Михаил ЛЕВАШОВ, зам. генерального директора группы «Инфосекьюрити»

Стандарт Банка России или ГОСТ?

Новые механизмы обеспечения информационной безопасности банков

В данной статье мы рассмотрим организационные и законодательные методики для реализации выполнения требований Банка России в области обеспечения информационной безопасности банковской системы РФ.

Техническое регулирование и стандарты

Техническое регулирование отношений, возникающих при разработке, принятии, применении и исполнении обязательных требований (а также при применении и исполнении требований на добровольной основе) к продукции и услугам в различных отраслях хозяйственной деятельности, осуществляется с использованием Федерального закона от 27.12.02 № 184-ФЗ «О техническом регулировании» (далее — закон № 184-ФЗ). При этом часть видов хозяйственной деятельности полностью выведена из-под действия этого закона, для другой части действует особый порядок применения. Особый порядок относится и к защите конфиденциальной информации ограниченного в соответствии с законодательством РФ доступа (ст. 5 закона № 184-ФЗ). В отношении подобной информации обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные государственными заказчиками, а также *федеральными органами исполнительной власти, уполномоченными в области защиты информации. При этом особенности технического регулирования защиты информации ограниченного доступа устанавливаются Президентом и Правительством РФ в соответствии с их полномочиями*.

В соответствии с законом № 184-ФЗ обязательные для исполнения требования к продукции и услугам содержатся в технических регламентах. Необязательные требования содержатся в стандартах различных уровней и лучших практиках. Стандарты бывают разных типов. В частности, это международные и национальные стандарты, региональные стандарты и стандарты организаций. В своё время были (по поручению Правительства РФ) попытки разработки технического регламента по защите информации, но в силу разных причин от этого пришлось отказаться. Таким образом, регулирующими документами в данной отрасли остались стандарты. Необязательность их исполнения компенсировалась различными способами. Это отдельные требования международных карточных платёжных систем (относятся к стандарту PCI DSS), добровольное принятие банками комплекса стандартов Банка России СТО БР ИББС, Положение Банка России № 382-П, подготовленное с учётом требований стандарта СТО БР ИББС, и др.

Пункт 8 статьи 7 закона № 184-ФЗ предоставляет разработчикам технических регламентов и других обязательных к исполнению нормативных актов возможность использовать международные и национальные стандарты (полностью или частично) в качестве основы для таких разработок. Кроме того, Федеральный закон от 29.06.15 № 162-ФЗ «О стандартизации в Российской Федерации» (далее — закон № 162-ФЗ) в статье 27 детально описывает возможность и механизмы применения ссылок на национальные стандарты в нормативных правовых актах (предприятий, отраслей и др.):

«— *нормативные правовые акты могут содержать ссылки на официально опубликованные национальные стандарты…*

— *ссылки на национальные стандарты в нормативных правовых актах применяются путём приведения в них наименования и обозначения национальных стандартов с указанием даты утверждения и даты регистрации, пунктов, разделов национальных стандартов».*

Закон о техническом регулировании указывает также информационную систему, где можно найти стандарты и технические регламенты. Это (ст. 44) Федеральный информационный фонд технических регламентов и стандартов.

После того как предприятие (организация) начало выпускать продукцию (предоставлять услуги), удовлетворяющие требованиям соответствующих технических регламентов, стандартов либо подготовленных на их основе внутренних нормативно-правовых актов, естественно, возникает вопрос о подтверждении соответствия. Закон № 184-ФЗ определяет формы этого действия: «*Подтверждение соответствия на территории РФ может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации. Обязательное подтверждение соответствия осуществляется в формах:*

— *принятия декларации о соответствии…*

— *обязательной сертификации.*

Добровольное подтверждение соответствия (статья 21) осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации.

Обязательное подтверждение соответствия (статья 21)… проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента… Форма и схемы обязательного подтверждения соответствия могут устанавливаться

только техническим регламентом с учётом степени риска недостижения целей технических регламентов».

Это общий порядок, который в отношении работ и услуг по защите информации ограниченного в соответствии с федеральным законодательством пользования может быть скорректирован решениями Правительства РФ и (или) исполнительными органами, регулирующими эту отрасль.

