Выгодно ли принять Стандарт Банка России

по информационной безопасности?

*«С целью выполнения в организациях банковской системы Российской Федерации (далее - БС РФ) требований Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее – Федеральный закон "О персональных данных")* ***Центральный банк Российской Федерации*** *при участии Ассоциации российских банков (далее - АРБ) и Ассоциации региональных банков России (Ассоциации «Россия»)* ***разработал отраслевые документы по приведению деятельности организаций БС РФ в соответствие с требованиями законодательства в области персональных данных****».*

ПИСЬМО ШЕСТЕРЫХ
(Банк России, Ассоциация российских банков, ФСТЭК России, Роскомнадзор, ФСБ и АРБР)*.*

В связи с выходом новых Стандартов Банка России по информационной безопасности (СТО БР ИББС), включающих требования по защите персональных данных (далее – ПДн), а также рекомендаций в области стандартизации, перед кредитными организациями встает вопрос: «В каком направлении двигаться: СТО БР, ISO? Как достичь соответствия требованиям федерального законодательства по защите ПДн? Как минимизировать расходы на соответствие?»

Целью данной статьи является разъяснение преимуществ и недостатков выполнения работ по защите ПДн в рамках СТО БР ИББС.

**Почему стандарт стал палочкой-выручалочкой? Основная часть**

Принятый летом 2006 года Федеральный закон «О персональных данных» (ФЗ № 152) поначалу не вызвал широкого резонанса. Этот документ воспринимали как один из нормативных документов, сравнимый по значимости с законом «Об информации, информатизации и защите информации»: «Закон важный, нужный, и во многом непонятный, но повода для паники нет, тем более что на уровне федеральных законов редко появляются принципиально новые требования, особенно в сфере ИТ». Так что документ оказался почти незамеченным.

Как тему информационной безопасности, ФЗ № 152 стали воспринимать только после подписания Постановления правительства РФ №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в ИСПДн» от 17 ноября 2007 г.№ 781. Именно в этот момент ИТ-рынок проявил первую негативную реакцию. Дело в том, что указанный документ носит явный технический характер и является обязательным для исполнения всеми операторами ПДн.

Отметим, что на волне защиты ПДн, рынок услуг информационной безопасности за 2008-2010 годы показал рост в размере 20-30%, при том, что рынок всего ИТ-консалтинга за эти кризисные годы показал падение более чем на 50%. Данный факт, безусловно, является хорошей новостью для рынка информационной безопасности. Однако здесь присутствуют свои НО.

Подавляющее большинство созданных систем защиты ПДн в рамках руководящих документов регуляторов (ФСТЭК, ФСБ) оказываются неэффективными. Причин здесь несколько:

1. Существующие документы ФСТЭК и ФСБ разрабатывались без учета работающих в организациях бизнес-процессов и технологий, а также практически переписывались с требований по защите государственной таны.
2. Согласно документам регуляторов, защиту ПДн необходимо организовывать почти во всех информационных системах (ИС) компании (везде, где обрабатываются ПДн, независимо от целей создания ИС).
3. Во все системы нужно внедрять сертифицированные средства защиты, которые далеко не всегда оказываются действительно эффективными, в тоже время, средства защиты, удовлетворяющие требованиям бизнеса остаются «за бортом».
4. Ну и самое главное, защита ПДн в рамках действующего подхода ФСТЭК в кредитных организациях превращается дорогой, трудоемкий и длительный процесс, не учитывающий реалий бизнеса.

**Как результат, ценность проекта по защите ПДн для бизнеса становится минимальной.**

На этом фоне новая версия СТО БР ИББС – безусловно успешная попытка Банка России вернуть рискоориентированный подход к процессу обеспечения информационной безопасности в кредитные организации, призванная значительно облегчить жизнь последним в части решения вопроса по защите ПДн.

