УДК 004.056

АНАЛИЗ МЕЖДУНАРОДНОГО СТАНДАРТА ISO-IEC 27001-2013

[1]Багров А.П., [2]Багрова В.А.

[1]Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», 105005, Россия, г. Москва, 2-я Бауманская ул., 5, e-mail solmayers@yandex.ru

[2]Акционерное общество «НИИ Аргон», 11740,г. Москва, 5 Варшавское шоссе, 125, стр.1, e-mail: Story_teller@bk.ru

Объектом анализа данной статьи является международный стандарт ISO-IEC 27001-2013. Авторами рассмотрена структура стандарта, его составляющие, включая требования к построению и эксплуатации систем управления информационной безопасности организации в современных условиях ведения коммерческой деятельности. Актуальность данной работы подкрепляется проведением анализа стандарта с точки зрения управления предприятием, а не только с точки зрения специалиста по информационной безопасности. Учитывая растущие риски и угрозы информационной безопасности и кризис доверия, образовывающийся к коммерческим организациям, которые уделяют недостаточное внимание управлению безопасности, анализ данного стандарта направлен на выявление и раскрытие основных преимуществ и недостатков стандарта на текущий момент развития коммерческой деятельности и информационных систем. Отдельное акцент в статье сделан на взаимодействие управленческого состава предприятия и отдела информационной безопасности.

Ключевые слова: информационная безопасность, международные стандарты, сертификация, системы управления информационной безопасностью, ISO-IEC 27001, риск-ориентированный подход

ANALYSIS OF THE INTERNATIONAL STANDARD ISO-IEC 27001-2013

[1]Bagrov A.P., [2]Bagrova V.A.

[1]Bauman Moscow State Technical University, 105005*, Russia, Moscow, 2nd Bauman Str., 5, e-mail solmayers@yandex.ru*
[2]Joint Stock Company "Research Institute Argon", 11740, Moscow, 5 Varshavskoe shosse, 125, b. 1, e-mail: Story_teller@bk.ru

The object of analysis given by the subject of analysis of this article is the international standard ISO-IEC 27001-2013. The authors considered the structure of the standard, its components, including the requirements for the construction and operation of information security management systems of the organization in the current business environment and trends. The relevance of this work is supported by the analysis of the standard not only from the point of view of an information security specialist, but also from the point of view of enterprise management. Given the growing risks and threats to information security and the crisis of confidence that is generated by commercial organizations that do not pay enough attention to security management, the analysis of this standard is aimed at identifying and disclosing the main advantages and disadvantages of the standard at the current state of commercial activities and information systems. A separate emphasis in the article is on the interaction between the management of the enterprise and the information security department.

Key words: information security, international standards, certification, information security management systems, ISO-IEC 27001, risk-oriented approach

В настоящее время международный стандарт ISO-IEC 27001 [1] является наиболее известным стандартом, определяющим требования к информационной безопасности организации в условиях современного ведения бизнеса. Первая версия данного документа, основанная на британском стандарте BS 7799–1:1995 «Практические рекомендации по управлению информационной безопасностью», была принята Объединенным техническим комитетом ISO/IEC JTC 1 по информационным технологиям в 2000 году, однако впоследствии подверглась тщательной переработке и многократному переизданию. Версия стандарта ISO-IEC 27001-2013 является последней вышедшей на данный момент.

В современном информационном мире организации вынуждены оценивать информацию как ценный ресурс, в связи с чем возникает необходимость защиты данного ресурса и сохранения его определяющих свойств: конфиденциальности, целостности и возможности применения. Безопасность информации на данный момент является одним из ключевых факторов успешного функционирования организации, следовательно, система менеджмента информационной безопасности должна быть гармонично внедрена в бизнес-процессы и общую структуру управления.

Основной целью рассматриваемого стандарта является установка требований для создания, внедрения, поддержания функционирования и непрерывного улучшения системы менеджмента информационной безопасности, а также оценка и обработка рисков. Стандарт не допускает пренебрежение ни одним из своих основных пунктов для организации, декларирующей соответствие его требованиям.

