СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2010

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-20xx

Дата введения: 2010-06-21

Издание официальное

Москва
2010

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 21 июня 2010 года № Р-705.

2. ВЗАМЕН СТО БР ИББС-1.2-2009.

Содержание

Введение

Стандартом Банка России СТО БР ИББС-1.0-20xx “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” с целью проверки уровня информационной безопасности (ИБ) как самого Банка России, так и организаций банковской системы (БС) Российской Федерации (РФ) определено требование проведения регулярной внешней и внутренней оценки ИБ, а также самооценки ИБ.

Настоящий стандарт устанавливает способы определения степени выполнения требований Стандарта Банка России СТО БР ИББС-1.0-20xx “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения”, а также итогового уровня соответствия ИБ требованиям Стандарта Банка России СТО БР ИББС-1.0-20xx “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” при проведении внутренней и (или) внешней оценки и самооценки ИБ.

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-20xx

Дата введения: 2010-06-21

1. Область применения

Настоящая методика распространяется на организации БС РФ, а также на организации, проводящие оценку уровня обеспечения ИБ организации БС РФ в соответствии с требованиями Стандарта Банка России СТО БР ИББС-1.0-20xx “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0).

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах организации БС РФ, а также в договорных документах, устанавливающих отношения сторон при проведении внешних оценок ИБ.

Положения настоящего стандарта применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена действующим законодательством Российской Федерации, нормативными актами Банка России или условиями договоров.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на стандарт СТО БР ИББС-1.0.

3. Термины и определения

В настоящем документе применены термины в соответствии с СТО БР ИББС-1.0, стандартом Банка России СТО БР ИББС-1.1-2007 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности”, а также следующие термины с соответствующими определениями.

3.1. **Показатель информационной безопасности:** Мера или характеристика для оценки информационной безопасности.

3.2. **Проверяющая организация:** Организация, проводящая оценку соответствия информационной безопасности организации БС РФ требованиям СТО БР ИББС-1.0.

3.3. **Проверяемая организация:** Организация БС РФ, информационная безопасность которой подвергается оценке на соответствие требованиям СТО БР ИББС-1.0.

4. Обозначения и сокращения

АБС — автоматизированная банковская система;
БС — банковская система;
ЖЦ — жизненный цикл;
ИБ — информационная безопасность;
ИСПДн — информационные системы персональных данных;

НСД — несанкционированный доступ;
НРД — нерегламентированные действия в рамках предоставленных полномочий;
РФ — Российская Федерация;
СКЗИ — средство криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
СИБ — система информационной безопасности;
СОИБ — система обеспечения информационной безопасности;
ЭВМ — электронная вычислительная машина;
ЭЦП — электронная цифровая подпись;
α_{ij} — коэффициент значимости частного показателя;
*EV*1 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению “текущий уровень ИБ организации”;
*EV*2 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению “менеджмент ИБ организации”;
*EV*3 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению “уровень осознания ИБ организации”;
$EV_{ООПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных;
$EV'_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;
$EV^2_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;
$EV_{БИТП}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс;
$EV_{БПТП}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс;
EV_{Mi} — оценка степени выполнения требований СТО БР ИББС-1.0 для группового показателя;
EV_{Mij} — оценка степени выполнения требований СТО БР ИББС-1.0 для частного показателя;
i — номер группового показателя;
j — номер частного показателя;
Mij — обозначение частного показателя;
R — итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0.

5. Общие положения

5.1. Целью настоящей методики является стандартизация подходов и способов оценки, используемых для определения уровня соответствия ИБ организации БС РФ (далее — организации) требованиям СТО БР ИББС-1.0 по направлениям оценки:
— текущий уровень ИБ организации;
— менеджмент ИБ организации;
— уровень осознания ИБ организации.
5.2. Задачами настоящей методики являются:
— определение состава показателей ИБ и способов их оценивания;
— определение способа оценивания текущего уровня ИБ организации с помощью установления степени выполнения требований, определенных в разделе 7 СТО БР ИББС-1.0;
— определение способа оценивания менеджмента ИБ организации и уровня осознания ИБ организации с помощью установления степени выполнения требований, определенных в разделе 8 СТО БР ИББС-1.0;
— определение итогового уровня соответствия ИБ организации требованиям СТО БР ИББС-1.0.

6. Показатели информационной безопасности. Способы оценивания показателей

6.1. Для оценки степени соответствия ИБ организации требованиям СТО БР ИББС-1.0 используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ. Оценки групповых показателей (EV_{Mi}) используются для получения оценки по направлениям (*EV*1, *EV*2 и *EV*3). Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки (EV_{Mij}), которые затем формируют оценки EV_{Mi} групповых показателей.

Приложение А содержит формы, предназначенные для заполнения при проведении оценки. Каждая из форм содержит групповой показатель ИБ, входящие в него частные показатели ИБ, метрику (шкалу) для оценивания частных показателей и коэффициенты значимости частных показателей ИБ, используемые при вычислении группового показателя.

6.2. Частные показатели разделены на две категории. Первую категорию составляют частные показатели, отражающие требования СТО БР ИББС-1.0, выполнение которых обязательно в организации. Вторую категорию составляют частные показатели, отражающие положения СТО БР ИББС-1.0, выполнение которых рекомендуется в организации. Информация о принадлежности частных показателей к указанным категориям определена в формах Приложения А.

6.3. Способ оценивания частного показателя зависит от его принадлежности к одной из категорий, определенных в п. 6.2 настоящей методики.

6.4. Оценка EV_{Mij} частного показателя формируется на основании выявленной аудиторской группой степени выполнения требований посредством экспертного оценивания.

Оценивание частного показателя должно сопровождаться внесением символа, например, “X”, в соответствующую графу представленных в Приложении А форм.

6.5. Для частных показателей, выполнение которых обязательно, устанавливается следующая шкала степени их выполнения:

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

Если частный показатель предназначен для оценки требований, которые не относятся к деятельности организации или на момент оценки не являются актуальными для организации, что документально зафиксировано во внутренних документах организации, то данный частный показатель определяется как неоцениваемый (должна быть заполнена графа “н/о” — нет оценки) и не учитывается в формировании дальнейших результатов оценки. При этом необходимо выполнить процедуру нормировки коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя.

6.6. Для частных показателей, выполнение которых рекомендуется, устанавливается следующая шкала степени их выполнения:

— “да” — оценке присваивается значение, равное единице;
— “нет” — частный показатель определяется как неоцениваемый (должна быть заполнена графа “н/о” — нет оценки) и не учитывается в формировании дальнейших результатов оценки. При этом необходимо выполнить процедуру нормировки коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя.

