Кокутин С.А. Международная стандартизация в области безопасности информационных и телекоммуникационных технологий // Информационно-экономические аспекты стандартизации и технического регулирования: Научный интернет-журнал. 2012. – № 5(9). Режим доступа http://iea.gostinfo.ru/files/2012_05/2012_05_17.pdf

УДК 338.49

МЕЖДУНАРОДНАЯ СТАНДАРТИЗАЦИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Кокутин С.А. ФГУП «Российский научно–технический центр информации по стандартизации, метрологии и оценке соответствия» (ФГУП «СТАНДАРТИНФОРМ»)

В статье рассматривается значение международных стандартов в области информационной безопасности и обоснована необходимость их применения в современных условиях ведения бизнеса. Дана обобщенная характеристика международному стандарту ISO/IEC 27033.

Ключевые слова: *информационная безопасность, менеджмент информационной безопасности, международный стандарт.*

UDC 338.49

INTERNATIONAL STANDARDIZATION IN THE SECURITY INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Kokutin S.A. FGUP «Russian Research and Development Information Center on Standartization, Metrology and Compliance Check» (FGUP «STANDARTINFORM»)

In the article discusses the importance of international standards in the field of information security and the necessity of their use in the modern business environment. Generalized description given international standard ISO / IEC 27033.

Keywords: *information security, information security management, international standard.*

Трудно себе представить предприятие или организацию без наличия современных информационных и телекоммуникационных систем различного назначения. Их широкое развитие и использование способствует

эффективной организации хозяйственной деятельности. Но в тоже время, информационные технологии предъявляют и особые требования к владельцам бизнеса, а также таят в себе серьезные угрозы. Прежде всего, это касается проблем связанных с информационной безопасностью. Программное обеспечение, базы данных, электронный документооборот, сетевые коммуникации и многое другое, нуждаются в ежедневной защите от злонамеренных действий пользователей.

Практика показала, что любая угроза имеет потенциальную возможность стать причиной нежелательного инцидента, который может повлечь за собой нанесение вреда, как информационной системе, так и организации, ее активам в целом. Такое нанесение вреда может произойти в результате несанкционированного доступа, раскрытия и модификации информации, коррупции среди персонала, приведения активов в состояние непригодности или их утери. Угрозы могут иметь естественное происхождение или исходить от людей, быть случайными или преднамеренными. Как случайные, так и преднамеренные угрозы должны быть определены, а уровень и вероятность их реализации должны быть установлены. Подход к определению степени опасности от конкретной угрозы аналогичен методике определения степени риска и использует определение вероятности возникновения данной угрозы и величины возможного ущерба, которые в свою очередь зависят от степени уязвимости актива и характера воздействия, а также от правильного использования защитных мер.

Именно поэтому специалистам, работающим в сфере ИТ-технологий, необходимо систематизировать и упорядочить основные требования и характеристики компьютерных систем и технологий в части обеспечения безопасности. Им следует обеспечить такое состояние устойчивости данных к случайным или преднамеренным воздействиям, которое будет исключать недопустимые риски их уничтожения, искажения и раскрытия, приводящие к материальному ущербу пользователя или владельца.

Из вышесказанного следует, что ИТ-специалисты нуждаются в наличии специальных руководств по управлению безопасностью информационных и телекоммуникационных технологий, норм, правил, требований, по вопросам безаварийной эксплуатации информационных систем, компьютерных сетей и т.д. Разрешение этих вопросов возложено на разработанные и принятые международные стандарты.

Среди них особое место занимают:

– ISO/IEC 27001:2005[1] – «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Этот международный стандарт был подготовлен с целью создания некоторой модели для введения, реализации, эксплуатации, мониторинга, пересмотра, поддержки и совершенствования системы менеджмента информационной безопасности (СМИБ).

– ISO/IEC 27003:2010[2] – «Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности».