В первую очередь стандарт предполагает определение контекста, а именно внутренних и внешних проблем конкретной организации, а также позиций и требований заинтересованных сторон, имеющих возможность влиять на политику информационной безопасности. Совокупность данных условий должна быть оформлена документально.

По рассматриваемому стандарту к высшему руководству организации предъявляются высокие требования. Основной обязанностью руководства является обеспечение возможностей и условий для организации менеджмента информационной безопасности организации, а именно гарантирование слаженной работы системы менеджмента с прочими процессами организации, согласования текущей политики безопасности со стратегией организации, доступности необходимых для ее реализации ресурсов, донесение важности информационной безопасности до персонала всех уровней и контроль за исполнением принятой стратегии.

При планировании системы менеджмента безопасности организация должна учесть проблемы и риски, установленные при первоначальном анализе контекста, а также убедиться, что внедрение системы принесет результаты и уменьшит количество и вероятность нежелательных рисков. Организация должна провести выявление рисков, при осуществлении которых информация лишается одного или сразу всех своих главных свойств - конфиденциальности, целостности и возможности применения. Определяются также источники рисков. Затем производится оценка предполагаемых последствий с вероятностью их возникновения и расстановка рисков по приоритетам для облегчения дальнейшей работы.

Завершение оценки рисков предполагает следующий за этим выбор методов управления рисками и подбор соответствующих средств управления. Стандарт ISO-IEC 27001-2013 делает ссылку на свое приложение А, в котором в краткой форме перечислены задачи управления и практические средства их реализации для обеспечение информационной безопасности организации. Организация имеет возможность выбрать все или несколько - в зависимости от контекста – методов из данного списка. Использование данного приложения гарантирует его пользователю, что никакие средства управления не были пропущены. Приложение А предоставляет максимально краткий вариант представления средств реализации задач. Более полная их реализация, делающая упор на практические технические методы решения, описана в смежном стандарте ISO-IEC 27002-2013[5]. Результатом анализа приложения должно стать формирование Заявления о применимости, содержащего перечисленные средства управления, обоснование их применимости, описание имеющихся уже в организации средств, а также обоснование исключения из плана по внедрению неиспользованных пунктов приложения А. По результатам анализа Заявления о применимости должен быть разработан план обработки рисков информационной безопасности и получено одобрение остаточных рисков. Также план в целом должен быть одобрен владельцами рисков. Вся информация о разработке данного плана должна храниться в документированном виде.

Ожидается, что организация установит цели в сфере информационной безопасности для всех своих уровней. Цели должны быть согласованы в целом с политикой безопасности, учитывать проведенный анализ рисков, быть доведены до сведения сотрудников и сохранять свою актуальность. Информацию по целям тоже необходимо документировать. При планировании достижения целей организация должна определить: конкретные ожидаемые результаты, ответственных лиц, сроки исполнения, необходимые для исполнения ресурсы и метод оценки результатов.

Организация должна определить и предоставить ресурсы для обеспечения системы менеджмента информационной безопасности на всех этапах развития. Информационная безопасность - интеллектуальный продукт, следовательно, главный ресурс, необходимый для ее реализации – человеческий. Высокую важность имеет проверка компетентности персонала, поскольку впоследствии организация обязана гарантировать

компетентность персонала, задействованного в обеспечении информационной безопасности, и поддерживать ее на требуемом уровне. В качестве доказательств компетенции используется документированная информация.

Политика по безопасности должна быть в обязательном порядке доведена до сведения персонала. Собственный вклад каждого конкретного сотрудника в систему безопасности и последствия несоответствий ее требованиям также должны быть известны и понятны всем сотрудникам.

Организацией должны быть определены правила коммуникации, включающие предмет обмена информацией, разрешенное для коммуникации время, круг лиц, имеющих допуск к информации, и методы передачи информации.

