системы менеджмента и определяющего для них новую единую высокоуровневую структуру [6].

Согласно данному документу специальные требования любого из стандартов должны быть отображены в следующих разделах:

1. Область действия.
2. Нормативные ссылки.
3. Термины и определения.
4. Контекст организации.
5. Руководство.
6. Планирование.
7. Поддержка.
8 Производственная деятельность.
9. Оценка эффективности.
10. Улучшение.

С целью облегчения понимания специалистами новшеств ISO/IEC 27001:2013 в сравнении ISO/IEC 27001:2005 при совершенствовании как разработанных ранее, так

и вновь внедряемых СМИБ, британским национальным органом по стандартизации (BritishStandardsInstitution (BSI)) было выпущено «Руководство по переходу от ISO/IEC 27001:2005 к ISO/IEC 27001:2013» [7], на основании которого авторами предлагается провести анализ основных изменений.

Приводя ISO/IEC 27001 в соответствие Приложению SL, изменения затронули структуру документа, количество и состав разделов и подразделов, в документе появился ряд новых терминов и определений, уточнена роль руководства, повышена роль коммуникаций, изменено Приложение А.

Первое, что может сразу броситься в глаза при рассмотрении ISO/IEC 27001:2013 – отсутствие явного отражения представленной в версии 2005 г. модели PDCA. Однако при внимательном анализе структуры нового документа можно увидеть, что цикл PDCA в нем все же прослеживается – в структуре выделяются разделы, расположенные последовательно один за другим:

– Планирование (Planning);
– Производственная деятельность (Operation);
– Оценка эффективности (Performance evaluation);
– Улучшение (Improvement).

Рассматривая разделы ISO/IEC 27001:2013, можно отметить, что значительным изменениям подвергся процесс, связанный с оценкой рисков ИБ. Взаимное соответствие пунктов стандартов, связанных с идентификацией и оценкой рисков представлено в табл. 1.

Таблица 1. **Соответствие пунктов ISO/IEC 27001:2013 и ISO/IEC 27001:2005 в части определения требований к идентификации и оценке рисков ИБ**

| ISO/IEC 27001:2013 | ISO/IEC 27001:20005 |
|---|---|
| 6.1.1. Действия в отношении рисков и возможностей, направленные на:<br>a) подтверждение способности СМИБ к достижению ожидаемых от нее результатов<br>b) предотвращение или сокращение нежелательных эффектов<br>c) достижение непрерывного совершенствования | 8.3. Предупреждающие действия |
| 6.1.2. Идентификация рисков<br>6.1.2. (c) Обязательное закрепление за каждым риском его владельца | 4.2.1. (c) Определение подхода к оценке риска<br>1. Методологии оценки риска<br>2. Разработка критериев и уровней риска<br>4.2.1. (d) Идентификация рисков<br>1. Идентификация активов и определение их владельцев<br>2. Идентификация угроз в отношении активов<br>3. Идентификация уязвимостей<br>4. Идентификация последствий<br>4.2.1. (e) Анализ и оценка рисков |
| 6.1.3. Обработка рисков ИБ | 4.2.1. (f) Определение и оценка вариантов обработки рисков<br>4.2.1. (g) Выбор целей и мер управления для обработки рисков<br>4.2.1. (h) Утверждение руководством остаточных рисков<br>4.2.1. (i) Разрешение руководства на внедрение и эксплуатацию СМИБ<br>4.2.1. (j) Разработка «Положение о применимости»<br>4.2.2. Разработка плана обработки рисков |
| 6.2. Цели информационной безопасности и планирование их достижения | 5.1. (b) Обеспечение руководством разработки целей и планов СМИБ |

Теперь, стандартом, который в данном аспекте стал соответствовать стандарту ISO 31000 «Менеджмент риска. Принципы и Руководство», предусматриваются следующие этапы оценки рисков:

– определение критериев принятия рисков и критериев к процессу их оценки;

– идентификация рисков;

– анализ рисков (определение последствий, вероятности, определение уровней рисков);

– сопоставление оценок рисков с установленными критериями. Определение приоритетов по их обработке.

Кроме этого, существенной особенностью ISO/IEC 27001:2013 является явное отсутствие такого основополагающего понятия менеджмента рисков, как «актив» (asset), а также подраздела, связанного с идентификацией активов и их владельцев. Вместо «актива» стандарт оперирует понятием «информация, попадающая в пределы СМИБ» (information within the scope of the information security management system).

Тем не менее рассматривая понятие «информация» с точки зрения международного стандарта ISO27000:2014, определяющего соответствующие отраслевые термины, можно отметить, что «информация является тем активом, который жизненно важен для эффективной хозяйственной деятельности организации и потому подлежит защите должным образом» [8].

Кроме того, документ относит к важнейшим активам организаций связанные с информацией процессы, системы и сети.

