Сетевое издание
Регион: государственное и муниципальное управление
www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)
№ 2 (26), 2021 года

УДК 351/354

Самсонов В.С., Черных Д.В.

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИСПОЛНИТЕЛЬНЫХ ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Российская академия народного хозяйства и государственной службы при Президенте РФ

Аннотация: В статье обоснована актуальность применения основных современных, международных стандартов информационной безопасности в исполнительных органах государственной власти Российской Федерации. Проводится оценка наиболее популярных стандартов информационной безопасности.

Ключевые слова: информационная безопасность, защита информации, интернет-защищенность.

UDC 351/354

Samsonov V.S., Chernykh D.V.

PRACTICE OF SUPPORTING PUBLIC INITIATIVES IN THE CITY OF MOSCOW

The Russian Presidential Academy of National Economy and Public Administration

Abstract: The article substantiates the relevance of the application of the main modern, international standards of information security in the executive bodies of state power of the Russian Federation. The most popular information security standards are evaluated.

Key words: information security, information security, Internet security.

Сетевое издание
Регион: государственное и муниципальное управление
www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)
№ 2 (26), 2021 года

Разработка рекомендаций по применению основных нормативных международных стандартов информационной безопасности в исполнительных органах государственной власти Российской Федерации

Актуальность проблемы стандартизации в сфере информационной безопасности (ИБ) обусловлена тем, что специалистам в данной области сегодня практически невозможно обойтись без знаний соответствующих стандартов и спецификаций. На то имеется несколько причин. Формальная состоит в том, что необходимость следования некоторым стандартам (например, криптографическим и Руководящим документам Гостехкомиссии России) закреплена законодательно. Однако наиболее убедительны содержательные причины. Во-первых, стандарты и спецификации - одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях ИБ. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами. Во-вторых, и те, и другие являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов, причем в интернет-сообществе это средство действительно работает, и весьма эффективно. С практической точки зрения, количество стандартов и спецификаций (международных, национальных, отраслевых и т.п.) в области информационной безопасности бесконечно. В статье рассматриваются наиболее важные из них, знание которых необходимо всем или почти всем разработчикам и оценщикам защитных средств, многим сетевым и системным администраторам, руководителям соответствующих подразделений, пользователям. Основное внимание уделяется международному стандарту ISO/IEC 27000-2018 и его

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

российскому аналогу ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий».

