ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2013. Т. 17, № 7 (60). С. 55–60 http://journal.ugatu.ac.ru

УДК 336.7:004.43

# СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СИСТЕМЕ

**Р. Х. МАРДАНОВ, И. В. ИЛЬИН**

bank@ufa.cbr.ru

Национальный банк Республики Башкортостан Центрального банка РФ

*Поступила в редакцию 10.09.2013*

**Аннотация.** Рассматривается применение стандартов информационной безопасности в банковской системе. Приведен обзор комплекса документов по стандартизации информационной безопасности Банка России. Кратко описаны подходы для построения эффективной системы информационной безопасности и изложены принципы оценки и самооценки соответствия информационной безопасности требованиям стандартов. В качестве примера практического применения стандартов информационной безопасности рассматриваются нормативные документы Банка России по регулированию вопросов обеспечения защиты информации в национальной платежной системе.

**Ключевые слова:** Банк России; информационная безопасность; стандарты; ABISS.

На современном этапе развития информационных технологий становится очевидным, что для создания надежных и эффективно работающих банковских продуктов существует необходимость в обеспечении высокого уровня их информационной безопасности. Для этого должны быть точно оценены риски, внедрены необходимые системы защиты. Расширение спектра и рост объемов банковских услуг требует наличие единых подходов, единой терминологии и единых критериев оценки состояния информационной безопасности банков на уровне национальных стандартов – только в этих условиях возможно обеспечить необходимый уровень устойчивости банковской системы.

В мировой практике такие стандарты существуют (COBIT, BS 7799 ISO 17799) и успешно используются, в том числе, и в банковском секторе.

В России существует отраслевой комплекс стандартов банка России под общим названием «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», состоящий из 8 документов, а именно:

- «Общие положения» СТО БР ИББС 1.0 – 2010;
- «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0-20XX» СТО БР ИББС-1.2-2010;
- «Руководство по самооценке информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0» РС БР ИББС-2.1-2007;
- «Аудит информационной безопасности» СТО БР ИББС-1.1-2007;
- «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиям стандарта СТО БР ИББС-1.0» РС БР ИББС-2.0-2007;
- «Методика оценки рисков информационной безопасности» РС БР ИББС-2.2-2009;
- «Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» РС БР ИББС-2.3-2010;
- «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» РС БР ИББС-2.4-2010.

Базовым документом является стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС 1.0 – 2010, где последовательно реализованы требования международных стандартов в области информационной безопасности с учетом условий современной банковской системы России.

Указанный стандарт содержит наиболее важные рекомендации по организации менеджмента информационной безопасности.

Логика стандарта заключается в описании следующих этапов создания системы обеспечения информационной безопасности организации.

1. Формирование целей информационной безопасности – в данном контексте на основе исходной концептуальной модели (парадигмы), принципов информационной безопасности описывается политика информационной безопасности в виде набора требований для областей деятельности организации (назначение и распределение ролей, обеспечение доверия персоналу; обеспечение ИБ на стадиях жизненного цикла АБС; защита от НСД; антивирусная защита; использование ресурсов Интернета; использование СКЗИ; защита технологических процессов и др.).

2. Реализация целей информационной безопасности – включает разделы стандарта, в которых приводятся требования к управлению информационной безопасностью, среди которых требования к организации и функционированию службы ИБ, оценке и обработке рисков ИБ, обучению и повышению осведомленности персонала, обнаружению и реагированию на инциденты ИБ, обеспечению непрерывности бизнеса и др.

3. Контроль достижения целей информационной безопасности – включает разделы стандарта, в которых приводятся требования по организации аудита информационной безопасности, проведению самооценки информационной безопасности, анализу функционирования системы обеспечения информационной безопасности, принятию решений по тактическим и стратегическим улучшениям системы обеспечения ИБ.

Стандарт рассматривает менеджмент информационной безопасности как часть общего корпоративного менеджмента организации. Менеджмент ИБ должен быть ориентирован на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы.

Для реализации и поддержания ИБ в организации реализуются группы процессов в виде циклической модели Деминга: «.. – планирование – реализация – проверка – совершенствование – планирование – ..», которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO/IEC IS 27001-2005.