6.7. При проведении оценки частных показателей, для которых оценивается как степень документированности, так и степень выполнения, рекомендуется использовать следующий общий подход:

Таблица 1 — Рекомендуемые критерии выставления оценок частных показателей ИБ, в которых оценивается как степень документированности, так и степень выполнения требований ИБ

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации и не выполняются
0	Требования частного показателя ИБ частично установлены в нормативных документах проверяемой организации, но не выполняются

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0,25	Требования частного показателя ИБ полностью установлены в нормативных документах проверяемой организации, но не выполняются
0,25	Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,25	Требования частного показателя ИБ частично установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,5	Требования частного показателя ИБ полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,5	Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
0,75	Требования частного показателя ИБ частично установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
1	Требования частного показателя ИБ полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в полном объеме

6.8. При проведении оценки частных показателей, для которых оценивается только степень документированности, рекомендуется использовать следующий общий подход:

Таблица 2 — Рекомендуемые критерии выставления оценок частных показателей ИБ, в которых оценивается только степень документированности требований ИБ

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации
0,5	Требования частного показателя ИБ частично установлены в нормативных документах проверяемой организации
1	Требования частного показателя ИБ полностью установлены в нормативных документах проверяемой организации

6.9. При проведении оценки частных показателей, для которых оценивается только степень выполнения, рекомендуется использовать следующий общий подход:

Таблица 3 — Рекомендуемые критерии выставления оценок частных показателей ИБ, в которых оценивается только степень выполнения требований ИБ

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не выполняются
0,5	Требования частного показателя ИБ выполняются в неполном объеме
1	Требования частного показателя ИБ выполняются в полном объеме

6.10. В случаях, если при проведении оценки частного показателя используется ограниченный набор объектов, входящих в область аудита ИБ (например, ограниченная выборка автоматизированных банковских систем), и по результатам оценивания частного показателя получены результаты, указывающие на полное выполнение или полное невыполнение/полную документированность или отсутствие документированности соответствующих требований ИБ, рекомендуется расширить набор указанных объектов (выборку) для подтверждения или коррекции полученных результатов.

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

- внутренние нормативные документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации;
- устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;
- результаты наблюдений членов аудиторской группы за деятельностью сотрудников проверяемой организации в области ИБ.

В процессе проведения устного опроса сотрудников проверяемой организации и наблюдений за деятельностью указанных сотрудников члены аудиторской группы должны сделать

вывод о степени соответствия оцениваемой деятельности требованиям внутренних нормативных документов проверяемой организации.

Полученные свидетельства аудита ИБ и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств аудита ИБ, пример которых приведен в Приложении Б. При заполнении листов для сбора свидетельств аудита ИБ необходимо указать ссылки на соответствующие внутренние нормативные документы проверяемой организации, результаты опроса сотрудников проверяемой организации, а также результаты наблюдений членов аудиторской группы. Результаты опроса и наблюдений должны быть подтверждены подписью опрашиваемого сотрудника организации и члена аудиторской группы соответственно.

6.12. Оценка группового показателя (EV_{Mi}), за исключением группового показателя М9 "Общие требования по обработке персональных данных в организации БС РФ", вычисляется из оценок входящих в него частных показателей (EV_{Mij}) с учетом коэффициентов значимости α_{ij}, определяющих важность частного показателя для оценивания группового показателя:

$$EV_{Mi} = \sum_{j} \alpha_{ij} \cdot EV_{Mij}.$$

При формировании коэффициентов значимости учитывалось следующее условие нормировки:

$$\sum_{j=1}^{k} \alpha_{ij} = 1,$$

где k — число частных показателей в i-м групповом показателе.

Коэффициенты значимости α_{ij} для каждого частного показателя, за исключением частных показателей группового показателя М9 "Общие требования по обработке персональных данных в организации БС РФ", приведены в Приложении А.

6.13. Оценка группового показателя (EV_{Mi}) для группового показателя М9 "Общие требования по обработке персональных данных в организации БС РФ" определяется по наименьшему значению оценок входящих в него частных показателей. При этом для группового показателя М9 "Общие требования по обработке персональных данных в организации БС РФ" коэффициенты значимости не определены.

6.14. Если в рамках группового показателя все входящие в него частные показатели определены как неоцениваемые, указанный групповой показатель также определяется как неоцениваемый и не учитывается в формировании дальнейших результатов оценки. В этом случае групповой показатель не учитывается в формулах расчета для $EV_{БИТП}$, $EV_{БПТП}$, $EV_{ООПД}$, $EV^{1}_{ОЗПД}$, $EV^{2}_{ОЗПД}$, $EV2$ или $EV3$ (см. разделы 7, 8, 9) с соответствующей корректировкой в формулах расчета количества оцениваемых групповых показателей. Оценки для таких групповых показателей не отображаются на круговой диаграмме (см. раздел 11).

7. Оценка текущего уровня информационной безопасности организации банковской системы Российской Федерации

7.1. Оценка текущего уровня ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС-1.0 для следующих областей:

- обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу;
- обеспечение ИБ на стадиях жизненного цикла АБС;
- обеспечение ИБ при управлении доступом и регистрацией;
- обеспечение ИБ средствами антивирусной защиты;
- обеспечение ИБ при использовании ресурсов сети Интернет;
- обеспечение ИБ при использовании средств криптографической защиты информации;
- обеспечение ИБ банковских платежных технологических процессов;
- обеспечение ИБ банковских информационных технологических процессов;
- обработка персональных данных в организации БС РФ;
- обеспечение ИБ банковских технологических процессов, в рамках которых обрабатываются персональные данные.

7.2. Групповые показатели по направлению оценки “текущий уровень ИБ организации” отражают совокупность требований ИБ к областям, определенным в разделе 7 СТО БР ИББС-1.0. Таблица 4 отражает соответствие между структурными элементами СТО БР ИББС-1.0, содержащими требования ИБ, и групповыми показателями ИБ, предназначенными для проверки реализации данных требований.

Таблица 4 — Соответствие групповых показателей ИБ совокупности требований ИБ к областям, определенным в разделе 7 СТО БР ИББС-1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M1	Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу	п. 7.2
M2	Обеспечение ИБ на стадиях жизненного цикла АБС	п. 7.3
M3	Обеспечение ИБ при управлении доступом и регистрации	п. 7.4
M4	Обеспечение ИБ средствами антивирусной защиты	п. 7.5
M5	Обеспечение ИБ при использовании ресурсов сети Интернет	п. 7.6
M6	Обеспечение ИБ при использовании средств криптографической защиты информации	п. 7.7
M7	Обеспечение ИБ банковских платежных технологических процессов	п. 7.8
M8	Обеспечение ИБ банковских информационных технологических процессов	п. 7.9
M9	Общие требования по обработке персональных данных в организации БС РФ	п. 7.10
M10	Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные	п. 7.11

7.3. Частные показатели по направлению оценки “текущий уровень ИБ организации” отражают отдельные требования ИБ СТО БР ИББС-1.0, предъявляемые по каждой из областей. Частные показатели по направлению оценки “текущий уровень ИБ организации” (показатели M1÷M10), метрики, а также коэффициенты значимости α_{ij} приведены в Приложении А.