Важно понимать, что менеджмент информационной безопасности следует рассматривать как процесс, использующийся для достижения и обслуживания соответствующих уровней конфиденциальности, целостности, пригодности, ответственности, аутентичности и надежности информации и информационных технологий. В целом функции менеджмента информационной безопасности могут быть сведены к следующему:

– определение организационных целей и стратегий защиты ИТ;

– определение организационных требований защиты ИТ;

– идентификация и анализ угроз активам ИТ в пределах организации;

– идентификация и анализ рисков;

---

[1] См.: International Standard ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements» // www.iso.org.

[2] См.: International Standard ISO/IEC 27003:2010 «Information technology – Security techniques – Information security management system implementation guidance» // www.iso.org.

– определение соответствующих защитных мер;

– контроль выполнения и функционирования защитных мер, которые являются необходимыми для обеспечения эффективной защиты информации и услуг в пределах организации;

– разработка и реализация программы осведомленности о защите;

– обнаружение инцидентов и реагирование на них.

Следует подчеркнуть, что в сфере информационной безопасности сетевая безопасность занимает одну из ключевых позиций. В связи с тем, что организации, для ведения своего бизнеса, в значительной степени зависят от использования сетевых коммуникаций, поэтому даже незначительное нарушение конфиденциальности, целостности и доступности информации, не говоря о потере данных, может привести к значительным неблагоприятным последствиям для ведения бизнеса в целом. Следовательно, основным требованием, касающимся обеспечения надлежащей защиты сетей и связанных с ними информационных систем и информации, является реализация и поддержка адекватной сетевой безопасности.

Именно поэтому, международный стандарт, ISO/IEC 27033, под общим заглавием «Информационная технология – Методы и средства обеспечения безопасности – Сетевая безопасность информационных технологий» предоставляет лицам, отвечающим за информационную безопасность, подробное руководство по вопросам функционирования и использования компьютерных сетей, информационных систем, и менеджмента информационной безопасности в целом. Естественно, что материал данного международного стандарта следует адаптировать к конкретным требованиям того или иного предприятия.

Целями настоящего стандарта, состоящего из нескольких частей, является следующее:

– ISO/IEC 27033-1[1] – Обзор и концепции. Стандартом представлены общий обзор сетевой безопасности и связанные с ней определения и требования, руководство по менеджменту, идентификации и анализу рисков. Он знакомит специалистов с возможностью обеспечения высокого качества специализированных архитектур безопасности, а также с аспектами риска, проектирования мер и средств контроля, и управления, связанными с типичными сетевыми сценариями и областями сетевых «технологий»;

– ISO/IEC 27033-2[2] – Рекомендации по проектированию и реализации сетевой безопасности. Стандарт представляет интерес для персонала, вовлеченного в планирование, проектирование и реализацию проектов архитектуры сетевой безопасности и определяет требуемый уровень качества специализированных архитектур сетевой безопасности, проектирования и реализации, обеспечивающие бизнесу успешность ведения хозяйственной деятельности;

– ISO/IEC 27033-3[3] – Типовые сетевые сценарии – Риски, методы проектирования и вопросы, касающиеся мер и средств контроля и управления. Этой частью представлены определение конкретных рисков, методы проектирования и вопросы, касающиеся мер и средств контроля и управления, связанные с типовыми сетевыми сценариями. Для каждого сценария, предоставляются подробные рекомендации по угрозам безопасности и безопасности методов проектирования и контроля, необходимые для смягчения связанных с ними рисков.

В целом, можно сказать, что приведенные в них положения носят общий универсальный характер и они применимы к различным организациям, с различными стилями и методами управления.

[1] См.: International Standard ISO/IEC 27033-1:2009 «Information technology – Security techniques – Network security – Part 1: Overview and concepts» // www.iso.org.

[2] См.: International Standard ISO/IEC 27033-2:2012 «Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security» // www.iso.org.

[3] См.: International Standard ISO/IEC 27033-3:2010 «Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues» // www.iso.org.

