РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.1-2007

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

РУКОВОДСТВО ПО САМООЦЕНКЕ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0

Дата введения: 2007-05-01

Москва
2007

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 28 апреля 2007 года № Р-347.

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение 4
1. Область применения 5
2. Нормативные ссылки 5
3. Термины и определения 5
4. Самооценка соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 6
5. Порядок проведения самооценки информационной безопасности организаций банковской системы Российской Федерации 8
5.1. Подготовка к проведению самооценки информационной безопасности 8
5.2. Анализ документов 9
5.3. Проведение самооценки информационной безопасности на месте 10
5.4. Подготовка и рассылка отчета с результатами самооценки информационной безопасности 10
Приложение А. Форма листов для сбора свидетельств самооценки информационной безопасности 11
Приложение Б. Документы, рекомендуемые в качестве источников свидетельств самооценки информационной безопасности организации БС РФ 12

Введение

Стандартом Банка России СТО БР ИББС-1.0-2006 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) с целью проверки уровня информационной безопасности (ИБ) как самого Банка России, так и организаций банковской системы (БС) Российской Федерации (РФ) определенно требование проведения регулярной самооценки ИБ.

Самооценка соответствия информационной безопасности организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 должна проводиться в соответствии со стандартом 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-1.0-2006”.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

РУКОВОДСТВО ПО САМООЦЕНКЕ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0

Дата введения: 2007-05-01

1. Область применения

Настоящее руководство распространяется на организации БС РФ, проводящие самооценку соответствия информационной безопасности (ИБ) требованиям СТО БР ИББС-1.0 и устанавливает подходы к проведению указанной самооценки.

Настоящее руководство рекомендовано для применения путем прямого использования устанавливаемых в нем положений при проведении самооценки ИБ в организациях БС РФ. Самооценка ИБ проводится собственными силами и по инициативе руководства организации.

Положения настоящего руководства применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена действующим законодательством Российской Федерации, нормативным актом Банка России или условиями договора.

2. Нормативные ссылки

В настоящем руководстве использованы нормативные ссылки на следующие стандарты:

СТО БР ИББС-1.0

СТО БР ИББС-1.1-2007 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности”

СТО БР ИББС-1.2-2007 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006”

3. Термины и определения

В настоящем руководстве применены термины в соответствии со стандартами СТО БР ИББС-1.0, СТО БР ИББС-1.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности” и 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-1.0-2006” (далее — Методика).

4. Самооценка соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0

4.1. Самооценка соответствия ИБ организаций БС РФ требованиям СТО БР ИББС-1.0 проводится согласно Методике по направлениям оценки:

— текущий уровень ИБ организации;
— менеджмент ИБ организации;
— уровень осознания ИБ организации.

4.2. При проведении самооценки соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 необходимо:

— ознакомиться с Методикой, в частности, с набором частных и групповых показателей ИБ, направлениями оценки, способом вычисления групповых показателей ИБ, способами вычисления оценок в рамках направлений и итогового уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0;
— провести определение набора частных показателей ИБ, попадающих в область самооценки;
— провести оценивание необходимых частных показателей ИБ;
— провести вычисление значений оценок групповых показателей ИБ, значений оценок в рамках направлений и итогового уровня соответствия ИБ.

4.3. Все частные показатели ИБ Методики должны быть оценены. Однако перед оцениванием частных показателей ИБ необходимо провести анализ актуальности требований ИБ, проверяемых частными показателями ИБ Методики, для основной или вспомогательной деятельности организации БС РФ. Неактуальным требование ИБ может быть признано только в том случае, если организация не занимается деятельностью, к которой данное требование ИБ имеет отношение. В этом случае соответствующие частные показатели определяются как неоцениваемые и не учитываются в формировании дальнейших результатов по самооценке.

4.4. Определение частного показателя как неоцениваемого может быть реализовано путем исключения частного показателя ИБ из числа оцениваемых, при этом необходимо выполнить процедуру пересчета коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя ИБ с сохранением степени их значимости на вычисляемое значение группового показателя ИБ.

При определении частного показателя ИБ как неоцениваемого должно быть подготовлено документально оформленное обоснование неактуальности указанного частного показателя ИБ для деятельности организации БС РФ.