7.4. Оценивание частных показателей в рамках групповых показателей M1÷M6 необходимо осуществлять раздельно по результатам анализа выполнения соответствующих требований СТО БР ИББС-1.0 по следующим направлениям:

— банковский платежный технологический процесс (M7);
— банковский информационный технологический процесс (M8);
— банковский технологический процесс, в рамках которого обрабатываются персональные данные (M10).

7.5. Оценки EV_{Mij} и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M1÷M10, вносятся в соответствующие графы представленных в Приложении А форм.

7.6. Итоговая оценка $EV1$, отражающая степень выполнения требований СТО БР ИББС-1.0 по направлению “текущий уровень ИБ организации”, определяется по наименьшему значению из следующих оценок:

$EV_{БИТП}$ — степень выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс;

$EV_{БПТП}$ — степень выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс;

$EV^2_{ОЗПД}$ — степень выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;

$EV_{ООПД}$ — степень выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных.

7.7. Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс, вычисляется по формуле, в которой оценки групповых показателей M1÷M6 выбираются по результатам их оценивания, применительно к банковскому платежному технологическому процессу:

$$EV_{БПТП} = \frac{\sum_{i} EV_{Mi} + EV_{M7}}{7}, \quad i = 1 \div 6.$$

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс, вычисляется по формуле, в которой оценки групповых показателей М1÷М6 выбираются по результатам их оценивания, применительно к банковскому информационному технологическому процессу:

$$EV_{БИТП} = \frac{\sum_{i} EV_{Mi} + EV_{M8}}{7},\ i = 1 \div 6.$$

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных (ИСПДн), без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании средств криптографической защиты информации (СКЗИ) вычисляется по формуле, в которой оценки групповых показателей М1÷М5 выбираются по результатам их оценивания, применительно к банковскому технологическому процессу, в рамках которого обрабатываются персональные данные в ИСПДн:

$$EV^{1}_{ОЗПД} = \frac{\sum_{i} EV_{Mi} + EV_{M8} + EV_{M10}}{7},\ i = 1 \div 5.$$

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в ИСПДн, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании СКЗИ вычисляется по формуле, в которой оценки групповых показателей М1÷М6 выбираются по результатам их оценивания, применительно к банковскому технологическому процессу, в рамках которого обрабатываются персональные данные в ИСПДн:

$$EV^{2}_{ОЗПД} = \frac{\sum_{i} EV_{Mi} + EV_{M8} + EV_{M10}}{8},\ i = 1 \div 6.$$

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных, вычисляется по формуле:

$$EV_{ООПД} = EV_{M9}.$$

7.8. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ М1÷М10, отображаются на круговой диаграмме (см. раздел 11) в секторах с 1-го по 10-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

7.9. Оценка *EV*1 отображается на круговой диаграмме (см. раздел 11) в секторах с 1-го по 10-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению *EV*1.

8. Оценка менеджмента информационной безопасности организации банковской системы Российской Федерации

8.1. Оценка менеджмента ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС-1.0 для следующих областей:

- организация и функционирование службы ИБ организации;
- определение/коррекция области действия СОИБ;
- выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ;
- разработка планов обработки рисков нарушения ИБ;
- разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- принятие руководством организации решений о реализации и эксплуатации СОИБ;
- организация реализации планов обработки рисков нарушения ИБ;
- разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ;

— организация обнаружения и реагирования на инциденты безопасности;
— организация обеспечения непрерывности бизнеса и его восстановления после прерываний;
— мониторинг и контроль защитных мер;
— проведение самооценки ИБ;
— проведение внешнего аудита ИБ;
— анализ функционирования СОИБ;
— анализ СОИБ со стороны руководства организации;
— принятие решений по тактическим улучшениям СОИБ;
— принятие решений по стратегическим улучшениям СОИБ.

8.2. Групповые показатели по направлению оценки “менеджмент ИБ организации” отражают совокупность требований ИБ к областям, определенным в разделе 8 СТО БР ИББС-1.0. Таблица 5 отражает соответствие между структурными элементами СТО БР ИББС-1.0, содержащими требования ИБ, и групповыми показателями ИБ, предназначенными для проверки реализации данных требований.

Таблица 5 — Соответствие групповых показателей ИБ требованиям к СМИБ, представленным в разделе 8 СТО БР ИББС-1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M11	Организация и функционирование службы ИБ организации	п. 8.2
M12	Определение/коррекция области действия СОИБ	п. 8.3
M13	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ	п. 8.4
M14	Разработка планов обработки рисков нарушения ИБ	п. 8.5
M15	Разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ	п. 8.6
M16	Принятие руководством организации решений о реализации и эксплуатации СОИБ	п. 8.7
M17	Организация реализации планов внедрения СОИБ	п. 8.8
M18	Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ	п. 8.9
M19	Организация обнаружения и реагирования на инциденты безопасности	п. 8.10
M20	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний	п. 8.11
M21	Мониторинг и контроль защитных мер	п. 8.12
M22	Проведение самооценки ИБ	п. 8.13
M23	Проведение аудита ИБ	п. 8.14
M24	Анализ функционирования СОИБ	п. 8.15
M25	Анализ СОИБ со стороны руководства организации	п. 8.16
M26	Принятие решений по тактическим улучшениям СОИБ	п. 8.17
M27	Принятие решений по стратегическим улучшениям СОИБ	п. 8.18

8.3. Частные показатели по направлению оценки “менеджмент ИБ организации” отражают отдельные требования ИБ СТО БР ИББС-1.0, предъявляемые по каждой из областей. Частные показатели по направлению оценки “менеджмент ИБ организации” (показатели M11÷M27), метрики, а также коэффициенты значимости α_{ij} для каждого частного показателя приведены в Приложении А.

8.4. Оценки EV_{Mij} и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M11÷M27, вносятся в соответствующие графы представленных в Приложении А форм.

8.5. Итоговая оценка *EV*2, отражающая степени выполнения требований СТО БР ИББС-1.0 по направлению “менеджмент ИБ организации”, вычисляется по формуле:

$$EV2 = \frac{\sum_{i=11}^{27} EV_{Mi}}{17}.$$

8.6. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M11÷M27, отображаются на круговой диаграмме (см. раздел 11) в секторах с 11-го по 27-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

8.7. Оценка *EV*2 отображается на круговой диаграмме (см. раздел 11) в секторах с 11-го по 27-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению *EV*2.

9. Оценка уровня осознания информационной безопасности организации банковской системы Российской Федерации

9.1. Оценка уровня осознания ИБ организации определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС-1.0 для следующих областей:

- деятельность руководства организации по поддержке функционирования службы ИБ организации;
- деятельность руководства организации по принятию решений о реализации и эксплуатации СОИБ;
- деятельность руководства организации по поддержке планирования СОИБ;
- деятельность руководства организации по поддержке реализации СОИБ;
- деятельность руководства организации по поддержке проверки СОИБ;
- деятельность руководства организации по анализу СОИБ;
- деятельность руководства организации по поддержке совершенствования СОИБ.

