**Стандартизация в области**

**информационной безопасности банковской системы**

**Эффективное и безопасное, в том числе бесперебойное, функционирование банковской системы в целом и платежной системы в частности, является основной целью Национального Банка Республики Беларусь. Важнейшее условие ее реализации – обеспечение необходимого и достаточного уровня информационной безопасности банков, их активов (в т.ч. информационных), которая во многом определяется уровнем информационной безопасности банковских технологических процессов (платежных, информационных и пр.), автоматизированных банковских систем.**

Особенности банковской системы таковы, что негативные последствия сбоев в работе отдельных банков могут привести к быстрому развитию системного кризиса платежной системы, нанести ущерб интересам собственников и клиентов. В случаях наступления угрозы информационной безопасности значительно возрастает риск и возможность нанесения ущерба банкам, что представляет для них существенную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов информационной безопасности (их влияния на операционный, репутационный, стратегический и иные риски) необходимо обеспечить достаточный (приемлемый) уровень информационной безопасности, а также сохранять его в течение длительного времени. По этим причинам обеспечение информационной безопасности является одним из основополагающих аспектов деятельности банков.

Важнейшая особенность информационной безопасности как состояния любого объекта информатизации заключается в том, что это состояние существенно нестабильно. Если непрерывно не предпринимать необходимых дополнительных мер по поддержанию и совершенствованию достигнутого уровня, то он будет снижается. В связи с этим Национальный Банк Республики Беларусь является сторонником регулярной оценки уровня информационной безопасности в банках страны, оценки риска нарушения информационной безопасности и принятия мер, необходимых для управления этим риском.

Наиболее распространенным подходом к оценке уровня безопасности в настоящее время является подтверждение соответствия информационной безопасности установленным требованиям по безопасности. Требования устанавливаются либо нормативными правовыми актами, либо техническими нормативными правовыми актами, либо собственником или владельцем системы на основе оценки рисков через политику информационной безопасности.

В данном случае Национальным банком Республики Беларусь было принято решение регламентировать процессы обеспечения информационной безопасности банков посредством их стандартизации. Основанием для разработки комплекса стандартов по обеспечению информационной безопасности банков Республики Беларусь послужили положения Банковского кодекса [1], в частности статьи 25, 26, 32, 34, 35.

В качестве основы были взяты отработанные, проверенные практикой достаточно успешного применения стандарты Банка России, и это является не случайным в свете тех интеграционных процессов, которые активно развиваются в настоящее время. Такое решение обеспечивает гармонизацию соответствующего нормативно-правового обеспечения в банковской сфере.

Представляемые в настоящей статье стандарты, которые вводятся в действие в июле 2014 года, включают:

- СТБ 34.101.41-2013 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения»;

- СТБ 34.101.42-2013 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности»;

- СТБ 34.101.61-2013 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки рисков нарушения информационной безопасности»;

- СТБ 34.101.62-2013 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41»;

СТБ 34.101.68-2013 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Методика оценки соответствия информационной безопасности банков Республики Беларусь требованиям СТБ 34.101.41».

При разработке данных документов ставились следующие цели:

- развитие, укрепление и повышение доверия к банковской системе Республики Беларусь;

- поддержание стабильности банков и на этой основе банковской системы республики в целом;

- достижение адекватности мер защиты реальным угрозам информационной безопасности;

- предотвращение и (или) снижение ущерба вследствие возможных нарушений штатных режимов функционирования информационных систем.

С принятием рассматриваемого комплекта стандартов устанавливаются единые требования по безопасности для всех банков Республики Беларусь, процедуры оценки достаточности мер по обеспечению безопасности, методика оценки соответствия установленным требованиям, что предоставляет возможность Национальному банку на легитимной основе эффективно осуществлять контроль за обеспечением безопасности и защиты информационных ресурсов в банках и небанковских кредитно-финансовых организациях.

Основные отличия от российских стандартов коснулись двух аспектов:

-обеспечения безопасности персональных данных;

- самооценки.

Понятие персональных данных[[1]](#footnote-1) исключено из стандартов, поскольку в Республике Беларусь пока нет соответствующего акта законодательства, а действующие правовые нормы [2, ст. 18] недостаточны для того, чтобы устанавливать технические требования по защите персональных данных в стандартах. Но это не означает, что защита персональных данных исключается: она осуществляется как защита информации, распространение, предоставление и доступ к которой ограничен законодательными актами Республики Беларусь.

Исключено также понятие «самооценка». Вместо него введено общепринятое в международной практике понятие «внутренний аудит информационной безопасности», важнейшей целью которого является помощь сотрудникам банка в эффективном выполнении ими своих обязанностей в сфере информационной безопасности. Для этого внутренний аудит снабжает аналитическими данными, оценками, рекомендациями, советами и информацией, касающимися деятельности по обеспечению информационной безопасности.

Особенности данного комплекта стандартов по отношению к стандартам серии СТБ ISO/IEC 27000, кроме того, что в них отражена отраслевая специфика банковской информатизации, заключаются в том, что требования представлены в двух разделах: к системе информационной безопасности и к системе менеджмента информационной безопасности банка (СТБ 34.101.40). Отличием является и то, что оценка осуществляется по трем направлениям – текущий уровень информационной безопасности, менеджмент информационной безопасности банка и уровень осознания информационной безопасности банком. Результирующая оценка представляет собой наихудшую из трех, в соответствии с принципом «Безопасность системы определяется самым слабым ее звеном».

Оценка рисков информационной безопасности представлена конкретной методикой оценки, которую можно выполнять как в качественной, так и в количественной форме. Аудит информационной безопасности представлен не только требованиями к проведению аудита информационной безопасности банков (СТБ 34.101.42-2013), но и обеспечивается прагматичной методикой – методикой количественной экспертной оценки соответствия (СТБ 34.101.68-2013), применимой как для внешнего, так и для внутреннего аудита.

В качестве отдельного стандарта представлены методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТБ 34.101.41-2013.

СТБ 34.101.62-2013 устанавливает рекомендации к структуре, составу, назначению и содержанию внутренних документов банка по обеспечению информационной безопасности в соответствии с требованиями СТБ 34.101.41-2013. Особо следует отметить, что в данном стандарте значительное внимание уделено такому неоднозначно трактуемому феномену как «политика информационной безопасности». В стандарте представлены рекомендации по содержанию политик различного уровня, а в приложениях к нему – структура (иерархия) рекомендуемых политик, рекомендации по вопросам формирования корпоративной политики информационной безопасности и пример состава возможных частных политик информационной безопасности.

Следует отметить, что, несмотря на отраслевую направленность, рассматриваемый комплект стандартов может быть с успехом использован в любой другой организации.

**Ю.И. Иванченко,** *Научно-исследовательский институт прикладных проблем математики и информатики БГУ, зав. научно-исследовательской лабораторией прикладной информатики, кандидат технических наук*

Библиография

1. Банковский кодекс Республики Беларусь N 441-З от 25 октября 2000 г.
2. Закон Республики Беларусь N 455-З от 10 ноября 2008 г. «Об информации, информатизации и защите информации». В ред. Закона Республики Беларусь № 102-З от 4 января 2014 г. «О внесении изменений и дополнений в Закон Республики Беларусь «Об информации, информатизации и защите информации»».

9571

1. «персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо» [↑](#footnote-ref-1)