Модель зрелости процессов управления информационной безопасностью организации в настоящем стандарте основывается на модели зрелости, определенной стандартом COBIT, которая определяет шесть уровней зрелости организации – с нулевого по пятый.

Нулевой уровень характеризует полное отсутствие каких-либо процессов управления информационной безопасностью в рамках деятельности организации. Организация не осознает существования проблем информационной безопасности.

Первый уровень («начальный») характеризует наличие документально зафиксированных свидетельств осознания организацией существования проблем обеспечения информационной безопасности. Однако используемые процессы управления информационной безопасностью нестандартизованы, применяются эпизодически и бессистемно. Общий подход к управлению информационной безопасностью не выработан.

Второй уровень («повторяемый») характеризует проработанность процессов управления информационной безопасностью до уровня, когда их выполнение обеспечивается различными людьми, решающими одну и ту же задачу. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а ответственность возложена на исполнителя. Руководство организации в значительной степени полагается на знания исполнителей, что влечет за собой высокую вероятность возможных ошибок.

Третий уровень («определенный») характеризует то, что процессы стандартизованы, документированы и доведены до персонала посредством обучения. Однако порядок использования данных процессов оставлен на усмотрение самого персонала. Это определяет вероятность отклонений от стандартных процедур, которые могут быть не выявлены. Применяемые процедуры не оптимальны и недостаточно современны, но являются отражением практики, используемой в организации.

Четвертый уровень («управляемый») характеризует то, что обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов управления информационной безопасностью обеспечивается их оптимизация. Процессы управления информационной безопасностью находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства авто-

матизации управления информационной безопасностью используются частично и в ограниченном объеме.

Пятый уровень («оптимизированный») характеризует разработанность процессов управления информационной безопасностью до уровня лучшей практики, основанной на результатах непрерывного совершенствования и сравнения уровня зрелости относительно других организаций. Защитные меры в организации используются комплексно, обеспечивая основу совершенствования процессов управления информационной безопасностью. Организация способна к быстрой адаптации при изменениях в окружении и бизнесе.

Процессы оценки степени соответствия информационной безопасности модели зрелости также стандартизированы. К этим стандартам относятся «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0-20ХХ», «Руководство по самооценке информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0» и «Аудит информационной безопасности».

Аудит ИБ организаций банковской системы позиционируется Банком России как один из важнейших процессов в управлении ИБ организации. Основными целями аудита являются:

- повышение доверия к организациям банковской системы;
- оценка соответствия ИБ организаций банковской системы критериям аудита, установленным основным стандартом СТО БР ИББС-1.0.

В ходе деятельности организации, развивающегося бизнеса в условиях изменяющейся внешней и внутренней среды, важно гибко адаптировать выстроенную систему ИБ к изменениям этих условий. Для этого необходимо осознанно и целенаправленно строить прогноз изменения среды, своевременно выполнять анализ и вести мониторинг выстроенной системы безопасности, а также оперативно вносить в нее корректировки. Поскольку изменения среды, особенно внутренней, носят непрерывный характер, данную работу требуется выполнять на постоянной основе с использованием объективно полученной информации, каковой и должна выступать, в том числе и информация, полученная в ходе проведения аудита. Аудит должен строиться на основе анализа существующей документации по обеспечению ИБ и объективных фактов, свидетельствующих о частичном, полном выполнении или невыполнении установленных требований ИБ.

Наряду с аудитом в процессах контроля важную роль играет процесс самооценки соответствия информационной безопасности. Самооценка – это регулярный процесс, позволяющий количественно оценить состояние уровня ИБ организации. В соответствии с «Методикой самооценки» уровень информационной безопасности организации складывается из следующих компонентов:

- текущий уровень ИБ организации;
- менеджмент ИБ организации;
- уровень осознания ИБ организации.

Оценка текущего уровня ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС 1.0 в части реализованных мер защиты.

Оценка менеджмента ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС 1.0 в части управления процессами ИБ.

Оценка уровня осознания ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС1.0 в части деятельности руководства организации по поддержке системы обеспечения ИБ.

При вычислении значения оценки каждого уровня используются таблицы, которые заполняются на основе результатов экспертного анализа нормативно-распорядительных документов организации, имеющих отношение к общим принципам безопасного функционирования и специальным принципам обеспечения ИБ, опросов сотрудников организации и наблюдения за выполнением процедур ИБ.