9.2. Групповые показатели по направлению оценки “уровень осознания ИБ организации” отражают совокупность требований ИБ к областям, определенным в разделе 8 СТО БР ИББС-1.0. Таблица 6 отражает соответствие между структурными элементами СТО БР ИББС-1.0, содержащими требования ИБ, и групповыми показателями ИБ, предназначенными для проверки реализации данных требований.

Таблица 6 — Соответствие групповых показателей ИБ требованиям, представленным в разделе 8 СТО БР ИББС-1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M28	Оценка деятельности руководства организации по поддержке функционирования службы ИБ организации	п. 8.2
M29	Оценка деятельности руководства организации по принятию решений о реализации и эксплуатации СОИБ	п. 8.7
M30	Оценка деятельности руководства организации по поддержке планирования СОИБ	пп. 8.3, 8.4, 8.5, 8.6, 8.8
M31	Оценка деятельности руководства организации по поддержке реализации СОИБ	пп. 8.9, 8.10, 8.11
M32	Оценка деятельности руководства организации по поддержке проверки СОИБ	пп. 8.12, 8.13, 8.14, 8.15
M33	Оценка деятельности руководства организации по анализу СОИБ	п. 8.16
M34	Оценка деятельности руководства организации по поддержке совершенствования СОИБ	пп. 8.17, 8.18

9.3. Частные показатели по направлению оценки “уровень осознания ИБ организации” отражают отдельные требования СТО БР ИББС-1.0 к СМИБ организации, относящиеся к деятельности руководства организации. Частные показатели по направлению оценки “уровень осознания ИБ организации” (показатели M28÷M34), метрики, а также коэффициенты значимости α_{ij} для каждого частного показателя приведены в Приложении А.

9.4. Оценки EV_{Mij} и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M28÷M34, вносятся в соответствующие графы представленных в Приложении А форм.

9.5. Итоговая оценка EV3, отражающая степень выполнения требований СТО БР ИББС-1.0 по направлению “уровень осознания ИБ организации”, вычисляется по формуле:

$$EV3 = \frac{\sum_{i=28}^{34} EV_{Mi}}{7}.$$

9.6. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ М28÷М34, отображаются на круговой диаграмме (см. раздел 11) в секторах с 28-го по 34-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

9.7. Оценка *EV*3 отображается на круговой диаграмме (см. раздел 11) в секторах с 28-го по 34-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению *EV*3.

10. Особенности оценки степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных

10.1. Для оценки степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в ИСПДн, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению ИБ при использовании СКЗИ и формирования оценки $EV^1_{ОЗПД}$ следует использовать уточняющие вопросы, которые детализируют и конкретизируют частные показатели ИБ.

Уточняющие вопросы составлены на основе положений РС БР ИББС-2.3 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации”.

Перечень указанных уточняющих вопросов, а также их связь с частными показателями содержится в Приложении В (таблица 1 и таблица 2 соответственно).

Если в конкретной организации БС РФ отдельные требования РС БР ИББС-2.3 заменены иными требованиями, обеспечивающими эквивалентный (аналогичный) уровень безопасности персональных данных то соответствующие изменения должны быть внесены в перечень уточняющих вопросов в Приложении В.

10.2. Для проведения оценки соответствия ИБ в части информационных систем персональных данных необходимо провести оценивание частных показателей настоящего стандарта, попадающих в область оценки, используя все соответствующие частным показателям детализирующие и конкретизирующие вопросы Приложения В. Для этого необходимо:

— на основании ссылок на частный показатель, приведенных в Приложении В, и в соответствии с классом информационной системы персональных данных составить перечень вопросов, соответствующих оцениваемому частному показателю (или воспользоваться таблицей соответствия частных показателей и вопросов, приведенной в Приложении В);
— провести оценивание вопросов Приложения В из перечня вопросов, соответствующих оцениваемому частному показателю;
— провести оценивание частного показателя настоящего стандарта, используя в том числе оценки для вопросов Приложения В.

10.3. Оценка вопросов Приложения В формируется на основании выявленной степени выполнения проверяемого требования посредством экспертного оценивания. Устанавливается следующая шкала степени выполнения проверяемых требований:

— “Выполняется в полном объеме”;
— “Выполняется не в полном объеме”;
— “Не выполняется”.

Оценка вопросов Приложения В должна основываться на свидетельствах аудита ИБ, приведенных в п. 6.11 настоящего стандарта.

10.4. Оценивание частных показателей следует проводить в соответствии с рекомендуемыми критериями выставления оценок частных показателей информационной безопасности, определенными в п. 6.7 настоящего стандарта.

Оценивание всех вопросов из составленного перечня вопросов Приложения В является необходимым для оценивания частного показателя.

При проведении оценивания частных показателей следует использовать следующий общий подход:

Таблица 7 — Рекомендуемые критерии выставления оценок частных показателей ИБ на основе оценки вопросов Приложения В

Максимальная оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, не установлены во внутренних нормативных документах проверяемой организации и не выполняются
0	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, частично установлены во внутренних нормативных документах проверяемой организации, но не выполняются
0,25	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, полностью установлены во внутренних нормативных документах проверяемой организации, но не выполняются
0,25	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, не установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,25	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, частично установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,5	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме
0,5	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, не установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
0,75	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, частично установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
1	Требования всех вопросов Приложения В, соответствующих оцениваемому частному показателю, полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в полном объеме

В ряде случаев оценивание всех вопросов из составленного перечня Приложения В может оказаться недостаточным для оценивания частного показателя. В этом случае оценка частного показателя должна проводиться в соответствии с требованиями раздела 6 настоящего стандарта.

Результаты оценивания вопросов Приложения В должны быть документально оформлены путем составления соответствующих листов для сбора свидетельств аудита ИБ, пример которых приведен в Приложении Б. При заполнении листов для сбора свидетельств аудита ИБ необходимо указать ссылки на соответствующие вопросы Приложения В и документы, содержащие свидетельства выполнения оцениваемой деятельности, привести результаты опроса сотрудников проверяемой организации, а также результаты наблюдений членов аудиторской группы. Результаты опроса и наблюдений должны быть подтверждены подписью опрашиваемого сотрудника или члена аудиторской группы соответственно.

10.5. Все вопросы Приложения В должны быть оценены. Однако перед оцениванием этих вопросов следует провести анализ актуальности соответствующих им требований для деятельности проверяемой организации. Неактуальным вопрос может быть признан только в том случае, если соответствующее ему требование не относится к деятельности организации или на момент оценки не является актуальным для организации, что документально зафиксировано во внутренних документах организации. В этом случае вопрос определяется как не оцениваемый (выставляется оценка “1”) и не учитывается в дальнейшем формировании оценок частных показателей. Решение о признании вопроса Приложения В как не оцениваемого должно приниматься ответственным за процесс оценки из числа представителей проверяемой организации и оформляться документально.