Таким образом, понятие «информация, попадающая в пределы СМИБ», по мнению авторов, можно рассматривать как «информационные активы, попадающие в пределы СМИБ».

Среди новых терминов и определений, появившихся в ISO/IEC 27001:2013, отметим такие как: контекст организации (context of the organization), владелец риска (risk owner) и цели информационной безопасности (information security objectives).

Контекст организации предполагает определение пределов СМИБ, исходя из различных внешних и внутренних аспектов, влияющих на управление рисками ИБ. Так, на пределы СМИБ, создаваемой и внедряемой на предприятиях ОПК страны, прямо влияют требования российского законодательства, национальных регуляторов в области ИБ, договорных обязательств. Описание контекста организации должно входить в документально оформленные пределы СМИБ.

В соответствии с ISO/IEC 27001:2013 для определенных рисков ИБ необходимо идентифицировать владельцев риска – субъектов, отвечающих за управление риском с соответствующими полномочиями.

Термин «цели информационной безопасности» предполагает четкое определение соответствующих целей, а также планирование мероприятий по их достижению для функций и уровней организации.

При планировании, оформляемом документально, должны отражаться проводимые для достижения целей ИБ мероприятия, ответственные за их выполнение должностные лица, необходимые средства и ресурсы, сроки проведения, а также форма оценки результатов.

Повышая роль коммуникаций, ISO/IEC 27001:2013 требует планирования в организациях внешних и внутренних, связанных с вопросами обеспечения ИБ, коммуникаций.

Уточняются такие пункты, как мониторинг, измерение, анализ и оценка, а также внутренний аудит (табл. 2.)

Таблица 2. **Соответствие пунктов ISO/IEC 27001:2013 и ISO/IEC 27001:2005 в части определения требований к мониторингу, измерениям, анализу и оценке, а также к внутреннему аудиту**

| ISO/IEC 27001:2013 | ISO/IEC 27001:20005 |
|---|---|
| 9.1. Мониторинг, измерение, анализ и оценка | 4.2.2 (d) Определение способа измерения результативности выбранных мер управления или их групп и использование этих измерений для оценки результативности управления…<br>4.2.3 (b) Проведение регулярного анализа результативности СМИБ и анализа мер управления безопасностью…<br>4.2.3 (c) Измерение результативности мер управления для проверки соответствия требованиям ИБ |
| 9.2. Внутренний аудит | 4.2.3 (e) Проведение внутренних аудитов СМИБ через установленные периоды времени<br>6. Внутренние аудиты СМИБ |

Выполняя пункт 9.1, организация должна определить, когда и какое должностное лицо будет осуществлять мониторинг и измерения, кто будет проводить анализ и оценку результатов.

В части проведения внутреннего аудита ISO/IEC 27001:2013 устанавливается требование выбора аудиторов и проведения аудита с обеспечением объективности и беспристрастности процесса аудита.

Особое внимание в ISO/IEC 27001:2013 уделено роли руководства в обеспечении результативного функционирования СМИБ. В соответствии со стандартом руководство предприятия ОПК должно обеспечивать:

– соответствие целей ИБ стратегическому направлению развития организации;
– разработку и внедрение в организации политики ИБ;
– интеграцию процесса обеспечения ИБ в бизнес-процессы организации;
– обеспечение СМИБ необходимыми средствами и ресурсами;
– контроль достижения СМИБ поставленных целей;
– разграничение полномочий и ответственности;
– и ряд других мероприятий, направленных на эффективное управление ИБ.

Исключен пункт, требующий ежегодного пересмотра СМИБ со стороны руководства.

По сравнению с версией 2005 г., в новой версии изменился и перечень контролей, который приводится в «Приложении А». Теперь данное приложение содержит перечень целей и средств управления, которые совпадают с аналогичными целями и средствами управления стандарта ISO 27002, при пересмотре которого количество средств управления было сокращено со 133 до 114, а число доменов расширено от 11 до 14. К существующим доменам добавились такие домены как:

– криптография (A.10);
– безопасность коммуникаций (A.13);
– взаимодействие с поставщиками (A.15).

Таким образом, в ISO/IEC 27001:2013 представлены 114 контролей, делящихся на 14 доменов. Подробная таблица соответствия контролей версий ISO/IEC 27001:2013 и ISO/IEC 27001:2005 приводится в документе [7].

«Приложение B» стандарта ISO/IEC 27001:2013 представлено таблицей, в которой показано соответствие процедур СМИБ и этапов цикла PDCA принципам «Организации по экономическому сотрудничеству и развитию» (OECD).

В «Приложении C» определяется соответствие требований стандартов ISO 9001, 14001 и 27001.