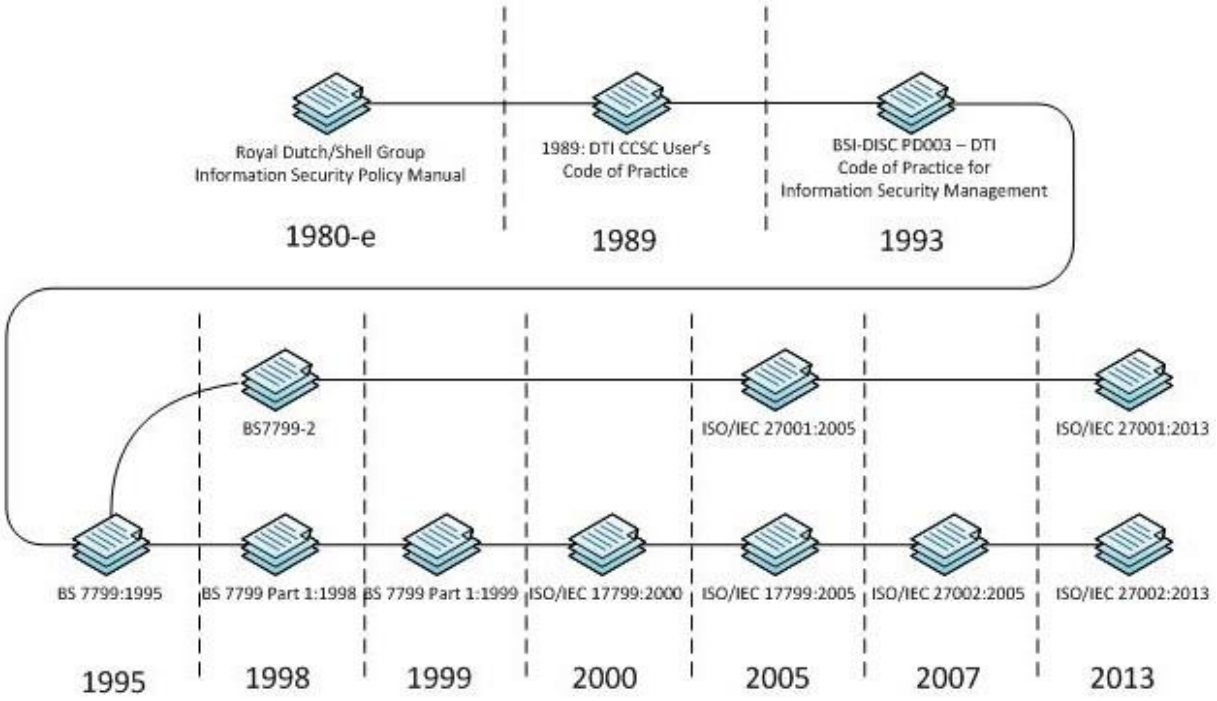

Рисунок 1 – Хронология развития стандарта ISO/IEC 27000 [3]

Статистика показывает, что в России используется более 140 международных стандартов информационных технологий. Более 30 из них касаются информационной безопасности. Некоторые международные стандарты защиты информации приняты и введены в действие в России, но эти стандарты не являются основой для решения проблем информационной безопасности.

Наиболее известным и популярным набором стандартов среди как зарубежных, так и российских ИБ-специалистов, к которому обращаются в первую очередь при внедрении системы управления информационной безопасности, являются документы из серии ИБ-стандартов ISO/IEC 27XXX.

ISO – Международная комиссия по стандартизации, которая разрабатывает и утверждает большинство признанных на международном уровне методик сертификации качества процессов производства и управления;

IEC – Международная энергетическая комиссия, которая внесла в стандарт свое понимание систем ИБ, средств и методов ее обеспечения

Самый известный стандарт серии - ISO/IEC 27000, определяющий аспекты менеджмента информационной безопасности и содержащий лучшие практики по выстраиванию процессов для повышения эффективности управления ИБ. Стандарт декларирует риск-ориентированный подход, который позволяет выбрать необходимые меры и средства защиты, наилучшим образом соответствующие потребностям и интересам организации.

Стандарт ISO/IEC 27000 дает рекомендации по функционированию системы ИБ как комплексной системы, направленной на защиту информационных активов организации от угроз и, следовательно, минимизацию рисков, и представляет собой одну из множества систем организации, к которой предъявляются определенные требования и которая должна оправдать ожидания и вернуть вложенные в нее средства (рис.2).