4.5. Оценка частного показателя ИБ формируется на основании выявленной степени выполнения проверяемого требования посредством экспертного оценивания. Методика устанавливает следующую шкалу степени выполнения проверяемых требований:

— “нет” — оценке присваивается значение, равное нулю;
— “частично” — оценке присваивается значение 0,25; 0,5 или 0,75;
— “да” — оценке присваивается значение, равное единице.

4.6. Оценка частного показателя ИБ должна основываться на свидетельствах самооценки, в качестве основных источников которых рекомендуется использовать:

— нормативные документы проверяемой организации БС РФ и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации БС РФ;
— устные высказывания сотрудников проверяемой организации БС РФ в процессе проводимых опросов;
— результаты наблюдений проверяющих за деятельностью сотрудников организации БС РФ в области ИБ.

В процессе проведения устного опроса сотрудников проверяемой организации БС РФ и наблюдений за деятельностью указанных сотрудников члены проверяющей группы должны сделать вывод о степени соответствия оцениваемой деятельности требованиям нормативных документов проверяемой организации БС РФ.

Полученные свидетельства самооценки ИБ и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств самооценки ИБ, пример которых приведен в приложении А. При заполнении листов для сбора свидетельств самооценки

ИБ необходимо указать ссылки на соответствующие нормативные документы проверяемой организации БС РФ, результаты опроса сотрудников организации БС РФ, а также результаты наблюдений проверяющей группы. Результаты опроса и наблюдений должны быть подтверждены подписью опрашиваемого сотрудника организации БС РФ или члена проверяющей группы соответственно.

4.7. Для выявления степени выполнения требований ИБ при проведении оценки частных показателей рекомендуется использовать следующий общий подход:

Таблица 1. Рекомендуемые критерии выставления оценок частных показателей ИБ

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования, степень выполнения которых оценивается в частном показателе ИБ, не установлены во внутренних нормативных документах проверяемой организации БС РФ и не выполняются
0	Требования, степень выполнения которых оценивается в частном показателе ИБ, частично установлены в нормативных документах проверяемой организации БС РФ, но не выполняются
0,25	Требования, степень выполнения которых оценивается в частном показателе ИБ, полностью установлены в нормативных документах проверяемой организации БС РФ, но не выполняются
0,25	Требования, степень выполнения которых оценивается в частном показателе ИБ, не установлены во внутренних нормативных документах проверяемой организации БС РФ и выполняются в неполном объеме
0,25	Требования, степень выполнения которых оценивается в частном показателе ИБ, частично установлены во внутренних нормативных документах проверяемой организации БС РФ и выполняются в неполном объеме
0,5	Требования, степень выполнения которых оценивается в частном показателе ИБ, полностью установлены во внутренних нормативных документах проверяемой организации БС РФ и выполняются в неполном объеме
0,5	Требования, степень выполнения которых оценивается в частном показателе ИБ, не установлены во внутренних нормативных документах проверяемой организации БС РФ, но выполняются в полном объеме
0,75	Требования, степень выполнения которых оценивается в частном показателе ИБ, частично установлены во внутренних нормативных документах проверяемой организации БС РФ, но выполняются в полном объеме
1	Требования, степень выполнения которых оценивается в частном показателе ИБ, полностью установлены во внутренних нормативных документах проверяемой организации БС РФ и выполняются в полном объеме

4.8. В случае исключения всех частных показателей ИБ в пределах отдельного группового показателя ИБ необходимо исключить указанный групповой показатель ИБ из числа показателей, формирующих оценку в рамках направления, что отражается в корректировке формулы вычисления оценки в рамках направления Методики.

4.9. Для выполнения самооценки соответствия ИБ рекомендуется использовать Систему автоматизации процессов самооценки соответствия ИБ положениям и требованиям СТО БР ИББС-1.0, для чего необходимо ознакомиться с рекомендуемыми Банком России документами, содержащими общее описание и руководство пользователя указанной Системы.

