КонсалтИнфоМенеджмент

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург,
ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64

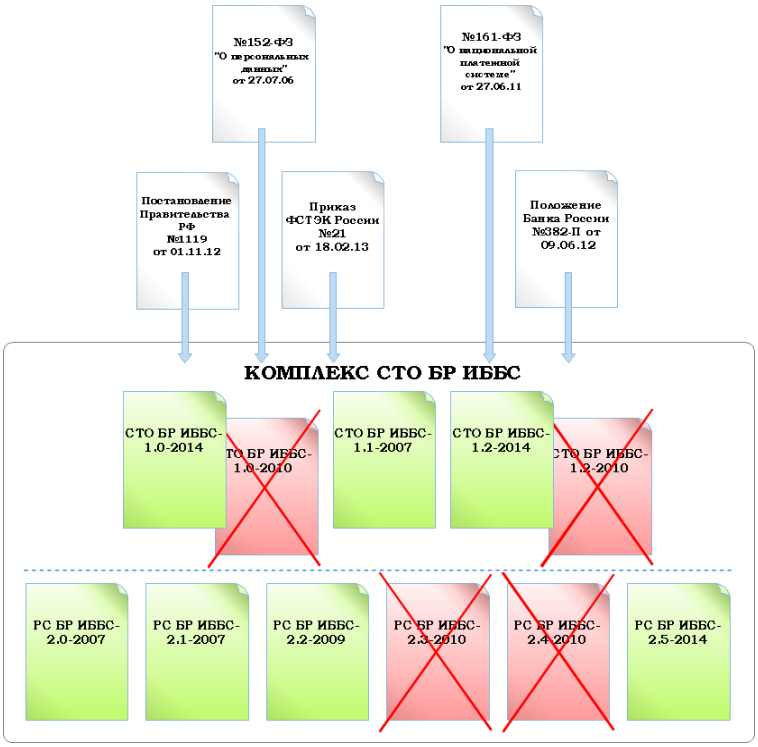
ОБЗОР ИЗМЕНЕНИЙ В КОМПЛЕКСЕ СТО БР ИББС

17 мая 2014 года распоряжениями Банка России от № Р-399 и № Р-400 с 1 июня 2014 года введены в действие новые редакции документов из комплекса стандартов Банка России по обеспечению информационной безопасности (СТО БР ИББС), а также отменены ранее действующие версии соответствующих документов.

Предпосылки

Необходимость приведения комплекса стандартов СТО БР ИББС в соответствие актуальным требованиям к обеспечению защиты информации привела к выпуску Банком России новых версий стандартов СТО БР ИББС-1.0 и СТО БР ИББС-1.2.

Данные изменения позволили гармонизировать Стандарт СТО БР ИББС-1.0 с требованиями Банка России к обеспечению защиты информации при осуществлении переводов денежных средств (Положение Банка России от 09.06.2012 г. №382-П, далее – Положение №382-П), текущими требованиями законодательства в сфере обработки и защиты персональных данных (Федеральный закон РФ от 27.07. 2006 г. №152-ФЗ, Постановление Правительства РФ от 01.11.2012 г. №1119, далее - №152-ФЗ, ПП №1119), а также требованиями к обеспечению защиты персональных данных при их обработке в информационных системах персональных данных ФСТЭК России (Приказ ФСТЭК России от 18.02.2013 г. №21, далее – Приказ №21).



Что изменилось

Значительно доработан раздел 7 Стандарта СТО БР ИББС-1.0, определяющий подход к построению системы информационной безопасности организаций банковской системы РФ. Раздел 8 Стандарта, определяющий требования к системе менеджмента информационной безопасности, был изменен в наименьшей степени.

Большая часть изменений была заимствована из аналогичных требований к направлениям деятельности по обеспечению информационной безопасности Положения №382-П и Приказа №21 и, в основной массе, расширила и дополнила уже существующие требования СТО БР ИББС-1.0-2010.