Международные стандарты являются неким руководством по идентификации и анализу рисков сетевой безопасности. Включают в себя обзор мер и средств контроля и управления, поддерживающих специализированные архитектуры сетевой безопасности и связанные с ними технические меры и средства контроля и управления, а также те нетехнические и технические меры и средства контроля и управления, которые применяются не только к сетям. Они знакомят специалистов с тем, каким образом следует добиваться высокого качества функционирования специализированных архитектур сетевой безопасности, а также с аспектами риска, проектирования мер и средств контроля и управления, связанными с типичными сетевыми сценариями и областями сетевых «технологий». Важным аспектом является и рассмотрение вопросов, связанных с реализацией и функционированием мер и средств контроля и управления сетевой безопасностью, постоянным мониторингом и проверкой их реализации.

В данном контексте отрадно подчеркнуть, что разработки в этой области продолжают вестись. В связи с этим планируется подготовить и другие части стандарта, которые будут охватывать проблемы связанные с широкополосными и локальными сетями, размещением информации на сервере веб-узлов, электронной почтой, маршрутизированным доступом для сторонних организаций и др. (см. рис. 1).

Помимо всего прочего, хотелось бы заметить, что основными областями стандартизации информационной безопасности являются: аудит информационной безопасности; модели информационной безопасности; методы и механизмы обеспечения информационной безопасности; криптография; безопасность межсетевых взаимодействий; управление информационной безопасностью. Поэтому приведенными международными стандартами ограничиваться не следует. Широкий спектр областей информационной безопасности, где нашли свое применение другие международные стандарты, наглядно характеризует ниже представленная таблица.