11. Определение уровня соответствия информационной безопасности организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Отображение оценок

11.1. Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0 до 0,25, то данному направлению оценки присваивается нулевой уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,25 до 0,5, то данному направлению оценки присваивается первый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,5 до 0,7, то данному направлению оценки присваивается второй уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,7 до 0,85, то данному направлению оценки присваивается третий уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,85 до 0,95, то данному направлению оценки присваивается четвертый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка *EV*1, *EV*2 или *EV*3 лежит в интервале от 0,95 до 1 включительно, то данному направлению оценки присваивается пятый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

11.2. Значение *R* определяется по наименьшему значению из трех оценок по направлениям оценки:

— оценки уровня осознания ИБ организации (*EV*3);
— оценки менеджмента ИБ организации (*EV*2);
— оценки текущего уровня ИБ организации (*EV*1).

11.3. Полученное в результате оценки соответствия ИБ организации требованиям СТО БР ИББС-1.0 значение *R* является основой для формирования аудиторского заключения по результатам аудита ИБ.

11.4. Значения *R*, соответствующие четвертому и пятому уровням, являются рекомендуемыми Банком России.

Значения *R*, соответствующие уровням с нулевого по третий, не являются рекомендуемыми Банком России.

11.5. Рисунок 1 представляет собой круговую диаграмму для отображения результатов оценивания.

Секторы с 1-го по 10-й используются для отображения оценки текущего уровня ИБ организации.

Секторы с 11-го по 27-й используются для отображения оценки процессов менеджмента ИБ организации.

Секторы с 28-го по 34-й используются для отображения оценки уровня осознания ИБ организации.

Пятому уровню соответствуют окружность радиусом 0,95 и кольцо до окружности радиусом 1.

Четвертому уровню соответствуют окружность радиусом 0,85 и кольцо до окружности радиусом 0,95.

Третьему уровню соответствуют окружность радиусом 0,7 и кольцо до окружности радиусом 0,85.

Второму уровню соответствуют окружность радиусом 0,5 и кольцо до окружности радиусом 0,7.

Первому уровню соответствуют окружность радиусом 0,25 и кольцо до окружности радиусом 0,5.

Нулевому уровню соответствует круг до окружности радиусом 0,25.

11.6. По результатам проведения оценки соответствия формируется документ — “Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-20xx”.

“Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-20xx” формируется на основе:

— аудиторского заключения в случае проведения оценки соответствия внешней организацией;
— отчета самооценки в случае проведения оценки соответствия силами организации БС РФ.

В “Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-20xx” как минимум следует включать следующие оценки:

$EV_{ООПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных;

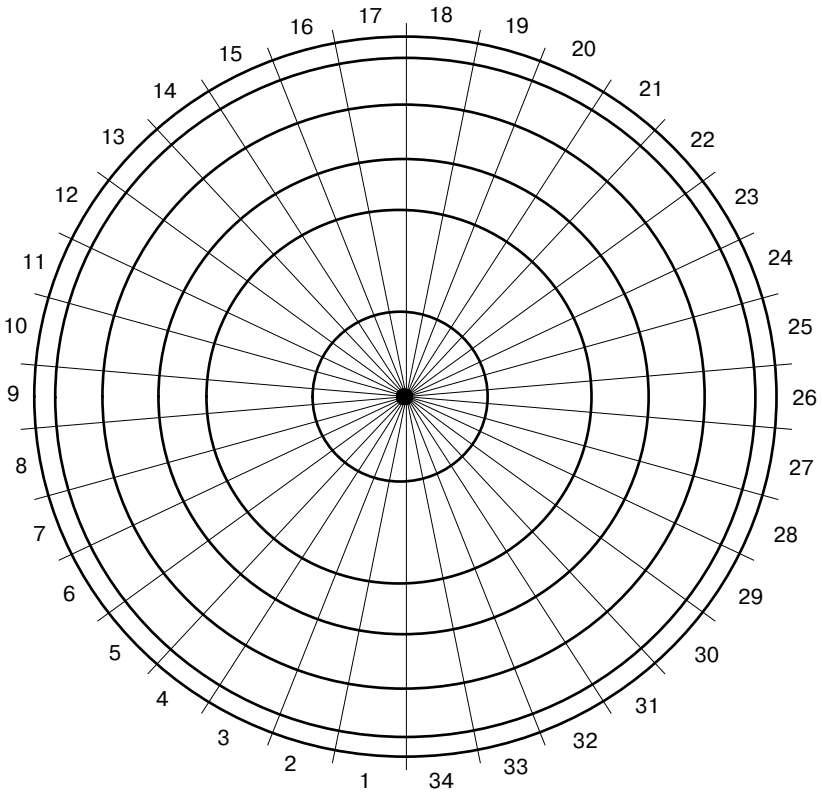
$EV^{I}_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;

$EV_{М6}$ — оценка группового показателя М6 “Обеспечение информационной безопасности при использовании средств криптографической защиты информации” применительно к банковскому технологическому процессу, в рамках которого обрабатываются персональные данные (оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных при использовании средств криптографической защиты информации);

R — итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0.

С целью направления “Подтверждения соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-20xx” регуляторам, осуществляющим надзор за выполнением законодательства в области персональных данных, данный документ следует составлять в пяти экземплярах, один из которых предназначен для использования в организации БС РФ.

Рисунок 1 — Круговая диаграмма для отображения результатов оценивания



Приложение А
(обязательное)