4.10. По результатам проведения самооценки должен быть подготовлен отчет, содержащий:

- заполненные анкеты оценивания групповых показателей ИБ;
- документы, обосновывающие исключение частных показателей из области самооценки;
- заполненные листы для сбора свидетельств самооценки, подтверждающие выставленные оценки частных показателей ИБ;
- документы, содержащие результаты самооценки соответствия ИБ по направлениям оценки и итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0, а также круговую диаграмму оценивания групповых показателей ИБ, определенную и описанную в Методике.

4.11. Полученное по результатам самооценки значение итогового уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0, соответствующее интервалу от 0,85 до 1 включительно, является рекомендуемым Банком России.

5. Порядок проведения самооценки информационной безопасности организаций банковской системы Российской Федерации

В состав работ по проведению самооценки ИБ в организации БС РФ рекомендуется включать следующие этапы:

- подготовка к проведению самооценки ИБ;
- анализ документов;
- проведение самооценки ИБ на месте;
- подготовка и рассылка отчета с результатами самооценки ИБ.

5.1. Подготовка к проведению самооценки информационной безопасности

5.1.1. В рамках подготовки к проведению самооценки ИБ рекомендуется выполнить:

- формирование группы для проведения самооценки из числа сотрудников подразделения ИБ организации БС РФ;
- определение руководителя проверяющей группы;
- формирование плана проведении самооценки ИБ;
- установление ролей и обязанностей для выполнения и использования результатов самооценки ИБ;
- определение формы отчета с результатами самооценки ИБ.

5.1.2. При определении размера и состава группы для проведения самооценки ИБ (проверяющей группы) должна учитываться компетентность проверяющей группы, в основе которой лежит уровень квалификации ее участников. Если участники проверяющей группы не обладают необходимыми знаниями и опытом по специальным вопросам, то в группу включают технических экспертов. Технические эксперты должны работать под руководством участников проверяющей группы.

5.1.3. Если при рассмотрении результатов работы технического эксперта проверяющей группой выявляются существенные несоответствия между заключением эксперта и информацией (документами) проверяемого подразделения либо проверяющая группа считает, что выводы эксперта необоснованны, то проверяющей группе рекомендуется провести дополнительные процедуры, обеспечивающие проверку обоснованности заключения эксперта, или назначить другого эксперта.

5.1.4. Заключение технического эксперта рекомендуется включать в рабочие документы проверяющей группы. Если в исключительном случае технический эксперт дает устные разъяснения, то такие разъяснения должны быть отражены проверяющей группой в ее рабочих документах.

5.1.5. Использование работы технического эксперта при проведении самооценок ИБ не снимает ответственности за заключение с членов проверяющей группы.

5.1.6. В план проведения самооценки ИБ как минимум рекомендуется включать следующую информацию:

- цель самооценки ИБ;
- объекты и деятельность, подвергающиеся самооценке ИБ;
- даты и продолжительность проведения самооценки ИБ;
- распределение ролей среди членов проверяющей группы, связанных с анализом документов, проведением самооценки на месте и подготовкой и рассылкой отчета с результатами самооценки;
- порядок и сроки выполнения мероприятий по анализу документов;
- порядок и сроки выполнения мероприятий по проведению самооценки ИБ на месте;
- порядок и сроки выполнения мероприятий по подготовке и рассылке отчета с результатами самооценки ИБ.

Рекомендуется согласовать план проведения самооценки со всеми заинтересованными сторонами, а также утвердить его ответственным за процесс самооценки ИБ (из числа представителей высшего руководства организации БС РФ).

5.1.7. Члены проверяющей группы должны подготовить рабочие документы, необходимые для регистрации результатов самооценки ИБ. Рабочие документы должны храниться по крайней мере до окончания самооценки ИБ. Документы, содержащие конфиденциальную или частную информацию, должны храниться с соблюдением соответствующих требований безопасности.

В приложении А представлена рекомендуемая форма листов для сбора свидетельств самооценки ИБ. В листах должна отражаться информация, которая получена проверяющими при проведении самооценки ИБ с помощью различных методов получения свидетельства самооценки ИБ (при опросе, наблюдении за деятельностью и анализе выявленных нормативных документов).