Система менеджмента информационной безопасности предполагает наличие документированной информации, которая требуется по данному стандарту, и дополнительной информации, необходимой для обеспечения безопасности конкретной организации. Для всех видов и форм хранения информации должны быть назначены идентификационные данные и обеспечено поддержание пригодности. Согласно данному стандарту, организация должна гарантировать возможность применения и надлежащую защиту документированной информации. Для этого должны быть осуществлены такие методы, как обеспечение доступа (как с возможностью ознакомления, так и внесения изменений) к информации, ее хранение в надлежащем состоянии, контроль над изменениями и установка срока хранения и способа уничтожения.

Организация обязана гарантировать осуществление процессов, необходимых для исполнения вышеуказанных требований, а вся документированная информация, подтверждающее их исполнение, должна быть сохранена в полном объеме.

В качестве контроля должен проводиться мониторинг и последующий анализ результатов образования и функционирования системы менеджмента информационной безопасности, для грамотного проведения которых требуется установить заблаговременно объекты и методы мониторинга, а также условия – время, место, ответственные лица – для его проведения. Должны быть организованы внутренние аудиты организации с целью постоянного контроля за следованием стандарту ISO-IEC 27001-2013, внутренним правилам безопасности и эффективностью самой системы безопасности. При проведении аудитов должны быть обеспечены объективность и беспристрастность проверяющих, а результаты в обязательном порядке передаваться ответственному руководству.

При необходимости по результатам аудита можно производить улучшения системы безопасности. В первую очередь необходимо устранять несоответствия стандарту: меры должны быть приняты как по исправлению несоответствий, так и для устранения их последствий.

В концепции современных трендов развития информационной безопасности [4] и угроз корпоративным ресурсам, включая материальные, данный стандарт позволяет выстроить систему управления безопасностью [2], отвечающую не только регуляторным требованиям, но и коммерческим интересам внедряющей организации.

Данный стандарт выгодно отличается от своих предшественников разделением на две части. Стандарт ISO-IEC 27001-2013 даёт рекомендации и требования с точки зрения управляющего персонала - «сверху-вниз». Данный подход предоставляет возможность сотрудникам отдела информационной безопасности использовать риск-ориентированный подход с учётом целей и терминологии коммерческого управляющего состава. При внедрении данного стандарта, сотрудникам отдела информационной безопасности необходимо не только совершать технические мероприятия, но и учитывать коммерческие интересы предприятия в целом, что позволяет, в текущих условиях, повысить конкурентноспособность предприятия на рынке в условиях изменчивого мира.

Использование данного стандарта позволяет выстроить долгосрочную стратегию информационной безопасности предприятия с потенциалом к гибкости и стойкости от внешних факторов изменчивого мира

Преимуществами применения данного стандарта с точки зрения информационной безопасности являются:

- Построение механизмов выявления рисков и их оптимизации и устранения;
- Гибкость систем и инструментов;
- Введение ответственности за риски и процессы.

Немаловажными факторами являются и те, которые влияют на коммерческую деятельность целиком:

- Сертификация по проверенному стандарту повышает доверие к предприятию в целом;
- Определение контекста рекомендуется использовать и в мероприятиях других сфер, таких как:
  - Оптимизация производственных процессов;

- Оптимизация ресурсов;
- Внедрение новых процессов или технологий.

Повышенное доверие к коммерческой деятельности предприятия позволяет в различных сферах потенциально повысить прибыль и привлечь потенциальных партнёров к ведению совместной деятельности [3].

Стандарт ISO/IEC 27001:2013 позволяет, при наличии существующей системы управления информационной безопасности в соответствии, например, с ISO 9001, произвести модификацию данной системы на основе методологий интеграции и внедрения последних лет[6].

Однако, несмотря на проработанность и очевидные преимущества, стандарт на данный момент имеет ряд недостатков:

- Развитие информационных систем со времени введения стандарта ушло далеко вперед, как и развитие технических средств у злоумышленников, поэтому некоторые меры обеспечения защищенности активов недостаточны для необходимого уровня защищенности

- В ходе приведения некоторых гармонизирующих с ISO/IEC 27001:2013 стандартов к требованиям данного стандарта, в стандарте остались артефакты законодательства данных стандартов. Поэтому рекомендуется применять объективный и последовательный подход при внедрении данного стандарта и аудите на соответствие требованиям данного стандарта, чтобы достичь наибольшей эффективности возможной в рамках данного стандарта.