Показатели информационной безопасности

Групповой показатель М1 “Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М1.1	Определены ли в документах организации роли ее работников?	обязательный							0,0581	
М1.2	Формируются ли роли, связанные с выполнением деятельности по обеспечению ИБ, на основании требований разделов 7 и 8 стандарта СТО БР ИББС-1.0?	обязательный							0,0291	
М1.3	Персонифицированы ли роли в организации с установлением ответственности за их выполнение?	обязательный							0,0502	
М1.4	Зафиксирована ли документально в должностных инструкциях ответственность за выполнение ролей?	обязательный							0,0461	
М1.5	Отсутствуют ли в организации роли, совмещающие функции разработки и сопровождения системы/ПО?	рекомендуемый							0,0522	
М1.6	Отсутствуют ли в организации роли, совмещающие функции разработки и эксплуатации системы/ПО?	рекомендуемый							0,0610	
М1.7	Отсутствуют ли в организации роли, совмещающие функции сопровождения и эксплуатации?	рекомендуемый							0,0522	
М1.8	Отсутствуют ли в организации роли, совмещающие функции администратора системы и администратора информационной безопасности?	рекомендуемый							0,0661	
М1.9	Отсутствуют ли в организации роли, совмещающие функции по выполнению операций в системе и контроля их выполнения?	рекомендуемый							0,0661	
М1.10	Определены ли документально в организации и выполняются ли процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации?	обязательный							0,1001	
М1.11	Определены ли в документах организации процедуры приема на работу, влияющую на обеспечение ИБ, включающие: — проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; — проверку в части профессиональных навыков и оценку профессиональной пригодности?	обязательный							0,0513	
М1.12	Предусматривают ли указанные в частном показателе М1.11 процедуры документальную фиксацию результатов проводимых проверок?	обязательный							0,0371	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М1.13	Определены ли в документах организации процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников?	рекомендуемый							0,0302	
М1.14	Предусматривают ли указанные в частном показателе М1.13 процедуры документальную фиксацию результатов проводимых проверок?	рекомендуемый							0,0302	
М1.15	Определены ли в документах организации процедуры внеплановой проверки работников при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии?	рекомендуемый							0,0433	
М1.16	Предусматривают ли указанные в частном показателе М1.15 процедуры документальную фиксацию результатов проводимых проверок?	рекомендуемый							0,0391	
М1.17	Обязаны ли все работники организации давать письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов?	обязательный							0,0383	
М1.18	Регламентируются ли положениями, включенными в договоры (соглашения) с внешними организациями и клиентами, требования по ИБ?	обязательный							0,0449	
М1.19	Определены ли в трудовых контрактах (соглашениях, договорах) и (или) должностных инструкциях обязанности персонала по выполнению требований ИБ?	обязательный							0,0582	
М1.20	Приравнивается ли невыполнение работниками организации требований ИБ к невыполнению должностных обязанностей и приводит ли как минимум к дисциплинарной ответственности?	обязательный							0,0462	
Итоговая оценка группового показателя М1										

Групповой показатель М2 “Обеспечение информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М2.1	Рассматриваются ли при формировании требований ИБ следующие стадии модели ЖЦ АБС: — разработка технических заданий; — проектирование; — создание и тестирование; — приемка и ввод в действие; — эксплуатация; — сопровождение и модернизация; — снятие с эксплуатации?	рекомендуемый							0,0504	
М2.2	Осуществляются ли разработка технических заданий и приемка АБС по согласованию и при участии подразделения (лиц) в организации, ответственного за обеспечение ИБ?	обязательный							0,0616	
М2.3	Осуществляются ли ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС под контролем подразделений (лиц) в организации, ответственных за обеспечение ИБ?	обязательный							0,0591	
М2.4	Имеют ли соответствующие лицензии организации, которые привлекаются на договорной основе для разработки и (или) производства средств и систем защиты АБС?	обязательный							0,0563	
М2.5	Снабжены ли разрабатываемые АБС и (или) их компоненты документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации?	обязательный							0,0646	
М2.6	Снабжены ли приобретаемые организацией АБС и (или) их компоненты документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации?	рекомендуемый							0,0604	
М2.7	Содержит ли документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки?	обязательный							0,0450	
М2.8	Реализуется ли при взаимодействии организации с разработчиком АБС и их компонентов одна из трех альтернатив: 1) в договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов включаются положения по сопровождению поставляемых изделий на весь срок их службы; 2) организация приобретает полный комплект рабочей конструкторской документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика; 3) руководство организации оценивает и документально оформляет допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов?	обязательный								0,0604	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М2.9	Учитывается ли при разработке технических заданий на системы дистанционного банковского обслуживания, что защита данных должна обеспечиваться в условиях: — попыток доступа к банковской информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования; — возможности ошибок авторизованных пользователей систем; — возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями?	обязательный							0,0596	
М2.10	Обеспечиваются ли на стадии тестирования анонимность данных и проверка адекватности разграничения доступа?	обязательный							0,0474	
М2.11	Определены ли в документах организации и выполняются ли на стадии эксплуатации АБС процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер?	обязательный							0,0700	
М2.12	Предусматривают ли указанные в частном показателе М2.11 процедуры документальную фиксацию результатов контроля?	обязательный							0,0626	
М2.13	Определены ли в документах организации и выполняются ли на стадии сопровождения (модернизации) АБС процедуры контроля, обеспечивающие защиту от: — умышленного несанкционированного раскрытия, модификации или уничтожения информации; — неумышленной модификации, раскрытия или уничтожения информации; — отказа в обслуживании или ухудшения обслуживания?	обязательный							0,0596	
М2.14	Предусматривают ли указанные в частном показателе М2.13 процедуры документальную фиксацию результатов контроля?	обязательный							0,0533	
М2.15	Проводятся ли на стадии сопровождения (модернизации) при любом внесении изменений в АБС процедуры проверки функциональности, результаты которых документируются?	обязательный							0,0646	
М2.16	Определены ли документально и выполняются ли на стадии снятия с эксплуатации процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и с внешних носителей (за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами)?	обязательный							0,0675	
М2.17	Предусматривают ли указанные в частном показателе М2.16 процедуры документальную фиксацию результатов их выполнения?	обязательный							0,0576	
Итоговая оценка группового показателя М2										