5.1.8. Руководство организации БС РФ должно установить и обеспечить ресурсы для поддержки самооценки ИБ, включая определение лиц, ответственных за все аспекты самооценки ИБ, и соответствующую финансовую и инфраструктурную поддержку для обеспечения необходимых функций самооценки ИБ, таких, как сбор, анализ, хранение, сообщение и распределение данных.

5.1.9. Руководству организации БС РФ рекомендуется установить ответственного за процесс самооценки ИБ (из числа представителей высшего руководства), а также утвердить регламент проведения самооценки, в котором определить:

— порядок формирования, сбора и хранения свидетельств самооценки;
— периодичность проведения самооценки ИБ;
— порядок хранения и распространения результатов самооценки ИБ.

5.1.10. Для ответственного за процесс самооценки ИБ рекомендуется определить следующие обязанности:

— взаимодействовать с руководителями проверяемых подразделений для содействия самооценке ИБ;
— создавать возможности сбора данных для самооценки ИБ;
— назначать квалифицированный персонал для разработки и реализации плана самооценки ИБ;
— обеспечивать использование единого процесса по всей организации для процедур самооценки ИБ.

5.1.11. Самооценку ИБ рекомендуется предварить вступительным совещанием. Данное совещание с участием членов проверяющей группы и лиц, ответственных за проверяемые подразделения, подлежащие проверке, должно проводиться с целью изложения действий по проведению самооценки ИБ и согласования способов обмена информацией между проверяющей группой и представителями проверяемых подразделений. Председательствовать на совещании должен руководитель проверяющей группы.

Изложение действий по проведению самооценки ИБ заключается прежде всего в рассмотрении вопросов об источниках, методах получения и достоверности свидетельств самооценки ИБ, необходимых для оценивания частных показателей Методики.

5.1.12. В одних случаях вступительное совещание может просто состоять из сообщения, что будет проводиться самооценка ИБ, и разъяснения характера самооценки ИБ.

В других случаях на совещании рекомендуется выполнить:

— представление участников проверяющей группы, включая изложение их ролей;
— согласование графика проведения самооценки;
— ознакомление с методами и процедурами, используемыми при проведении самооценки ИБ;
— согласование способов обмена информацией между проверяющей группой и проверяемыми подразделениями организации БС РФ;
— согласование доступности ресурсов и оборудования, необходимых проверяющей группе;
— согласование принципов обеспечения конфиденциальности;
— ознакомление с формой составления отчета с результатами проведения самооценки ИБ;
— информирование о порядке рассмотрения замечаний проверяемых подразделений организации БС РФ по проведению или заключению по результатам самооценки ИБ.

5.2. Анализ документов

5.2.1. До проведения самооценки на месте проверяющей группой рекомендуется провести анализ необходимой документации, регламентирующей обеспечение ИБ в проверяемых подразделениях организации БС РФ для определения соответствия положений, отраженных в документации, требованиям СТО БР ИББС-1.0.

5.2.2. Анализ документов, выполняемый в процессе самооценки, производится с целью сбора свидетельств самооценки, позволяющих оценить значения частных показателей ИБ Методики.

Рекомендуемый перечень документов, необходимый членам проверяемой группы для анализа соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0, приведен в приложении Б.

5.2.3. Кроме перечисленных в приложении Б документов, на этапе анализа могут быть получены другие документы, содержащие свидетельства выполнения деятельности по обеспечению ИБ. Это могут быть:

— реестры и описи;
— регистрационные журналы;
— протоколы;
— приказы и распоряжения;
— акты;
— договоры;
— отчеты.

5.3. Проведение самооценки информационной безопасности на месте

5.3.1. Проведение самооценки ИБ на месте должно включать:

— сбор дополнительных свидетельств самооценки ИБ;
— оценку частных показателей ИБ Методики;
— проведение заключительного совещания.

5.3.2. Основными источниками свидетельств самооценки ИБ при проведении ИБ на месте являются:

— документы, которые по каким-либо причинам не были выявлены на этапе анализа документов и содержащие необходимые свидетельства самооценок ИБ;
— устные высказывания сотрудников проверяемых подразделений;
— результаты наблюдений членов проверяющей группы за деятельностью по реализации требований нормативных документов в области обеспечения ИБ.

