УДК 65.012 006

Т.Ю. Сячина

О СОВРЕМЕННЫХ МЕТОДАХ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

T.Y. Syachina

ABOUT ACTUAL TECHNIQUES OF INFORMATION SECURITY MANAGEMENT

Предлагаемая в статье классификация методов менеджмента информационной безопасности, позволяет реализовать требования основополагающих стандартов, поддерживать и улучшать системы менеджмента информационной безопасности (СМИБ) конкретной организации.

МЕТОДЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СМИБ.

The classification of techniques information security management in this publication will can to realize requires of main standards for organizations, to keep and improvement their system.

TECHNIQUES INFORMATION SECURITY MANAGEMENT, INFORMATION SECURITY MANAGEMENT SYSTEM, ISMS.

В связи с совершенствованием организациями систем менеджмента информационной безопасности (СМИБ) на основе международных стандартов начинает формироваться соответствующая практика, которая необходима для эффективной работы таких систем.

Существуют основополагающие и дополняющие стандарты для реализации требований в области информационной безопасности, самыми распространенными являются стандарты ISO серии 27000, которые предъявляют требования к системе менеджмента информационной безопасности [1] и содержат руководящие указания к построению, реализации и улучшению СМИБ [2,3,4]. Дополняющие стандарты содержат свод правил по выбору методов и руководящих принципов для реализации СМИБ, которые организация должна выбрать, исходя из специфики своей деятельности. Формирование системы методов менеджмента информационной безопасности позволит организациям реализовать требования основополагающих стандартов, поддерживать и улучшать систему.

Ключевые требования к информации включают в себя комплекс подходов для их выполнения – управление рисками, управление событиями информационной безопасности, их учет и исправление, минимизация возможных рисков, снижение ущерба негативных последствий, установление привилегированного доступа к информации, маркировка информации, ограничение физического доступа и его контроль и т.д. Важными составляющими достижения и оценки конфиденциальности, целостности и доступности информации является учет изменений, их оценка, классификация рисковых событий, изменчивость системы менеджмента ИБ вследствие внешних и внутренних факторов (внедрение новых элементов в СМИБ, вывод компонентов, оборудования, технологий, экономическая и законодательная ситуации и прочее). Систематизировать всю собранную информацию, оценить текущее состояние СМИБ и цели организации можно только с применением статистических методов, результатом использования которых будет более четкое и грамотное прогнозирование ожидаемых результатов процессов и управление