Групповой показатель М3 “Обеспечение информационной безопасности при управлении доступом и регистрации”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М3.1	Определен ли в документах организации перечень информационных активов (их типов)?	обязательный							0,0356	
М3.2	Зафиксированы ли документально права доступа работников и клиентов к информационным активам организации?	обязательный							0,0360	
М3.3	Применяются ли в составе АБС встроенные защитные меры?	обязательный							0,0345	
М3.4	Применяются ли в составе АБС сертифицированные или разрешенные к применению руководством организации средства защиты информации от НСД и НРД?	рекомендуемый							0,0334	
М3.5	Определены ли в документах организации, утверждены ли руководством организации, выполняются ли и контролируются ли процедуры идентификации, аутентификации и авторизации?	обязательный							0,0366	
М3.6	Документируются ли результаты контроля процедур, указанных в частном показателе М3.5?	обязательный							0,0345	
М3.7	Определены ли в документах организации, выполняются ли и контролируются ли процедуры управления доступом?	обязательный							0,0360	
М3.8	Документируются ли результаты контроля процедур, указанных в частном показателе М3.7?	обязательный							0,0334	
М3.9	Определены ли в документах организации, выполняются ли и контролируются ли процедуры контроля целостности?	обязательный							0,0340	
М3.10	Документируются ли результаты контроля процедур, указанных в частном показателе М3.9?	обязательный							0,0319	
М3.11	Определены ли в документах организации, выполняются ли и контролируются ли процедуры регистрации событий и действий?	обязательный							0,0319	
М3.12	Документируются ли результаты контроля процедур, указанных в частном показателе М3.11?	обязательный							0,0286	
М3.13	Исключают ли процедуры управления доступом возможность “самосанкционирования”?	обязательный							0,0308	
М3.14	Определены ли в документах организации процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявить неправомерные или подозрительные операции и транзакции?	обязательный							0,0331	
М3.15	Используются ли специализированные программные и (или) технические средства для проведения процедур мониторинга и анализа данных регистрации, действия и операций?	рекомендуемый							0,0255	
М3.16	Используют ли процедуры мониторинга и анализа документально определенные критерии выявления неправомерных или подозрительных действий и операций?	обязательный							0,0266	
М3.17	Применяются ли процедуры мониторинга и анализа на регулярной основе (например, ежедневно) ко всем выполненным операциям и транзакциям?	обязательный							0,0286	
М3.18	Регламентирован ли во внутренних документах организации порядок доступа работников организации в помещения, в которых размещаются объекты среды информационных активов?	обязательный							0,0292	
М3.19	Контролируется ли выполнение порядка доступа работников организации в помещения, в которых размещаются объекты среды информационных активов?	обязательный							0,0297	
М3.20	Оформляются ли документально результаты выполнения контроля порядка доступа работников организации в помещения, в которых размещаются объекты среды информационных активов?	обязательный							0,0263	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М3.21	Обеспечивают ли используемые в организации АБС, в том числе системы дистанционного банковского обслуживания, возможность регистрации: — операций с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов; — проводимых транзакций, имеющих финансовые последствия; — операций, связанных с назначением и распределением прав пользователей?	обязательный							0,0328	
М3.22	Реализованы ли в системах дистанционного банковского обслуживания, используемых в организации, защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций (например, ЭЦП)?	обязательный							0,0344	
М3.23	Придано ли протоколам операций, выполняемых посредством дистанционного банковского обслуживания, свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание?	рекомендуемый							0,0312	
М3.24	Производится ли при заключении договоров со сторонними организациями юридическое оформление договоренностей, определяющих необходимый уровень взаимодействия в случае выхода инцидента ИБ за рамки отдельной организации?	рекомендуемый							0,0274	
М3.25	Определены ли в документах организации процедуры, определяющие действия работников и клиентов организации в случае компрометации информации, необходимой для их идентификации, аутентификации и (или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев?	обязательный							0,0294	
М3.26	Доведены ли до сведения работников и клиентов организации процедуры, указанные в частном показателе М3.25?	обязательный							0,0283	
М3.27	Предусматривают ли указанные в частном показателе М3.26 процедуры документирование работниками и клиентами своих действий и их результатов?	обязательный							0,0254	
М3.28	Реализованы ли в системах дистанционного банковского обслуживания механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имени?	обязательный							0,0239	
М3.29	Применяются ли в организации защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников организации?	обязательный							0,0319	
М3.30	Регистрируются ли все попытки НСД и НРД к информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и сотрудников организации?	обязательный							0,0326	
М3.31	Определена ли в документах организации и выполняется ли процедура пересмотра прав доступа при увольнении или изменении должностных обязанностей работников организации, имевших доступ к информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и сотрудников организации?	обязательный							0,0316	
М3.32	Осуществляется ли работа всех пользователей АБС под уникальными учетными записями?	обязательный							0,0349	
Итоговая оценка группового показателя М3										

Групповой показатель М4 “Обеспечение информационной безопасности средствами антивирусной защиты”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М4.1	Применяются ли на всех автоматизированных рабочих местах и серверах АБС организации, если иное не предусмотрено технологическим процессом, средства антивирусной защиты?	обязательный							0,0744	
М4.2	Определены ли в документах организации процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС?	обязательный							0,0721	
М4.3	Осуществляются ли установка и регулярное обновление средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС администраторами АБС или иными официально уполномоченными лицами?	обязательный							0,0653	
М4.4	Организован ли автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных?	рекомендуемый							0,0559	
М4.5	Контролируются ли установка и обновление антивирусных средств представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ?	обязательный							0,0688	
М4.6	Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме?	рекомендуемый							0,0583	
М4.7	Разработаны и введены ли в действие инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов?	обязательный							0,0619	
М4.8	Проводится ли антивирусная фильтрация всего трафика электронного почтового обмена?	обязательный							0,0706	
М4.9	Построена ли в организации эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах?	рекомендуемый							0,0501	
М4.10	Определены ли в документах организации и выполняются ли процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов?	обязательный							0,0605	
М4.11	Проводится ли антивирусная проверка после установки и изменения программного обеспечения?	обязательный							0,0616	
М4.12	Документируются ли результаты установки, изменения программного обеспечения и антивирусной проверки?	обязательный							0,0619	
М4.13	Определены ли в документах организации процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых зафиксированы: — необходимые меры по отражению и устранению последствий вирусной атаки; — порядок официального информирования руководства; — порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки)?	обязательный							0,0651	
М4.14	Определены ли в документах организации и выполняются ли процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АБС?	обязательный							0,0557	
М4.15	Предусматривают ли указанные в частном показателе М4.14 процедуры документальную фиксацию результатов контроля?	обязательный							0,0513	
М4.16	Возложена ли обязанность по выполнению предписанных мер антивирусной защиты на каждого работника организации, имеющего доступ к ЭВМ и (или) АБС, а ответственность за выполнение требований инструкции по антивирусной защите — на руководителей функциональных подразделений организации?	обязательный							0,0665	
Итоговая оценка группового показателя М4										