5.3.3. На основании собранных свидетельств самооценки, зафиксированных в листах для сбора свидетельств самооценки, проверяющие формируют оценки частных показателей Методики.

5.3.4. По окончании этапа проведения самооценки ИБ на месте рекомендуется провести заключительное совещание с участием представителей проверяющей группы и проверяемых подразделений под председательством руководителя проверяющей группы.

На совещании должны быть представлены результаты оценивания по каждому из частных показателей Методики таким образом, чтобы они были понятны и признаны всеми заинтересованными лицами и подразделениями организации БС РФ. Любые разногласия по оцениванию частных показателей Методики должны быть обсуждены и по возможности разрешены. Если единое мнение не найдено, то это должно быть зафиксировано документально.

На совещании могут быть представлены рекомендации по повышению уровня ИБ.

5.4. Подготовка и рассылка отчета с результатами самооценки информационной безопасности

5.4.1. По результатам оценивания частных показателей ИБ Методики проверяющая группа должна провести оценку уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 и подготовить отчет самооценки ИБ. Помимо документов, определенных в пункте 4.10 настоящего руководства, отчет с результатами самооценки ИБ должен содержать:

— сведения об организации БС РФ, проводившей самооценку ИБ;
— сведения о руководителе и членах проверяющей группы;
— сроки проведения самооценки;
— краткое изложение процесса самооценки;
— любые неразрешенные разногласия;
— заявление о конфиденциальном характере содержания отчета с результатами самооценки ИБ;
— лист рассылки отчета с результатами самооценки ИБ.

Отчет с результатами самооценки ИБ должен быть утвержден ответственным за процесс самооценки ИБ (из числа представителей высшего руководства организации БС РФ).

5.4.2. Проверенный и приобретший окончательную форму отчет с результатами самооценки ИБ может быть распространен между всеми причастными сторонами, включая главу организации БС РФ, руководителей и сотрудников подразделения информационной безопасности и другие заинтересованные стороны.

Члены организации БС РФ должны иметь доступ к отчету с результатами самооценки ИБ в соответствии с принципом необходимого знания и имеющимися у них правами.

Может потребоваться распространить результаты самооценки ИБ среди внешних причастных сторон, включая органы регулирования, акционеров, клиентов и поставщиков.

Приложение А

Форма листов для сбора свидетельств самооценки информационной безопасности

Групповой показатель ИБ _____

Обозначение частного показателя ИБ	Источники свидетельств и свидетельства самооценки ИБ (документы, результаты опроса или наблюдений)	Кем предоставлены свидетельства самооценки ИБ	Подпись сотрудника/руководителя	Дата

_____
(подпись)

_____
(подпись)

_____
(подпись)

Приложение Б

Документы, рекомендуемые в качестве источников свидетельств самооценки информационной безопасности организации БС РФ

1. Политика ИБ и частные политики ИБ организации, в том числе:

а) частная политика по обеспечению ИБ банковских платежных систем;
б) частная политика по обеспечению ИБ банковских информационных систем;
в) частная политика по обеспечению ИБ банковских телекоммуникационных систем.

2. Документы (положения, руководства, инструкции), регламентирующие деятельность и(или) содержащие свидетельства выполнения деятельности:

а) по назначению и распределению ролей в организации;
б) по работе с персоналом, в т.ч. документы, определяющие внутренние требования организации БС РФ:
   — по приему сотрудников на работу;
   — по соблюдению конфиденциальности информации сотрудниками организации;
   — по соблюдению правил корпоративной этики сотрудниками организации;
   — по недопущению конфликта интересов;
   — к проведению обучения, осведомления персонала и проверки уровня компетентности в области ИБ;
в) по обеспечению ИБ автоматизированных банковских систем на стадиях жизненного цикла, в т.ч. требования:
   — к выдвижению технических требований, разработке технических заданий, проектированию, созданию, тестированию и приемке средств обеспечения ИБ автоматизированных банковских систем;
   — к вводу в действие, эксплуатации, сопровождению и снятию с эксплуатации автоматизированных банковских систем;
г) по управлению доступом к ресурсам ЭВМ, локальным вычислительным сетям и автоматизированным банковским системам организации БС РФ;
д) по обеспечению антивирусной защиты;
е) по использованию ресурсов сети Интернет;
ж) по использованию средств криптографической защиты информации;
з) по обеспечению ИБ банковских платежных технологических процессов организации БС РФ;
и) по обеспечению ИБ банковских информационных технологических процессов организации БС РФ.