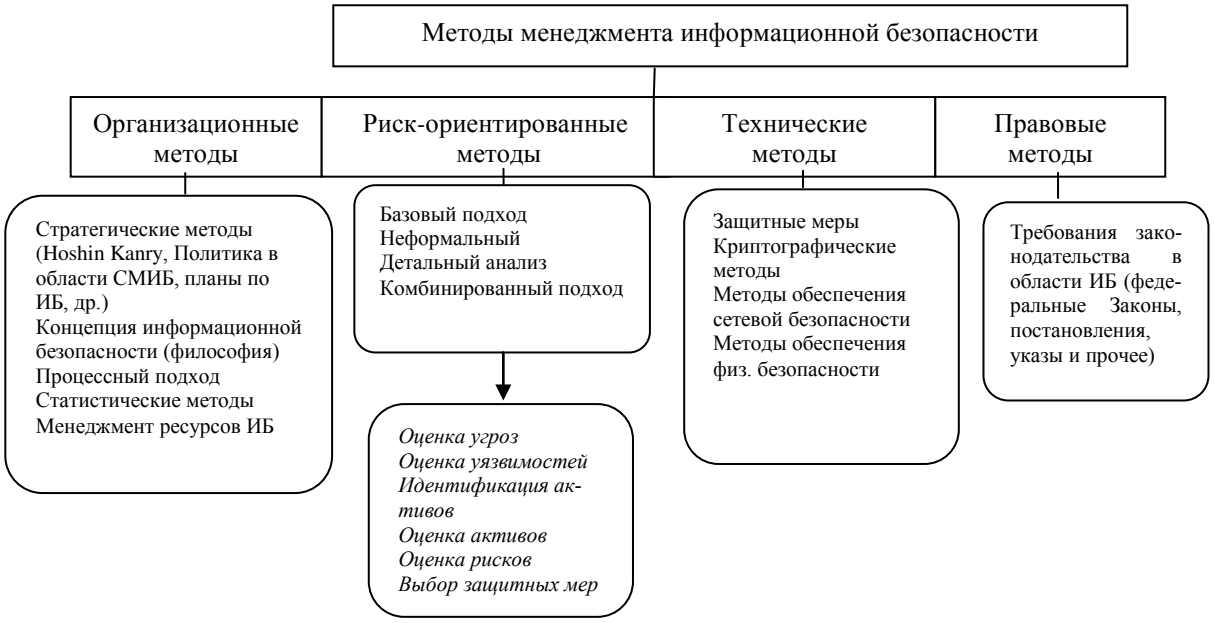

Рис. 1. Классификация методов менеджмента информационной безопасности

ими на основе фактов и данных.

Согласованность стандартов ISO/IEC 27001 и ISO 9001 позволяет сделать вывод об идентичности структуры требований к СМК и СМИБ [1, 5], принципов и методов, применяемых в данных системах. Методы менеджмента качества направлены на координацию деятельности по руководству и управлению организацией в области качества и могут быть разделены на три вида [6]: Организационные - развертывание политики, организация кружков качества, «точно во время»; Инженерные - QFD, FMEA, SPC, метод Тагути, семь сложных статистических методов; Простейшие методы – универсальные методы командного решения проблем, включая семь простых методов, метод «пять почему», алгоритмизация. Данная классификация направлена на группировку методов с позиции способов повышения эффективности производства. На рис. 1 приведена предлагаемая классификация методов в области менеджмента информационной безопасности с учетом приведённой классификации методов менеджмента качества и источников в области информационной безопасности [7,8], включающая в себя: организационные методы, риск-ориентированные методы, технические методы, правовые методы.

Организационные методы - это группа методов, включающая аспекты, которые основываются на принципе ответственности и приверженности руководства в области информационной безопасности. Применение методов включает анализ требований к информационной безопасности, разработку плана выполнения этих требований, управление и административный контроль над реализуемой системой информационной безопасности, определение целей и политики, разработка стратегии в области ИБ и управления рисками [9]. Риск-ориентированные методы – группа методов, направленных на координацию деятельности по управлению и контролю за организацией в отношении рисков. Методы содержат основные подходы к оценке рисков и способах управления ими с учетом направления деятельности организации и её организационной структуры [7,8]. Технические методы содержат различные практики по управлению информационной безопасностью (средства управления) для достижения целей управления в случае возникновения риска. Защитные меры позволяют обеспечить информационную безопасность, уменьшить уязвимости, ограничить воз-

действие инцидентов и облегчить восстановление активов. Технические методы являются инструментарием для осуществления организационных и риск-ориентированных методов, так как подразумевают комплекс действий, механизмов, которые направлены на защиту информационной безопасности техническими способами [2]. Правовые методы помогают поддерживать функционирование СМИБ на основе реализации правовых норм по информационной безопасности. Правовое направление основывается на государственной политике в области информационной безопасности, основных правилах и процедурах обязательной сертификации средств защиты информации и правилам аттестации объектов, правилах лицензирования и технической защиты конфиденциальной информации; формах ответственности за нарушение правовых и нормативных требований ИБ [10].

Особо важными для руководства организации в области СМИБ являются статистические методы. Стандарт ISO/IEC 27001 требует поддерживать и улучшать СМИБ посредством мониторинга и оценки функционирования системы. Для такого анализа необходимы записи и свидетельства мониторинга и измерений СМИБ, которые при помощи применения статистических методов станут основой для разработки корректирующих и предупреждающих действий для постоянного улучшения, и принятого на объективных результатах анализа. Статистические методы являются общим компонентом всех групп методов менеджмента информационной безопасности, они применяются при оценке риска, при тестировании защитных систем ИБ и программного обеспечения, при аттестации объектов, лицензировании и технической защите конфиденциальной информации.

Статистические методы в СМИБ ещё не получили широкого распространения, в отличие от применения в системах менеджмента качества. Использование данных методов позволяет специалистам принимать обоснованные управленческие решения, подкрепленные количественными данными.

СПИСОК ЛИТЕРАТУРЫ

1. ИСО/МЭК 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Изд-во стандартов, 2009 -49 с.

2. ИСО/МЭК 27000:2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общее представление и словарь». М.: Изд-во стандартов, 2012-25с.