Подводя итог, отметим, что с обновлением ISO/IEC 27001 подобной процедуре подвергся и «идущий рядом» стандарт ISO/IEC 27002. Рассмотренные выше основные изменения стандарта ISO/IEC 27001 требуют наиболее пристального внимания как при разработке и внедрении на предприятиях ОПК страны СМИБ по новому стандарту, так и при приведении в соответствие с ISO/IEC 27001:2013 существующих систем. При создании и актуализации документированной информации организация должна обеспечить соответствующие идентификацию и наименование, формат, анализ и официальное одобрение с точки зрения адекватности и пригодности.

**Литература**

1. Смирнова О.Г., Хитов С.Б. Правовые основы защиты информационных систем Российской Федерации от компьютерных атак // Право. Безопасность. Чрезвычайные ситуации. 2016. № 1 (30). С. 38–42.

2. Васильева И.Н. Управление информационной безопасностью: учеб. пособие. СПб.: Изд-во СПбГЭУ, 2014. 82 с.

3. Еременко С.П., Хитов С.Б., Можаев О.А. Анализ нормативно-правовой базы для задачи формирования модели и метода оценки результативности СМИБ в организациях МЧС России // Проблемы управления рисками в техносфере. 2015. № 4 (36). С. 101–107.

4. Еременко С.П., Хитов С.Б. Оценка результативности как важнейший аспект построения системы обеспечения информационной безопасности в системе распределенных ситуационных центров МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2016. № 2. С. 84–90.

5. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Госстандарт России. 2008. 31 с.

6. ISO/IECDirectives, Part 1ConsolidatedISOSupplement – Procedures specificto ISO. Seventhedition, 2016. URL: http://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/ISO_IEC_Directives_Part_1_and_Consolidated_ISO_Supplement_%2D_2016_%287th_edition%29_%2D_PDF.pdf?nodeid=17668772&vernum=-2 (дата обращения: 28.06.2016).

7. Transitionguide. MovingfromISO/IEC 27001:2005 toISO/IEC 27001:2013.BSIGROUP, UnitedKingdom. 16 p.

8. Международный стандарт ISO/IEC 27000. 3-е изд. URL: http://pqm-online.com/assets/files/lib/std/iso-mek-27000-2014.pdf (дата обращения: 28.06.2016).

**References**

1. Smirnova O.G., Khitov S.B. Pravovyeosnovyzacschityinformacionnyh system RossijskojFederaciiotkompjuternahatak [Legal bases of protection of information systems of the Russian Federation against computer attacks] // Law. Safety. Emergency situations. 2016. № 1 (30). p. 38–42 (In Russ.).

2. Vasiljeva I.N. Upravlenieinformacionnojbezopasnostju: Uchebnoeposobie [Management of information security: tutorial]. SPb.: SPbGEU, 2014. 82 p.

3. Eremenko S.P., Khitov S.B. Analiz normativno-pravovoj bazy dlya zadachi formirovanija modeli i metoda ocenki rezultativnosti SMIB v organizaciyah MCHS Rossii // Problemy upravlenija riskami v tehnosfere [Analysis legal norms for the task of construction of model and method of estimation of efficiency of ISMS in the organizations of Emercom of Russia] // Problems in the technosphere risk management. 2015. № 4 (36). p. 101–107 (In Russ.).

4. Eremenko S.P., Khitov S.B. Ocenka rezultativnosti kak vazhnejshij aspect postroenija sistemy obespechenija informacionnoj bezopasnosti v sisteme raspredelennyh situacionnyh centrov Mchs Rossii. [Productivity assessment as the most important aspect of creation of system of ensuring information security in system of the distributed situational centers of EMERCOM of Russia] // Vestnik S.-Peterb. un-ta GPS MCHS Rossii.2016. № 2. p. 84–90 (In Russ.).

5. GOST R ISO/MEK 27001–2006 «Informacionnayatehnologiya. Metody i sredstva obespecheniya bezopasnosti. Systemy menedzhmenta informacionnoj bezopasnosti. Trebovaniya» [National standard of Russia ISO/IEC 27001 – 2006 Information technology – Security techniques – Information security management systems – Requirements]. M.: Gosstandart Rossii. 2008. 31 p.

6. ISO/IEC Directives, Part 1Consolidated ISO Supplement – Procedures specific to ISO. Seventh edition, 2016. URL: http://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/ISO_IEC_Directives_Part_1_and_Consolidated_ISO_Supplement_%2D_2016_%287th_edition%29_%2D_PDF.pdf?nodeid=17668772&vernum=-2 (data obrascheniya: 28.06.2016).

7. Transition guide. Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013. BSIGROUP, UnitedKingdom. 16 p.

8. Mezhdunarodnyj standart ISO/IEC 27000, Tretie izdanie. [International standard ISO/IEC 27000, Third version] URL: http://pqm-online.com/assets/files/lib/std/iso-mek-27000-2014.pdf (data obrascheniya: 28.06.2016).