В заключение, необходимо сказать, что использование данного стандарта позволяет:

- Снизить расходы и издержки на поддержание высокого уровня защищённости;
- Повысить видимость информационных активов для управленческого состава предприятия;
- Повысить видимость и наладить диалог между управленческим составом и отделом информационной безопасности
- Эффективно применить риск-ориентированный подход с точными и подробными обоснованиями;
- Чётко определять личную ответственность и границы ответственность
- Сформировать эффективный план реагирования в экстренных ситуациях
- Выстроить непрерывную систему контроля уровня защищённости и качества средств безопасности

Список литературы

1. ISO/IEC 27001:2013 Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности – Требования. URL: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf(дата обращения: 22.05.2017).

2. Андреева Н.В. Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799)// 2007. №39.URL: http://cyberleninka.ru/article/n/funktsionalnaya-model-sistemy-upravleniya-informatsionnoy-bezopasnostyu-kak-sredstvo-vnedreniya-standartov-lineyki-iso-iec-2700x-bs (дата обращения: 22.05.2017).

3. Давыденко Владимир Александрович, Ахмедзянова Рузиля Маратовна Роль доверия в регулировании взаимоотношений партнеров на потребительском рынке // . 2013. №5.URL: http://cyberleninka.ru/article/n/rol-doveriya-v-regulirovanii-vzaimootnosheniy-partnerov-na-potrebitelskom-rynke (дата обращения: 22.05.2017).

4. Дорофеев Александр Владимирович Менеджмент информационной безопасности: переход на ISO 27001:2013 //2014. №3 (4).URL: http://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-perehod-na-iso-27001-2013 (дата обращения: 22.05.2017).

5. Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27002-2013.pdf (дата обращения: 22.05.2017).

6. Лившиц Илья Иосифович, Лонцих Павел Абрамович Анализ современных трендов по сертификации систем менеджмента информационной безопасности по требованиям ISO 27001 // Вестник ИрГТУ. 2015. №3 (98).URL: http://cyberleninka.ru/article/n/analiz-sovremennyh-trendov-po-sertifikatsii-sistem-menedzhmenta-informatsionnoy-bezopasnosti-po-trebovaniyam-iso-27001 (дата обращения: 22.05.2017).

References

1. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. URL: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf(accessed: 02.05.2017).

2. Andreeva N.V. Functional model of information security management system as a tool of implementation of standards ISO/IEC 2700x (BS 7799)// 2007. №39.URL: http://cyberleninka.ru/article/n/funktsionalnaya-model-sistemy-upravleniya-informatsionnoy-bezopasnostyu-kak-sredstvo-vnedreniya-standartov-lineyki-iso-iec-2700x-bs (accessed: 02.05.2017).

3. Davydenko Vladimir Aleksandrovich, Akhmedzyanova Ruzilya Maratovna The role of trust in regulating the relationships of partners in the consumer market // . 2013. №5.URL: http://cyberleninka.ru/article/n/rol-doveriya-v-regulirovanii-vzaimootnosheniy-partnerov-na-potrebitelskom-rynke (accessed: 21.05.2017).

4. Dorofeev A.V. Information Security Managemant: Transition to ISO 27001:2013 //2014. №3 (4).URL: http://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-perehod-na-iso-27001-2013 (accessed: 19.05.2017).

5. Information technology -- Security techniques -- Code of practice for information security controls. URL: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27002-2013.pdf (accessed: 13.05.2017).

6. Livshits Ilya Iosifovich, Lontsikh Pavel Abramovich Analysis of modern trends in certification of information security management systems according to the requirements ISO 27001 // Bulletin of IrSTU. 2015. №3 (98).URL: http://cyberleninka.ru/article/n/analiz-sovremennyh-trendov-po-sertifikatsii-sistem-menedzhmenta-informatsionnoy-bezopasnosti-po-trebovaniyam-iso-27001 (accessed: 14.05.2017).