3. ИСО/МЭК 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью». М.: Изд-во стандартов, 2007 -163с.

4. ИСО/МЭК 27003:2010 «Информационные технологии. Руководство по осуществлению системы менеджмента информационной безопасности». М.: Изд-во стандартов, 2010 – 68с.

5. ИСО 9001:2008. «Системы менеджмента качества. Требования». М.: Изд-во стандартов, 2008 – 27с.

6. **Балукова М.В.** «Петербургские тайны» качества - Методы менеджмента качества № 1, 2006, с. 57-58.

7. ГОСТ Р 53110-2008 «Система обеспечения информационной безопасности сети связи общего пользования. Общие положения». М.: Изд-во стандартов , 2009-23 с.

8. ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология - Методы и средства обеспечения безопасности – Часть 1: Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий». М.: Изд-во стандартов, 2007 -23 с.

9. **Андрианов В.В., Зефиров С.Л., Голованов В.Б., Голдуев Н.А.** Обеспечение информационной безопасности бизнеса- 2-е изд., перераб. и доп. - М.:ЦИПСиР: Альпина Паблишерз, 2011. - 373 с.

10. **Крат Ю.Г., Шрамкова И.Г.** Основы информационной безопасности : учеб. пособие /– Хабаровск : Изд-во ДВГУПС, 2008. –112 с.

REFERENCES

1. ISO/MEK 27001:2005 «Informatsionnye tekhnologii. Metody obespecheniia bezopasnosti. Sistemy menedzhmenta informatsionnoi bezopasnosti. Trebovaniia». M.: Izd-vo standartov, 2009 -49 s.

2. ISO/MEK 27000:2012 «Informatsionnye tekhnologii. Metody obespecheniia bezopasnosti.

Sistemy menedzhmenta informatsionnoi bezopasnosti. Obshchee predstavlenie i slovar'». M.: Izd-vo standartov, 2012-25s.

3. ISO/MEK 27002:2005 «Informatsionnye tekhnologii. Metody obespecheniia bezopasnosti. Prakticheskie pravila upravleniia informatsionnoi bezopasnost'iu». M.: Izd-vo standartov, 2007 -163s.

4. ISO/MEK 27003:2010 «Informatsionnye tekhnologii. Rukovodstvo po osushchestvleniiu sistemy menedzhmenta informatsionnoi bezopasnosti». M.: Izd-vo standartov, 2010 – 68s.

5. ISO 9001:2008. «Sistemy menedzhmenta kachestva. Trebovaniia». M.: Izd-vo standartov, 2008 – 27s.

6. **Balukova M.V. «**Peterburgskie tainy» kachestva - Metody menedzhmenta kachestva № 1, 2006, s. 57-58.

7. GOST R 53110-2008 «Sistema obespecheniia informatsionnoi bezopasnosti seti sviazi obshchego pol'zovaniia. Obshchie polozheniia». M.: Izd-vo standartov , 2009-23 s.

8. GOST R ISO/MEK 13335-1-2006 «Informatsionnaia tekhnologiia - Metody i sredstva obespecheniia bezopasnosti – Chast' 1: Kontseptsiia i modeli menedzhmenta bezopasnosti informatsionnykh i telekommunikatsionnykh tekhnologii». M.: Izd-vo standartov, 2007 -23 s.

9. **Andrianov V.V., Zefirov S.L., Golovanov V.B., Golduev N.A.** Obespechenie informatsionnoi bezopasnosti biznesa- 2-e izd., pererab. i dop. - M.:TsIPSiR: Al'pina Pablisherz, 2011. - 373 s.

10. **Krat Iu.G., Shramkova I.G.** Osnovy informatsionnoi bezopasnosti : ucheb. posobie /– Khabarovsk : Izd-vo DVGUPS, 2008. – 112 s.

СВЕДЕНИЯ ОБ АВТОРАХ/AUTHORS

СЯЧИНА Татьяна Юрьевна – специалист по качеству, ООО «СП ТЕКНОПЛАСТ-СПб». Россия, 198515, г. Санкт-Петербург, г. Петергоф, ул. КарлаСименса, д.1, лит. А., e-mail: tania-siatchina@yandex.ru

SYACHINA Tatiana Y. – OOO «JV TECNOPLAST SPB». Russia, 198515, Saint-Petersburg, Petergof, St. Karl Siemens 1/a, e-mail: tania-siatchina@yandex.ru