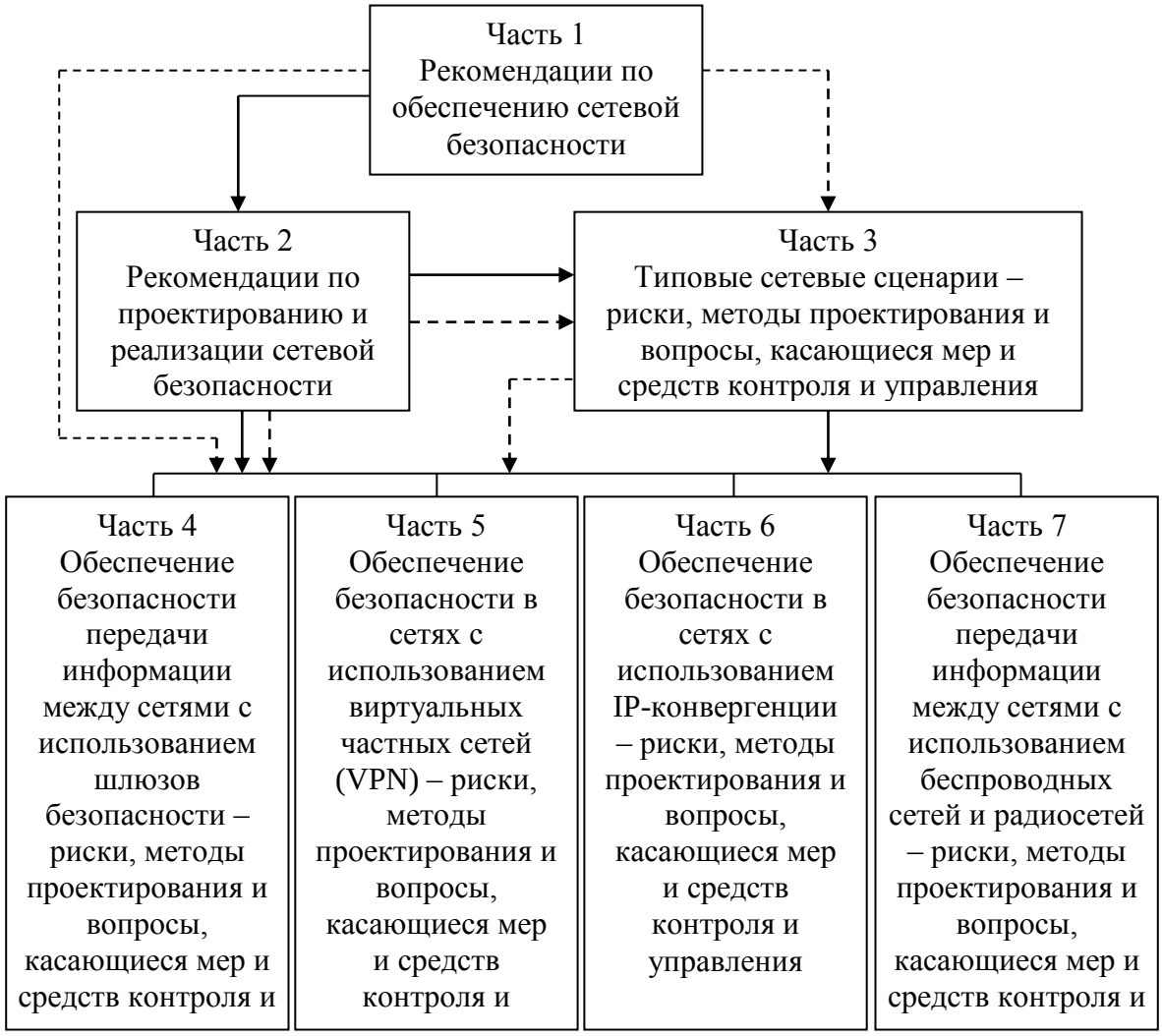

Рис. 1. Проектные темы для рассмотрения в последующих частях стандарта ISO/IEC 27033

Таблица 1

Перечень базовых международных стандартов, разработанных ISO и IEC отражающих проблемы информационной безопасности

Обозначение НД	**Заглавие на русском языке**
ISO/IEC 27001:2005	Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ISO/IEC 27002:2005	Информационные технологии. Свод правил по управлению защитой информации
ISO/IEC 27004:2009	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
ISO/IEC 27005:2011	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
ISO/IEC 27033-1:2009	Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции

ISO/IEC 27033-2:2012	Информационные технологии. Методы и средства обеспечения защиты. Защита сети. Часть 2. Руководящие указания по проектированию и внедрению защиты сети
ISO/IEC 27033-3:2010	Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления
ISO/IEC TR 15443-1:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 1. Обзор и основы
ISO/IEC TR 15443-2:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия
ISO/IEC TR 15443-3:2007	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий Часть 3. Анализ методов доверия
ISO/IEC 15408-1:2009	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель
ISO/IEC 15408-2:2008	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности
ISO/IEC 15408-3:2008	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты
ISO/IEC 18045:2008	Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности ИТ
ISO/IEC TR 19791:2010	Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности действующих систем
ISO/IEC 24762:2008	Информационная технология. Методы и средства обеспечения безопасности. Руководство по услугам по восстановлению информационно-коммуникационных технологий после бедствия
ISO/IEC 21827:2008	Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса (sse-cmm®)

Таким образом, практика показала, что цели и стратегии защиты ИТ-систем должны охватывать следующие основные вопросы защиты информационных технологий, такие как: конфиденциальность; целостность; доступность; аутентичность; надежность.

Безусловно, что исходя из целей, стратегии и имеющихся методов устанавливаются уровень защиты активов, пороговый уровень принятия риска и организационные требования на случай непредвиденных обстоятельств, для каждой организации индивидуально. Правильное

управление активами является важнейшим фактором успешной деятельности организации и основной обязанностью всех уровней руководства.

Не следует забывать и о важности таких аспектов информационной безопасности, как прослеживаемость, осведомленность о защите и мониторинг. Недостаток осведомленности о защите и недостаточная защитная практика персонала организации может также значительно снижать эффективность защитных мер. Поэтому эффективность защитных мер должна подвергаться своевременным проверкам. Это достигается посредством мониторинга и контроля согласованности элементов защиты, чтобы гарантировать, что данные защитные меры функционируют и используются в соответствии со своим назначением.

Список источников и литературы

1. International Standard ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements» // www.iso.org.
2. International Standard ISO/IEC 27003:2010 «Information technology – Security techniques – Information security management system implementation guidance» // www.iso.org.
3. International Standard ISO/IEC 27033-1:2009 «Information technology – Security techniques – Network security – Part 1: Overview and concepts» // www.iso.org.
4. International Standard ISO/IEC 27033-2:2012 «Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security» // www.iso.org.
5. International Standard ISO/IEC 27033-3:2010 «Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues» // www.iso.org.