3. Документы (положения, руководства, инструкции и т.д.), регламентирующие деятельность и(или) содержащие свидетельства выполнения деятельности в рамках системы менеджмента информационной безопасности (СМИБ) организации БС РФ:

а) определение/уточнение области действия СМИБ и выбор подхода к оценке рисков ИБ. Такими документами могут быть:
   — документ, определяющий выбранные подход и методы оценки рисков ИБ;
   — документ, описывающий область действия СМИБ;
б) анализ и оценка рисков ИБ, выбор вариантов обработки рисков ИБ. Такими документами могут быть:
   — документ, отражающий результаты анализа и оценки рисков ИБ;
   — документ, содержащий варианты обработки рисков ИБ;
в) определение/уточнение политик ИБ организации;
г) выбор/уточнение целей ИБ и защитных мер. Такими документами могут быть:
   — документ, содержащий результаты выбора (уточнения) состава защитных мер;
   — документ, содержащий результаты выбора (уточнения) целей ИБ организации;
д) принятие руководством организации остаточных рисков и решения о реализации и эксплуатации/совершенствовании СМИБ. Такими документами могут быть:
   — решения о реализации и эксплуатации (совершенствовании) СМИБ;
   — документы, определяющие деятельность службы ИБ;
   — документы, отражающие принятие высшим руководством организации остаточных рисков ИБ;
   — документы, определяющие роли по обеспечению ИБ;
е) разработка плана обработки рисков ИБ. Такими документами могут быть документы, определяющие план обработки рисков ИБ;
ж) реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СМИБ. Такими документами могут быть:

— свидетельства эксплуатации реализованных защитных мер;
— свидетельства реализации плана обработки рисков ИБ;
— программы по обучению и осведомлению об ИБ;
— документы, определяющие состав документации и порядок управления документацией в области ИБ организации БС РФ;

з) реализация программ по обучению и осведомлению об ИБ. Такими документами могут быть:
— свидетельства реализации программы по обучению ИБ;
— свидетельства реализации программы по осведомлению об ИБ;

и) обнаружение и реагирование на инциденты безопасности. Такими документами могут быть:
— документы, определяющие процедуры обнаружения инцидентов ИБ и информирования об инцидентах;
— документы, определяющие процедуры оценивания и принятия решений по событиям/инцидентам ИБ;
— документы, определяющие процедуры реагирования на инциденты ИБ;

к) обеспечение непрерывности бизнеса и восстановления после прерываний. Такими документами могут быть:
— политика обеспечения непрерывности бизнеса;
— план восстановления бизнеса после прерываний;
— документы, определяющие процедуру периодического тестирования плана восстановления бизнеса после прерываний;
— программа обучения и осведомления по восстановлению бизнес-процессов после прерываний;

л) мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ. Такими документами могут быть:
— отчетность по оперативной оценке ИБ;
— документы, определяющие процедуры мониторинга и контроля;

м) анализ эффективности СМИБ, включая анализ уровней остаточного и приемлемого рисков ИБ. Такими документами могут быть:
— отчетность, содержащая результаты переоценки рисков ИБ и анализ уровней остаточных и приемлемых рисков ИБ;
— документы, определяющие процедуры по анализу эффективности функционирования СМИБ;

н) внутренний аудит ИБ. Такими документами могут быть:
— документы, определяющие порядок проведения внутреннего аудита ИБ;
— программа аудита ИБ;
— документы по результатам проведенных внутренних аудитов ИБ с предложениями по развитию в области обеспечения ИБ;

о) анализ СМИБ со стороны высшего руководства. Такими документами могут быть:
— документы по результатам анализа СМИБ высшим руководством;
— документ, определяющий перечень документов, предоставляемых высшему руководству для анализа;

п) внешний аудит ИБ. Такими документами могут быть:
— программа аудита ИБ, включающая описание деятельности, необходимой для планирования, организации, проведения и совершенствования внешнего аудита ИБ;
— аудиторские отчеты;