Участники рынка очень долго ждали новой версии Стандарта Банка России включающего требования по защите персональных данных. Первоначально согласование планировалось до 15 апреля, но по ряду причин работа затянулась. И вот теперь **«Комплекс БР ИББС» окончательно согласован с ФСТЭК, ФСБ и Роскомнадзором**.

На самом деле, выход новой версии СТО БР ИББС является знаковым событием, т.к. теперь **банковское сообщество получило адаптированные для применения в банковской системе РФ методические рекомендации по защите** ПДн. Требования по защите ПДн в рамках СТО БР ИББС стали более понятными, по сравнению с общими требованиями ФСБ и ФСТЭК.

Теперь перед кредитными организациями стоит вопрос выбора одного из двух вариантов:

1. Вводить СТО БР ИББС в организации в качестве обязательного, что позволит защищать ПДн в разрезе требований стандарта. Однако принятие стандарта подразумевает планирование работы по планомерному внедрению других требований стандарта.
2. Не вводить СТО БР ИББС и выполнять требования по защите ПДн в соответствии с методическими рекомендациями ФСБ, ФСТЭК и Роскомнадзора на общих с остальными операторами основаниях.

**По мнению авторов, выбор очевиден, нужно вводить СТО БР ИББС и двигаться в направлении достижения соответствия его требованиям и рекомендациям, т.е. проводить планомерную работу по приведению в соответствие.**

Почему? Ниже мы раскроем нашу позицию, а для этого необходимо ответить на ряд вопросов:

* Что получает кредитно-финансовое учреждение, если вводит у себя СТО БР ИББС в качестве обязательного?
* Что проще для компании с точки зрения изменения подходов к защите информации: переход с ISO 27001 на СТО БР ИББС, или совместное выполнение требований и ISO 27001 и 152-ФЗ.
* Чем будут отличаться подходы к взаимодействию с регуляторами в рамках проведения проверочных мероприятий или обработки жалоб субъектов ПДн при применении СТО БР и 152-ФЗ соответственно?
* Зачем вводить стандарт Банка России СТО БР ИББС в качестве обязательного к выполнению, если полное соответствие ему намного дороже, чем выполнение требований в части защиты ПДн при общем подходе ФСТЭК и ФСБ?

**Что получает кредитно-финансовое учреждение, если вводит у себя СТО БР ИББС в качестве обязательного?**

Всем хорошо известно, что стоимость реализации тех или иных требований прямо зависит от величины границ области внедрения, т.е. в нашем случае от размеров и количества автоматизированных систем в которых есть ПДн. Основные затраты при проведении проекта по защите ПДн появляются на стадии покупки и внедрения технических решений.

Руководствуясь рекомендациями СТО БР ИББС, возможно значительно минимизировать количество информационных систем, относящихся к ИСПДн, тем самым уменьшить расходы на внедрение технических решений.

Остановимся на этом подробнее.

Согласно «Методическим рекомендациям по выполнению законодательных требований при обработке ПДн в организациях банковской системы Российской Федерации» **(**<http://www.cbr.ru/credit/Gubzi_docs/recommendations.pdf>**)**, **если вы защищаете систему, в которой присутствует, например, банковская тайна, то защищать нужно не по требованиям защиты ПДн, а по требованиям защиты банковской тайны**. В этом положении и заключаются основные преимущества защиты ПДн по требованиям СТО БР ИББС.

Раскроем эту позицию.



По стандарту, **Банковские технологические процессы** можно разделить на 2 типа:

* **Банковские платежные технологические процессы;**
* **Банковские информационные технологические процессы.**
1. **Банковские платежные технологические процессы:**

Согласно Стандарту **Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»** **(СТО БР ИББС-1.0-2010)** (<http://www.cbr.ru/credit/Gubzi_docs/st-10-10.pdf>), *«АБС, реализующие банковские платежные технологические процессы, не относятся к ИСПДн».* Другими словами, если автоматизированная банковская система реализует банковский платежный технологический процесс, то она не относится к ИСПДн.