Вычисленные значения групповых показателей по направлениям оценки отображаются круговой диаграммой, разбитой на 32 сектора. Для оценивания текущего уровня организации отведены с 1 по 8 сектор, отображениям оценки процессов менеджмента ИБ отводится с 9 по 27 сектор. Сектора с 28 по 32 используются для оценки уровня осознания ИБ. За единицу рассматриваемой оценки принято внешнее кольцо диаграммы. Радиальный отрезок от центра до внешнего кольца разбит на шесть диапазонов:

- [0–0.25] – нулевой уровень ИБ,
- ]0.25–0.5] – первый уровень ИБ,

- ]0.5–0.7] – второй уровень ИБ,
- ]0.7–0.85] – третий уровень ИБ,
- ]0.85 – 0.95] – четвертый уровень ИБ,
- ]0.95 – 1] – пятый уровень ИБ.

Методическими рекомендациями по документации в области обеспечения информационной безопасности в соответствии с требованиями стандарта СТО БР ИББС-1.0 устанавливаются требования к составу и структуре документов, регламентирующих процессы ИБ организации. Определяются принципы менеджмента документации и приводятся примеры структуры и содержания корпоративных политик информационной безопасности.

Одним из подходов к построению эффективной системы обеспечения информационной безопасности, изложенным в Стандарте Банка России, является принцип определения защищенности по величине остаточных рисков. В реальности риски не всегда можно исключить полностью, а можно понизить лишь до определенного уровня. Остаточная часть риска должна быть признана приемлемой и принята, либо отклонена. В последнем случае от риска следует уклониться (изменить деятельность), либо перевести на другой объект (например, застраховать).

Процесс оценки рисков описан в документе «Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

Суть процесса заключается в определении и классификации информационных активов, выявлении объектов среды, составляющих информационные активы, определении степени возможности реализации угроз и определении степени тяжести последствий от реализации угроз для каждого актива. Далее, на основе качественного сопоставления возможности реализации и возможной тяжести последствий от реализации угроз определяются значения допустимого и недопустимого риска для каждого информационного актива.

Организации защиты информации в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» посвящены «Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» и «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации».

Применение Стандарта Банка России в организациях банковской системы в настоящее время приобретает особую актуальность в связи с вводом в действие Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе».

Обеспечение информационной безопасности играет ключевую роль в сфере минимизации операционных рисков и обеспечения бесперебойности функционирования платежной системы. Система безопасности должна обеспечивать достаточный уровень защиты от возможных внутренних и внешних угроз, которым могут подвергнуться платежные системы.

С принятием закона «О национальной платежной системе» законодательное регулирование сферы функционирования платежных систем, обеспечения бесперебойности их функционирования и, в том числе информационной безопасности выходит на принципиально новый уровень.

Закон о НПС дает четкое представление о структуре национальной платежной системы, ее субъектах (операторах). В соответствии с законом под национальной платежной системой понимается совокупность:

- операторов по переводу денежных средств (включая операторов электронных денежных средств);
- банковских платежных агентов (субагентов);
- платежных агентов;
- организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации;
- операторов платежных систем, операторов услуг платежной инфраструктуры.

Учитывая, что национальная платежная система представляет собой совокупность различных организаций, безопасность ее функционирования должна обеспечиваться путем налаживания наиболее эффективных инструментов и методов взаимодействия данных организаций.

Указанным законом расширены полномочия и ответственность Банка России в сфере НПС посредством определения новой цели деятельности Банка России – обеспечение стабильности и развитие национальной платежной системы. При этом стабильность национальной платежной системы определяется бесперебойностью ее

функционирования, важным компонентом которой является обеспечение информационной безопасности.