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

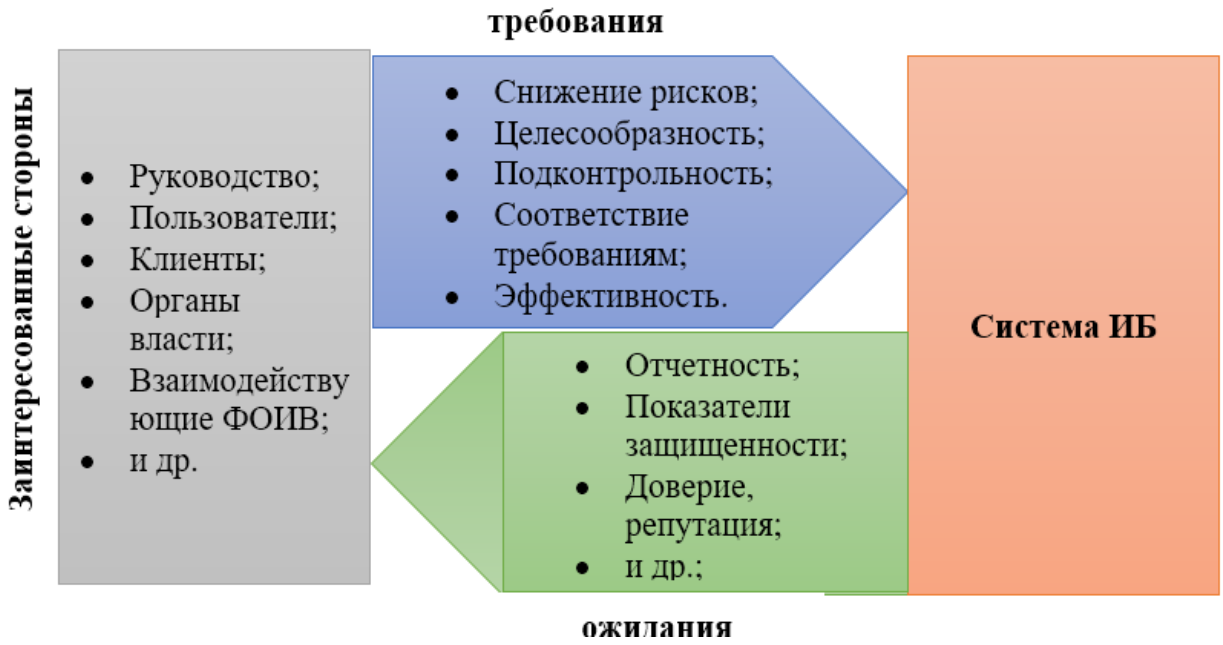

Рисунок 2 – Место системы ИБ в организации. [2]

Стандарт ISO/IEC 27000 состоит из двух частей:

Описание подхода к созданию системы управления информационной безопасности;

Приложение А (требования ИБ и средства их реализации, структурированные по разделам).

Стандарт ISO/IEC 27000 имеет российский аналог ГОСТ Р ИСО/МЭК 27001.

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary	Термины и определения.
ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Requirements	Системы обеспечения информационной безопасности. Документ описывает требования к системе управления информационной безопасностью и средства их реализации.
ISO/IEC 27002 Information technology. Security techniques. Code of practice for information security management	Методы и средства обеспечения информационной безопасности. Стандарт разъясняет практические аспекты управления ИБ с более детальным описанием средств реализации, приведенных в ISO/IEC 27001:2013.
ISO/IEC 27003:2017 Information technology. Security techniques. Information security management system implementation guidance	Реализация систем менеджмента информационной безопасности. Руководство по реализации системы управления информационной безопасностью, описывающее все этапы внедрения.
ISO/IEC 27004:2016 Information technology. Security techniques. Information security management. Measurement	Измерение эффективности информационной безопасности. Описывает подход к использованию метрик для оценки эффективности системы управления информационной безопасности. Стандарт применим к компаниям, достигшим четвертого (управляемого) уровня зрелости процессов ИБ согласно CMMI.
ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management (также можно обратиться к ISO 31000:2018 — Risk management)	Менеджмент риска информационной безопасности. Стандарт предназначен для определения в компании подхода к менеджменту рисков.
ISO/IEC 27035:2016 Information technology. Security techniques. Information security incident management (Part 1 & Part 2)	Управление инцидентами и событиями ИБ. Стандарт содержит руководящие указания по планированию и подготовке к реагированию на инциденты.

Также специалисты часто обращаются к стандарту ISO/IEC 27002:2013 (ранее выходил под номером ISO/IEC 17799), более подробно раскрывающему высокоуровневые требования ISO/IEC 27001:2013 к выстраиванию процессов в системе управления информационной безопасностью. Документ описывает

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

рекомендуемые практические меры в области управления информационной безопасностью.

Еще одним стандартом, применяемым зарубежными ИБ-специалистами, является ISO 15408, состоящий из трех частей:

ISO/IEC 15408-1:2009 Evaluation criteria for IT security — Part 1: Introduction and general model — «Общие критерии оценки безопасности информационных технологий».

ISO/IEC 15408-2:2008 Evaluation criteria for IT security — Part 2: Security functional components model — «Функциональные компоненты безопасности».

ISO/IEC 15408-3:2008 Evaluation criteria for IT security — Part 3: Security assurance components — «Компоненты доверия к безопасности».