Банковское регулирование

Полноценное и систематическое регулирование уровня обеспечения информационной безопасности в банковской системе РФ началось с появлением комплекса стандартов Банка России СТО БР ИББС. В статусе стандарта организации этот комплекс вобрал в себя самые известные международные стандарты и лучшие практики обеспечения безопасности информационных технологий, а также российские рекомендации. Применённые к специфике банковской деятельности в целом и к банковским информационным технологиям в частности, они позволили создать полноценный набор рекомендаций по обеспечению информационной безопасности всех российских банков.

По сути, единственным вопросом, который оставался длительное время нерешённым, являлся вопрос об обязательности исполнения банками требований банковского стандарта. Этот вопрос пытались решить по-разному. Вначале были попытки подготовить соответствующий технический регламент. Затем, после отказа от этой идеи в соответствии с отредактированным федеральным законом о техническом регулировании, вышел ряд нормативных документов на уровне Правительства РФ. В Банке России в отношении переводов денежных средств также были изданы обязательные для выполнения документы, основные из которых приведены в приложении к письму Банка России от 13.08.13 № 157-Т «О методических рекомендациях по проведению проверок операторов по переводу денежных средств, операторов платёжных систем, операторов услуг платёжной инфраструктуры при осуществлении Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». Среди этих документов:

- Положение Банка России от 09.06.12 № 382-П «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»;
- Положение Банка России от 09.06.12 № 381-П «О порядке осуществления надзора за соблюдением не являющимися кредитными организациями операторами платёжных систем, операторами услуг платёжной инфраструктуры требований Федерального закона от 27 июня 2011 года № 161-ФЗ „О национальной платёжной системе“, принятых в соответствии с ним нормативных актов Банка России»;
- Указание Банка России от 09.06.12 № 2831-У «Об отчётности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платёжных систем, операторов услуг платёжной инфраструктуры, операторов по переводу денежных средств».

Не прекращались попытки сделать комплекс стандартов СТО БР ИББС обязательным для исполнения всеми банками РФ. Вершиной достижений в этом направлении стало так называемое «письмо шести», в котором шесть государственных структур, регулирующих вопросы информационной безопасности и банковскую деятельность, согласовали текст рассматриваемого комплекса стандартов для его безусловного выполнения в банках. Однако все эти попытки не увенчались успехом. Стандарт оставался стандартом в определении федерального закона о техническом регулировании и поэтому не мог являться обязательным для исполнения. Затем было найдено красивое и простое решение проблемы. Банкам настойчиво предложили ввести у себя этот комплекс внутрибанковским нормативным документом и исполнять как обязательный акт. Это решение оказалось более жизнеспособным. Почти половина всех банков РФ ввели в действие этот стандарт таким способом.

Хотя указанное выше решение и было легитимным, но эта легитимность исходила от инициативы банков. Они в любой момент могли отказаться от выполнения этого комплекса. В настоящее время наряду с продолжением развития направления стандартизации вопросов банковской информационной безопасности в форме актуализации комплекса стандартов организации СТО БР Банк России расширяет практику издания обязательных для исполнения внутренних документов (положений, указаний и т. д.), в которых присутствуют многочисленные технические и организационные детали, обеспечивающие информационную безопасность.

Эти детали существенно отягощают внутрибанковские документы и приводят к необходимости их периодического пересмотра — так, указанные детали периодически меняются. Изменения диктуются непрерывным развитием и совершенствованием угроз нарушений банковской информационной безопасности, которым необходимо противостоять.

Поэтому для того, чтобы избавить такие документы от технических деталей, Банк России приступил к реализации идеи, основанной на приведённом выше законе № 162-ФЗ (ст. 27), который даёт банку возможность делать в своих положениях и указаниях прямые ссылки на пункты и разделы национальных стандартов (ГОСТов). С этой целью начата разработка ГОСТа, содержащего базовый уровень информационной безопасности. Естественно, основу этого национального стандарта составляет комплекс СТО БР ИББС. Выход этого стандарта ожидается в 2017 году. ■