В целях реализации требований 161-ФЗ Банком России выпущено Положение «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» от 09 июня 2012 года № 382-П. Положение устанавливает требования, в соответствии с которыми операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обеспечивают защиту информации при осуществлении переводов денежных средств, а также устанавливает порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

Требования по защите информации, изложенные в 382-П, базируются на требованиях Стандарта Банка России СТО БР ИББС 1.0-2010 и устанавливаются в части:

– назначения и распределения функциональных прав;

– жизненного цикла – создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры;

– осуществления доступа к объектам информационной инфраструктуры;

– защиты информации от воздействия вредоносного кода;

– использования информационно-телекоммуникационной сети Интернет;

– использования средств криптографической защиты информации;

– использования технологических мер защиты информации;

– организации и функционирования службы информационной безопасности;

– повышения осведомленности работников в области обеспечения защиты информации;

– выявления инцидентов и реагирования на них;

– определения и реализации порядка обеспечения защиты информации;

– оценки выполнения требований к обеспечению защиты информации;

– доведения информации об обеспечении защиты информации;

– совершенствования защиты информации.

Положение предусматривает проведение периодической оценки выполнения требований информационной безопасности при осуществлении переводов денежных средств операторами платежных систем, операторами по переводу денежных средств, операторами услуг платежной инфраструктуры и устанавливает формы контроля со стороны Банка России

Также Банк России Указанием №2831-У от 09.06.2012 г. устанавливает формы отчетности по обеспечению защиты информации при осуществлении переводов денежных средств, в том числе отчетность по выявлению инцидентов, связанных с нарушений требований к обеспечению защиты информации при осуществлении перевода денежных средств.

Указанием предусмотрено две формы отчетности, направляемые в Банк России, а также приведены методики составления отчетности, позволяющие формировать количественную оценку показателей выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств.

В заключение следует отметить, что в настоящее время стандарты информационной безопасности Банка России широко используются в кредитных организациях, существует сообщество пользователей стандартов информационной безопасности ABISS, целью которого является продвижение стандартов в организациях – участниках национальной платежной системы Российской Федерации.

Начиная с 2009 года в Республике Башкортостан на базе санатория «Юбилейный» ежегодно проводится межбанковская конференция «Информационная безопасность банков», организованная Ассоциацией российских банков совместно с Сообществом пользователей стандартов Банка России (ABISS) при официальной поддержке Банка России. В конференции традиционно принимают участие руководители банков и кредитных организаций, специалисты в области информационной безопасности, риск-менеджеры, специалисты службы внутреннего контроля, внутренних и внешних аудиторов информационных технологий и информационной безопасности, руководители процессинговых центров. В программу конференции неизменно входит тематическое заседание, посвященное вопросам стандартизации информационной безопасности.

**ОБ АВТОРАХ**

**МАРДАНОВ Рустэм Хабибович**, председатель Национального банка Республики Башкортостан. Дипл. инж.-экономист (УАИ, 1986). Канд. экон. наук (Баш. филиала АН СССР, 1992), доцент.

**ИЛЬИН Игорь Владимирович**, зам. нач. управления безопасности и защиты информации Национального банка Республики Башкортостан.

**METADATA**

**Title:** Information security standards in the banking system.

**Authors:** R. Kh. Mardanov, I. V. Ilyin

**Affiliation:** The National Bank of the Republic of Bashkortostan Bank of Russia.

**Email:** bank@ufa.cbr.ru

**Language:** Russian.

**Source:** Vestnik UGATU (Scientific journal of Ufa State Aviation Technical University), vol. 17, no. 7 (60), pp. 55-60, 2013. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

**Abstract:** Article is devoted to application of standards of information security in a banking system. The review of a complex of documents on standardization of information security of Bank of Russia is provided. In article approaches for creation of effective system of information security are briefly described and the principles of an assessment and a self-assessment of compliance of information security are stated to requirements of standards. As an example of practical application of standards of information security the authors consider normative documents of Bank of Russia on regulation of questions of ensuring information security in national payment system. This article is intended for a wide audience.

**Key words:** Bank of Russia; information security; standards; ABISS.

**About authors:**

**MARDANOV, Rustem Khabibovich**, dipl. of engineer-economist (UAI, 1986). Cand. of Econ. Sci (Bashkir Branch of the Academy of Sciences of the USSR, 1992), docent, chairman of the National Bank of the Republic of Bashkortostan Bank of Russia, Ufa.

**ILYIN, Igor Vladimirovich**, Deputy Head of the Security and Information Protection of National Bank of the Republic of Bashkortostan Bank of Russia, Ufa.