р) реализация тактических улучшений в СМИБ. Такими документами могут быть документы, отражающие действия по совершенствованию СМИБ;

с) реализация стратегических улучшений СМИБ и использование опыта. Такими документами могут быть:
— документы, содержащие описание изменений (в политиках ИБ, плане обработки рисков ИБ и др.);
— документы, содержащие решения руководства о корректирующих и превентивных действиях в отношении СМИБ;

т) информирование об изменениях и их согласование с заинтересованными сторонами. Такими документами могут быть:
— документы, определяющие процедуры информирования заинтересованных сторон об изменениях в обеспечении ИБ;
— документы, определяющие процедуры согласования изменений в обеспечении ИБ с заинтересованными сторонами;

— документы, определяющие процедуры внесения изменений в договоры (соглашения) о взаимодействии с третьими сторонами;

у) оценка достижения поставленных целей. Такими документами могут быть документы, утвержденные руководством по результатам анализа причин несоответствий в реализации и/или эксплуатации СМИБ, относящиеся к уточнению политик ИБ и целей ИБ.

4. Документы (положения, руководства, инструкции и т.д.), регламентирующие деятельность и(или) содержащие свидетельства выполнения деятельности по реализации общих принципов обеспечения информационной безопасности организации БС РФ:

а) своевременность обнаружения, прогноз развития проблем ИБ и оценка их влияния на бизнес-цели организации. Такими документами могут быть:
— документы, отражающие результаты классификации ресурсов по степени их критичности для обеспечения непрерывности бизнеса;
— документы, содержащие модель угроз и модель нарушителя;
— документы, содержащие требования к процедурам обработки инцидентов ИБ;
— документы, содержащие свидетельства деятельности по анализу и обработке инцидентов ИБ;
— документы, содержащие свидетельства выполнения деятельности по управлению рисками ИБ;

б) определение целей, адекватность выбора защитных мер, их эффективность и контролируемость. Такими документами могут быть:
— документы, определяющие цели и задачи обеспечения ИБ организации БС РФ;
— документы, содержащие свидетельства выполнения уточнения/пересмотра целей и задач обеспечения ИБ организации БС РФ;
— документы, обосновывающие выбор защитных мер;
— документы, содержащие план реализации защитных мер;
— документы, содержащие свидетельства контроля правильности реализации и эксплуатации защитных мер;
— документы, определяющие порядок тестирования используемых защитных мер;
— документы, содержащие свидетельства выполнения деятельности по тестированию используемых защитных мер;
— документы, содержащие выполнение деятельности по контролю за реализацией действующих положений и требований по обеспечению ИБ;

в) непрерывность обеспечения ИБ и использование опыта при принятии и реализации решений. Такими документами могут быть:
— документы, регламентирующие деятельность службы ИБ организации БС РФ;
— документы, определяющие роли по обеспечению ИБ организации БС РФ;
— свидетельства выполнения деятельности по анализу и совершенствованию ИБ организации БС РФ;
— документы, определяющие план обеспечения непрерывности бизнеса и восстановления бизнеса после прерываний;
— документы, содержащие свидетельства выполнения процедур периодического тестирования плана восстановления бизнес-процессов после прерываний;

г) знание своих клиентов и служащих, персонификация и адекватное разделение ролей и ответственности и адекватность ролей функциям и процедурам. Такими документами могут быть:
— документы, регламентирующие процедуры, выполняемые при приеме и отборе претендентов на рабочие места;
— договоры организации БС РФ с ее клиентами;
— документы, определяющие роли по обеспечению ИБ организации БС РФ;

д) доступность услуг и сервисов, наблюдаемость и оцениваемость обеспечения ИБ. Такими документами могут быть:
— договоры организации БС РФ с ее клиентами и контрагентами;
— документы, определяющие процедуры мониторинга и контроля;
— программы аудита и самооценки;
— аудиторские отчеты и отчеты с результатами самооценки.

Ключевые слова: банковская система Российской Федерации, информационная безопасность, самооценка информационной безопасности, показатели информационной безопасности, текущий уровень информационной безопасности, система менеджмента информационной безопасности, осознание информационной безопасности, требования информационной безопасности.