Первая часть стандарта содержит единые критерии оценки безопасности ИТ-систем на программно-аппаратном уровне (по аналогии с документом «Критерии оценки пригодности компьютерных систем Министерства обороны» (Department of Defence Trusted Computer System Evaluation Criteria - TCSEC), также известным как «Оранжевая книга» из стандартов «Радужной серии» Министерства обороны США). Стандарт ISO/IEC 15408-1:2009 определяет полный перечень объектов анализа и требований к ним, не заостряя внимания на методах создания, управления и оценки системы безопасности.

Вторая часть приводит требования к функциональности средств защиты, которые могут быть использованы при анализе защищенности для оценки полноты реализованных функций безопасности.

Третья часть серии содержит обоснования угроз, политик и требований. Стандарт определяет компоненты доверия к безопасности, каталогизирует наборы компонентов и классов доверия. ISO/IEC 15408-3:2008 включает в себя оценочные уровни доверия, определяющие шкалу измерения и компоненты доверия, а также критерии оценки профилей защиты и заданий безопасности.

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

В целом эти стандарты содержат техническую часть, не акцентируя внимание на вопросах управления информационной безопасностью.

На основании данного стандарта в свое время был разработан руководящий документ ФСТЭК (Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187).

В данной статье рассматриваются основные нормативные средства обеспечения информационной безопасности[1].

Эта категория средств представлена законодательными актами и нормативно-распорядительными документами, которые действуют на уровне организации.

Актуальная версия ISO/IEC 27000 предлагает готовые стандарты и опробованные методики, необходимые для внедрения ИБ. По мнению авторов методик, основа информационной безопасности заключается в системности и последовательной реализации всех этапов от разработки[2].

Для получения сертификата, который подтверждает соответствие стандартам по обеспечению информационной безопасности, необходимо внедрить все рекомендуемые методики в полном объеме. Если нет необходимости получать сертификат, в качестве базы для разработки собственных ИБ-систем допускается принять любую из более ранних версий стандарта, начиная с ISO/IEC 27000-2002, или российских ГОСТов, имеющих рекомендательный характер.

Практика использования стандарта ISO/IEC 27000 за рубежом показывает, что данный регламент один из самых динамично развивающихся стандартов по информационной безопасности. Об этом говорит не только заложенный в серию стандартов объем полезных знаний, но и статистика. По данным последнего опубликованного отчета ISO, с 2015-го по 2020 год количество сертифицированных объектов ИБ выросло более чем в два раза – с

33 тыс. до 68 тыс. Наибольшее количество сертификаций прошло в Японии, Китае, Великобритании, Индии, США, Германии, Италии и других странах Европейского союза. Тенденция к росту популярности стандарта, вероятно, закрепится – в связи с необходимостью создания эффективной системы информационной безопасности для выполнения требований General Data Protection Regulation (GDPR).

Однако Россия по количеству выданных сертификатов (на 2021 год – 235) пока находится только в третьем десятке стран Европы, даже при том, что при подсчете учитывались сертификаты, выданные как в международной, так и в национальной системе сертификации (т.е. аудиторами, аккредитованными национальным органом по сертификации (Росстандарт), а не только International Accreditation Forum (IAF)).

По статистике за 2021 год, наиболее популярной была сертификация в ИТ-отрасли и телекоммуникациях. Можно предположить, что преобладание сертифицированных ИТ- и сервисных организаций во многом связано с передачей крупными компаниями своих ИТ-процессов на аутсорсинг и распространением облачных и сервисных услуг. В числе компаний-аутсорсеров можно выделить - Яндекс, Google, Microsoft, Amazon, IBM, Atos Origin, CSC, BNP Paribas Partners for Innovation и др. Кроме того, множество компаний непублично следуют рекомендациям 27000, не сертифицируя собственную систему ИБ.

Постоянный рост числа приверженцев стандарта во всем мире не случаен и объясняется преимуществами его применения. Так, опрос, проведенный компанией IT Governance в организациях, которые внедрили ISO/IEC 27000, дал следующие результаты:

98% респондентов заявили о повышении уровня информационной безопасности;

67% отметили актуальность стандарта в своей отрасли бизнеса;

56% респондентов отметили новые конкурентные преимущества;

у 56% организаций выросла способность выполнять нормативные правовые требования;

77% используют стандарт одновременно с другими инструментами контроля в сфере информационной безопасности;

71% получали от клиентов запросы подтверждения соответствия требованиям ISO/IEC 27001.

