



Комплекс Стандарта Банка России: перспективы модернизации и развития.

**Выборнов А.О.,
начальник отдела
Главного управления
безопасности и
защиты информации,
Банк России.**



Основная цель пересмотра документов Комплекса БР ИББС :

Гармонизация:

1. С действующим законодательством Российской Федерации в области защиты персональных данных, в частности Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
2. Гармонизация с действующей редакцией Положения Банка России от 9 июня 2012 года № 382-П.



Новые версии документов Комплекса БР ИББС включают в себя следующие изменения:

- пересмотр 7-го раздела действующей редакции Стандарта Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;
- включение в состав действующей редакции Стандарта Банка России СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» таблицы соответствия частных показателей методики оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 и требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в приложении 2 к Положению Банка России от 09 июня 2012 года №382-П;
- исключение из состава действующей редакции Стандарта Банка России СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0» весовых коэффициентов частных показателей.



Цель установления рекомендаций:

Выполнение задач по принятию мер к обеспечению ИБ на стадиях жизненного цикла автоматизированных банковских систем для установления доверия к реализации обеспечения ИБ в АБС

Проект рекомендаций в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем»



Проект рекомендаций устанавливает следующие положения:

- по организации работ на этапах жизненного цикла автоматизированных банковских систем, в том числе обеспечивающей возможность контроля с целью установления доверия к проведению указанных работ и, соответственно, доверия к реализации обеспечения ИБ в автоматизированных банковских системах;
- по составу типовых недостатков в реализации требований к обеспечению ИБ в автоматизированных банковских системах, создающих условия для возникновения недопустимых рисков нарушения ИБ при эксплуатации автоматизированных банковских систем;
- по составу, содержанию и порядку проведения работ по анализу исходного кода программного обеспечения автоматизированных банковских систем, оценке защищенности автоматизированных банковских систем и по контролю параметров настроек технических защитных мер.



Цель установления рекомендаций:

Определение подходов к реализации организацией БС РФ процесса обнаружения и реагирования на инциденты ИБ для снижения степени тяжести последствий от нарушений ИБ

Проект рекомендаций в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности»



Проект рекомендаций устанавливает следующие положения:

- Рекомендации по планированию в рамках системы менеджмента инцидентов ИБ, в числе которых, среди прочего, установлены рекомендации:
 - к разработке документационного обеспечения;
 - к определению организационной структуры;
 - к определению ролей процесса реагирования на инциденты ИБ (формирование ГРИИБ);
 - по выбору технических средств;
 - по осуществлению контроля за выполнением установленных процессов;
- Рекомендации по реализации в рамках системы менеджмента инцидентов ИБ;
- Рекомендации по анализу в рамках системы менеджмента инцидентов ИБ;
- Рекомендации к классификации инцидентов ИБ и использованию классификатора инцидентов ИБ в процессе их обработки;



Цель установления рекомендаций:

Выполнение задач по организации планирования и контроля эффективности ресурсов, необходимых для реализации и эксплуатации системы обеспечения ИБ. Обеспечение баланса между рисками, связанными с наличием уязвимостей в реализации процессов СОИБ, и ресурсными обеспечением ИБ, направленным на повышение зрелости процессов СОИБ и, соответственно, на снижение указанных рисков



Проект рекомендаций устанавливает следующие положения:

- рекомендации к определению потребностей в обеспечении системы обеспечения ИБ финансовыми средствами, включая рекомендации к шести уровням зрелости реализации процессов системы обеспечения ИБ;
- рекомендации к определению потребностей службы ИБ организации БС РФ в обеспечении кадровыми ресурсами, включая рекомендации к функциям службы ИБ, необходимых к обеспечению на каждом из уровней зрелости процессов системы обеспечения ИБ;
- рекомендации по контролю эффективности использования финансовых средств.

Рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации



Область применения:

- 1.** Создание и модернизация АБС организации БС РФ, реализующих технологию виртуализации;
- 2.** Создание и модернизация АБС организации БС РФ, функционирование которых организуется с использованием технологии виртуализации;
- 3.** Разработка технических заданий, технорабочих проектов и эксплуатационной документации на АБС организации БС РФ, реализующим технологию виртуализации.



Документ устанавливает рекомендации по:

- разделению потоков информации и изоляции виртуальных машин;
- обеспечению ИБ образов виртуальных машин;
- обеспечению ИБ серверных компонент виртуализации;
- обеспечению ИБ виртуальных машин;
- обеспечению ИБ АРМ пользователей (терминалов и персональных электронных вычислительных машин), используемых при реализации технологии виртуализации рабочих мест пользователей;
- мониторингу ИБ;
- составу ролей и разграничению полномочий эксплуатационного персонала;
- обеспечению ИБ СХД.



Спасибо за внимание!