	СТО БР ИББС-1.2-2010	СТО БР ИББС-1.2-2014
Общее количество частных показателей	**423**	**491** (+68)
По направлениям оценки:		
требований	**EV1**	**EV2**	**EV3**
осталось неизменными	147 (59%)	139 (87%)	76 (94%)
изменение (ужесточение) формулировки	31 (12%)	14 (9%)	3 (4%)
новых	72 (29%)	7 (4%)	2 (2%)

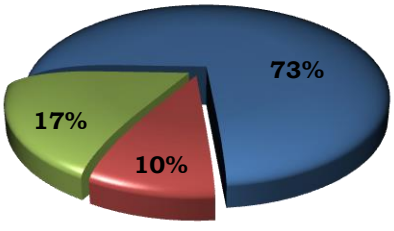
Формулировки многих требований были скорректированы и приведены к общему виду. Так, большинство процедур обеспечения безопасности теперь предполагают документирование, выполнение, регистрацию и контроль их выполнения.

Часть требований СТО БР ИББС-1.0, носивших ранее рекомендованный характер, в новой версии Стандарта стала обязательной к выполнению.

К наиболее существенным требованиям, появившимся в новой версии СТО БР ИББС-1.0, или ставшим обязательными, можно отнести:

- требования к учету и обращению носителей защищаемой информации;
- требования к выделению сегментов локальной вычислительной сети в зависимости от реализуемых банковских технологических процессов;
- требования к контролю конфигураций средств межсетевого экранирования;
- требования к использованию специализированных средств анализа событий безопасности;
- требования к контролю отсутствия уязвимостей в оборудовании и программном обеспечении.

Изменения в СТО БР ИББС-1.2-2014



КонсалтИнфоМенеджмент

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург,
ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64

Персональные данные

Изменения и дополнения в СТО БР ИББС-1.0-2014 позволили в рамках Стандарта в полной мере отразить требования законодательства РФ к организации процессов обработки персональных данных и частично определить требования к процессам обработки и защиты персональных данных в информационных системах персональных данных. Так, выполнение требований разделов 7 и 8 Стандарта рекомендуется для выполнения требований к защите персональных данных для третьего и четвертого уровня защищенности персональных данных при их обработке в информационных системах персональных данных. Обязанность по определению критериев отнесения автоматизированных банковских систем (далее – АБС) к информационным системам персональных данных лежит на организации БС РФ. АБС (ИСПДн), участвующие в банковском платежном технологическом процессе, до сих пор требуют реализации только требований СТО БР ИББС-1.0. Для остальных АБС (ИСПДн) организации БС РФ по результатам моделирования угроз информационной безопасности и определения необходимого уровня защищенности в соответствии с требованиями ПП №1119 могут применяться дополнительные защитные меры, в том числе, определенные Приказом №21. Следует отметить, что во время подготовки данного материала, документ, аналогичный «письму шести», подтверждающий признание регуляторами СТО БР ИББС-1.0-2014 в качестве общего подхода к защите информации, в том числе персональных данных, в организациях БС РФ, опубликован не был.

Новые РС БР ИББС

Решениями Банка России также были введены в действие рекомендации в области стандартизации РС БР ИББС-2.5 «Менеджмент инцидентов информационной безопасности». Кроме того, в скором времени будет опубликован документ РС БР ИББС-2.x «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».

Изменения состава рекомендаций к защите персональных данных

Наряду с вводом в действие новых версий стандартов, было отменено распоряжение Банка России от 21 июня 2010 года № Р-705 и документы РС БР ИББС-2.3-2010 и РС БР ИББС-2.4-2010, определяющие требования к защите персональных данных при их обработке в информационных системах персональных данных и отраслевую модель угроз безопасности персональных данных соответственно.

Новая версия документа РС БР ИББС-2.4 «Отраслевая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» Банком России разработана и сейчас находится на стадии согласования с ФСТЭК России и ФСБ России.

Положение №382-П

СТО БР ИББС-1.0-2014 был адаптирован с учетом необходимости реализации требований Положения №382-П и дополнен аналогичными требованиями таким образом, чтобы реализация требований СТО БР ИББС-1.0-2014 по направлению защиты банковских платежных технологических процессов и построения системы менеджмента информационной безопасности позволила выполнить требования Положения №382-П. Так, Приложение В Стандарта СТО БР ИББС-1.2-2014 содержит таблицу соответствия требований СТО БР ИББС-1.0-2014 и требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в Приложении 2 к Положению №382-П.