По итогам изучения стандарта разрабатываются два документа, которые касаются безопасности информации. Основной, но менее формальный – концепция ИБ в исполнительных органах государственной власти, которая определяет меры и способы внедрения ИБ-системы для информационных систем организации. Второй документ, который обязаны исполнять все сотрудники организации, – положение об информационной безопасности, утверждаемый на уровне руководства исполнительного органа государственной власти.

Кроме положения на уровне организации должны быть разработаны перечни подлежащие защите сведений, приложения к трудовым договорам, закрепляющие ответственность за разглашение конфиденциальных данных, иные стандарты и методики. Внутренние нормы и правила должны содержать механизмы реализации и меры ответственности. Чаще всего меры носят дисциплинарный характер, и нарушитель должен быть готов к тому, что за нарушение разработанных правил последуют существенные санкции вплоть до увольнения.

Организационные и административные меры:

В рамках административной деятельности по защите ИБ для сотрудников, назначенных ответственными за обеспечение информационной

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

безопасности, открывается простор для творчества. Это и архитектурно-планировочные решения, позволяющие защитить кабинеты сотрудников руководства от прослушивания, и установление различных уровней доступа к информации. Важными организационными мерами станут сертификация деятельности организации по стандартам ISO/IEC 27000, сертификация отдельных аппаратно-программных комплексов, аттестация субъектов и объектов на соответствие необходимым требованиям безопасности, получений лицензий, необходимых для работы с защищенными массивами информации.

С точки зрения регламентации деятельности сотрудников важным станет оформление системы запросов на допуск к интернету, внешней электронной почте, другим ресурсам. Отдельным элементом станет получение электронной цифровой подписи для усиления безопасности охраняемых сведений и другой информации, которую передают другим государственным органам по каналам электронной почты.

Морально-этические меры:

Морально-этические меры определяют личное отношение сотрудника к конфиденциальной информации или информации, ограниченной в обороте. Повышение уровня знаний сотрудников касательно влияния угроз на деятельность исполнительного органа государственной власти влияет на степень сознательности и ответственности сотрудников. Чтобы бороться с нарушениями режима информации, включая, например, передачу паролей, неосторожное обращение с носителями, распространение конфиденциальных данных в частных разговорах, требуется делать упор на личную сознательность сотрудника. Полезным будет установить показатели эффективности, которые будут зависеть от отношения к корпоративной системе ИБ [4].

По мере развития технологий, роста объема информационных ресурсов и появления новых нормативных требований увеличиваются и затраты на

www.regiongmu.ru
ЭЛ № ФС77-58405 от 25.06.2014
ISSN 2411-7331 (online)

обеспечение информационной безопасности. Все важнее становятся вопросы обоснования расходов на эффективную систему ИБ. В таких условиях необходимо избежать дублирования процессов защиты информации, исключить корпоративные «двойные стандарты», поднять защиту информации на качественно новый уровень и оправдать вложенные в обеспечение информационной безопасности средства. Решить эти задачи позволяет внедрение в организации стандарта информационной безопасности ISO/IEC 27000.

Необходимо понимать, что для качественного построения системы ИБ использовать только нормативные средства не корректно, требуется совмещать комплексные подходы, обеспечения информационной безопасности, полученные из разных источников, так как каждая система взглядов содержит плюсы и минусы и требует адаптации к условиям конкретной организации. Специалистам по информационной безопасности необходимо постоянно совершенствоваться, расширять набор компетенций и профессиональных знаний, и принятые за рубежом стандарты существенно помогают в этом.

Список использованных источников

1. Код безопасности - [Электронный ресурс] URL: https://www.securitycode.ru/
2. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
3. Официальный сайт ISO/IEC 27000:2018 - [Электронный ресурс] URL: https://www.iso.org/ru/standard/73906.html

4. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права № 8 - 2015. - С.100-109.