1. **Банковские информационные технологические процессы:**

Можно разделить на:

* 1. **процессы в которых не обрабатываются ПДн**;
	2. **процессы в которых обрабатываются ПДн.**

В первом случае система не относится к ИСПДн по определению.

Во втором случае разделение на ИСПДн и «неИСПДн» происходит в зависимости от целей создания системы, если таковой является обработка персональных данных, то это ИСПДн, если же автоматизированная банковская система содержит персональные данные, но помимо них присутствует информация, защищаемая в соответствии с требованиями составляющими банковскую тайну, коммерческую тайну и др., то защищать нужно не по требованиям защиты персональных данных, а по требованиям конкретного вида тайны.

В результате, по требованиям ФСТЭК нужно защищать очень немногие автоматизированные банковские системы (порядка 20% от тех систем, который необходимо защитить не идя по СТО БР ИББС). Следовательно затраты на технические средства будут значительно ниже. Учитывая, что затраты на закупку сертифицированных средств защиты являются основными в проектах по защите персональных данных, то и стоимость всего проекта становится значительно ниже.

**Что проще для компании с точки зрения изменения подходов к защите информации: переход с ISO 27001 на СТО БР ИББС, или совместное выполнение требований ISO 27001 и 152-ФЗ.**

СТО БР ИББС был разработан с учетом основных отечественных и зарубежных стандартов в этой сфере. Его цель - обеспечить повышение доверия ко всей банковской системе РФ посредством установки единых требований по обеспечению ИБ кредитных организаций.

СТО БР ИББС разработан на основе ISO 27001 и является преломлением лучшего мирового и отечественного опыта в сфере управления информационной безопасностью. Поэтому он никак не идет вразрез с международными стандартами по информационной безопасности, в том числе ISO 27001. Таким образом, если в кредитной организации принят ISO 27001, то можно считать, что средства, затраченные на его внедрение, потрачены, в том числе и на соответствие СТО БР ИББС. Связка ISO 27001 + СТО БР ИББС организуется значительно проще и дешевле, чем ISO 27001 + ПДн.

**Зачем вводить стандарт Банка России СТО БР ИББС в качестве обязательного к выполнению, если соответствие ему намного дороже, чем выполнение требований и рекомендаций ФСБ и ФСТЭК в части защиты ПДн?**

Во время бесед с представителями кредитных организаций нам часто задают этот вопрос.

Заметим, что Банк России прекрасно понимает, что лишь небольшой процент кредитных организаций достиг рекомендуемого стандартом четвертого уровня соответствия. Поэтому, на наш взгляд, введение стандарта необходимо позиционировать как выбор вектора движения или расстановку приоритетов.

Ведь информационная безопасность – прежде всего процесс, которым необходимо управлять. Стандарт предлагает процессный подход – построение непрерывного циклического процесса обеспечения ИБ, предполагающего как планирование, так и управление.

Нельзя говорить о том, что банк, даже потратив значительные инвестиции, в одночасье достигнет соответствия. Построение системы обеспечения информационной безопасности (СОИБ) не должно рассматриваться как разработка регламентов и внедрение технических средств. Построение СОИБ стоит рассматривать как построение процессов, включающих техническую, технологическую и организационную стороны. А инвестиции на построение таких процессов, несомненно, будут растянуты во времени.

Кроме того, внедряя СТО БР ИББС, банк решает массу сопутствующих задач по информационной безопасности (так, например, требования по безопасности к участникам Банковских Электронных Срочных Платежей также найдут свое отражение в стандарте).

Поэтому выбирая СТО БР ИББС как вектор развития информационной безопасности, кредитная организация выигрывает как с точки зрения тактики (решая вставшую остро проблему защиты ПДн), так и с точки зрения стратегии (экономя на решении последующих задач информационной безопасности).

Е.Царев

М.Плахута