Новая методика оценки соответствия

Существенные изменения затронули Стандарт СТО БР ИББС-1.2 и методику оценки соответствия требованиям СТО БР ИББС-1.0. Аналогично методике оценки соответствия, приведенной в Приложении 1 к Положению №382-П, в новой версии СТО БР ИББС-1.2:

- для каждого частного показателя однозначно определена категория проверки (документирование и выполнение, документирование, выполнение);
- вводятся корректирующие коэффициенты, значение которых зависит от количества частных показателей, которые полностью не выполняются (значение которых равно «нулю»);
- большое внимание уделяется **документированию** процессов обеспечения информационной безопасности и результатов их выполнения, подтверждению наличия в финансовой организации последовательного и системного подхода к обеспечению информационной безопасности;
- невыполнение даже одного частного показателя теперь приводит к значительному снижению общей оценки соответствия по направлению обеспечения информационной безопасности за счет корректирующего коэффициента.

Следует отметить, что в соответствии с СТО БР ИББС-1.2, оценка выполнения частных показателей по обеспечению информационной безопасности банковских платежных технологических процессов должна производиться **с учетом** оценки выполнения аналогичных требований, полученных в ходе проведения оценки соответствия Положению №382-П.

Резюме

Для организации БС РФ, начавших внедрять СТО БР ИББС-1.0-2010, приводить систему обеспечения информационной безопасности в соответствие требованиям Положения №382-П, а также реализовавшим необходимый комплекс мероприятий по организации обработки персональных данных, нововведения в комплексе СТО БР ИББС не будут существенно влиять на реализуемые процессы обеспечения информационной безопасности и результаты оценки их соответствия требованиям стандарта СТО БР ИББС-1.0-2014.

КонсалтИнфоМенеджмент

ООО «КиМ», www.km-ltd.ru, info@km-ltd.com
197375, г. Санкт-Петербург,
ул. Вербная, д. 27, оф. 817
Тел. (812) 309-36-64

В качестве подтверждения приведенного выше заключения, ниже приведена таблица, содержащая реальные оценки соответствия требованиям СТО БР ИББС-1.0-2010 и СТО БР ИББС-1.0-2014, полученные в ходе практической реализации компанией КонсалтИнфоМенеджмент комплекса мероприятий по модернизации СОИБ одного из банков-клиентов, направленного на выполнение требований Стандарта Банка России СТО БР ИББС-1.0 и Положения Банка России от 09.06.12 №382-П в соответствии с базовым уровнем услуг.

СТО БР ИББС				**Положение №382-П**	
Обозначения показателя	**Наименование показателя**	**СТО БР ИББС-1.0-2010**	**СТО БР ИББС-1.0-2014**	**Обозначения показателя**	**Положение №382-П**
EV1	Оценка текущего уровня информационной безопасности	0,62	0,5[1]	**$EV1_{пс}$**	0,73
EV2	Оценка менеджмента информационной безопасности	0,6	0,51	**$EV2_{пс}$**	0,71
EV3	Оценка уровня осознания информационной безопасности	0,65	0,55		
Итоговое значение степени выполнения требований					
R	Итоговое значение степени выполнения требований СТО БР ИББС-1.0-2014	0,6 (2 уровень)	0,5 (2 уровень)	**$R_{пс}$**	0,71 (удовлетворительно)

Сведения о составе и содержании указанного (типового) комплекса мероприятий, соответствующего базовому уровню услуг, реализуемых компанией КонсалтИнфоМенеджмент, по внедрению СТО БР ИББС-1.0-2014, целях проекта и особенностях его реализации, могут быть предоставлены по запросу, направленному на адрес нашей электронной почты: info@km-ltd.com.

Консультации по вопросам, связанным с модернизацией СОИБ, реализацией требований СТО БР ИББС и Положения №382-П Вы можете получить, связавшись с нашими сотрудниками по телефону (812) 309-36-64.

[1] Оценка соответствия требованиям СТО БР ИББС-1.0-2014 по направлению банковских информационных технологических процессов.