Групповой показатель М5 “Обеспечение информационной безопасности при использовании ресурсов сети Интернет”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М5.1	Принято ли документально руководством организации решение об использовании сети Интернет для производственной и (или) собственной хозяйственной деятельности, в котором явно перечислены цели использования сети Интернет?	обязательный							0,0586	
М5.2	Запрещается ли использование ресурсов сети Интернет в неустановленных целях?	обязательный							0,0512	
М5.3	Проведено ли в организации выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей?	рекомендуемый							0,0398	
М5.4	Проводится ли наделение работников организации правами пользователя конкретного пакета в соответствии с его должностными обязанностями, в частности, в соответствии с назначенными ему ролями?	рекомендуемый							0,0355	
М5.5	Оформляется ли документально наделение работников организации правами пользователя конкретного пакета?	рекомендуемый							0,0398	
М5.6	Определен ли документально в организации порядок подключения и использования ресурсов сети Интернет, включающий в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственного за обеспечение ИБ?	обязательный							0,0583	
М5.7	Применяются ли при осуществлении дистанционного банковского обслуживания с использованием сети Интернет средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации), которые обеспечивают прием и передачу информации только в установленном формате и только по конкретной технологии?	обязательный							0,0518	
М5.8	Выполнено ли выделение и организована ли физическая изоляция от внутренних сетей тех ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line?	рекомендуемый							0,0292	
М5.9	Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный							0,0479	
М5.10	Регистрируются ли регламентированным образом попытки подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный							0,0440	
М5.11	Все ли операции клиентов в течение сеанса работы с системами дистанционного банковского обслуживания выполняются только после выполнения процедур идентификации, аутентификации и авторизации?	обязательный							0,0581	
М5.12	Обеспечивается ли повторное выполнение процедур идентификации, аутентификации и авторизации в случаях нарушения или разрыва соединения при работе с системами дистанционного банковского обслуживания?	обязательный							0,0415	
М5.13	Используется ли специализированное клиентское программное обеспечение для доступа пользователей к системам дистанционного банковского обслуживания?	рекомендуемый							0,0331	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М5.14	Применяются ли защитные меры для осуществления почтового обмена через сеть Интернет?	обязательный							0,0450	
М5.15	Определены ли в документах организации перечень защитных мер и порядок их использования для осуществления почтового обмена через сеть Интернет?	обязательный							0,0491	
М5.16	Организован ли почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски)?	рекомендуемый							0,0331	
М5.17	Осуществляется ли архивирование электронной почты?	обязательный							0,0368	
М5.18	Доступен ли архив электронной почты подразделению (лицу), ответственному за обеспечение ИБ?	обязательный							0,0368	
М5.19	Не допускаются ли изменения в архиве электронной почты?	обязательный							0,0390	
М5.20	Определен ли документально порядок доступа к информации архива электронной почты?	обязательный							0,0433	
М5.21	Не применяется ли в организации практика хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которой осуществляется взаимодействие с сетью Интернет в режиме on-line?	рекомендуемый							0,0436	
М5.22	Всегда ли наличие банковской информации на ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, определяется бизнес-целями организации и документально санкционируется ее руководством?	обязательный							0,0430	
М5.23	Определены ли документально и используются ли защитные меры, позволяющие обеспечить противодействие атакам хакеров и распространению спама?	обязательный							0,0415	
Итоговая оценка группового показателя М5										

Групповой показатель М6 “Обеспечение информационной безопасности при использовании средств криптографической защиты информации”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М6.1	Проводится ли применение СКЗИ в организации в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией? Имеют ли СКЗИ, применяемые для защиты персональных данных, класс не ниже КС2? Проводятся ли работы по обеспечению безопасности информации с помощью СКЗИ в соответствии с действующими в настоящее время нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России?	обязательный							0,0857	
М6.2	Утверждена ли частная политика, касающаяся применения СКЗИ в организации?	рекомендуемый							0,0628	
М6.3	Допускают ли СКЗИ возможность встраивания в технологические процессы обработки электронных сообщений?	обязательный							0,0628	
М6.4	Обеспечивают ли СКЗИ взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов?	обязательный							0,0628	
М6.5	Поставляются ли СКЗИ разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения?	обязательный							0,0842	
М6.6	Сертифицированы ли СКЗИ уполномоченным государственным органом или имеют ли СКЗИ разрешение ФСБ России?	обязательный							0,0857	
М6.7	Осуществляются ли установка и ввод в эксплуатацию, а также эксплуатация СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам?	обязательный							0,0845	
М6.8	Поддерживается ли непрерывность процессов протоколирования работы СКЗИ при применении СКЗИ?	обязательный							0,0651	
М6.9	Поддерживается ли непрерывность процессов обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований?	обязательный							0,0651	
М6.10	Обеспечивается ли ИБ процессов изготовления криптографических ключей СКЗИ комплексом технологических, организационных, технических и программных мер и средств защиты?	обязательный							0,0776	
М6.11	Реализованы ли процедуры мониторинга, регистрирующие все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ?	рекомендуемый							0,0651	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М6.12	Определен ли руководством на основании указанных в разделе 7.7 СТО БР ИББС-1.0 документов порядок применения СКЗИ, включающий: — порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС; — порядок эксплуатации; — порядок восстановления работоспособности в аварийных случаях; — порядок внесения изменений; — порядок снятия с эксплуатации; — порядок управления ключевой системой; — порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей?	обязательный							0,0671	
М6.13	Самостоятельно ли изготавливаются в организации и (или) клиентом организации ключи СКЗИ?	рекомендуемый							0,0607	
М6.14	Регулируются ли заключаемыми договорами отношения, возникающие между организациями и их клиентами?	обязательный							0,0708	
Итоговая оценка группового показателя М6										

Групповой показатель М7 “Обеспечение информационной безопасности банковских платежных технологических процессов”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М7.1	Определен ли в документах организации банковский платежный технологический процесс?	обязательный							0,0405	
М7.2	Определены ли документально перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских платежных технологических процессов?	обязательный							0,0365	
М7.3	Соответствует ли состав установленного и используемого в ЭВМ и АБС программного обеспечения определенному перечню?	обязательный							0,0389	
М7.4	Контролируется ли выполнение требований, оцениваемых в частных показателях М7.2, М7.3, с документированием результатов контроля?	обязательный							0,0319	
М7.5	Зафиксирован ли порядок обмена платежной информацией в договорах между участниками данного обмена?	обязательный							0,0451	
М7.6	Отсутствуют ли в организации работники, обладающие полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведение несанкционированных операций по изменению состояния банковских счетов?	обязательный							0,0448	
М7.7	Контролируются (проверяются) ли и удостоверяются ли результаты технологических операций по обработке платежной информации лицами / автоматизированными процессами?	обязательный							0,0458	
М7.8	Осуществляется ли обработка платежной информации и контроль (проверка) результатов обработки разными работниками / автоматизированными процессами?	рекомендуемый							0,0442	
М7.9	Возложены ли обязанности по администрированию средств защиты платежной информации приказами или распоряжениями по организации на администраторов ИБ с отражением этих обязанностей в должностных инструкциях?	рекомендуемый							0,0365	
М7.10	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений?	обязательный							0,0436	
М7.11	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса доступ работника организации только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации?	обязательный							0,0384	
М7.12	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации?	обязательный							0,0389	
М7.13	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса аутентификацию входящих электронных платежных сообщений?	обязательный							0,0412	
М7.14	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями?	обязательный							0,0412	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М7.15	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса возможность ввода платежной информации в АБС только для авторизованных пользователей?	обязательный							0,0436	
М7.16	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверку, установление ограничений в зависимости от суммы совершения операций и т.д.)?	обязательный							0,0436	
М7.17	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники?	обязательный							0,0392	
М7.18	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса при осуществлении межбанковских расчетов сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями?	обязательный							0,0436	
М7.19	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса доставку электронных платежных сообщений участникам обмена?	обязательный							0,0408	
М7.20	Организован ли в организации авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип “двойного управления”)?	рекомендуемый							0,0364	
М7.21	Определены ли в документах организации и выполняются ли при проектировании, разработке, эксплуатации систем дистанционного банковского обслуживания процедуры, реализующие механизмы: — снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами; — доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов?	обязательный							0,0337	
М7.22	Обеспечены ли клиенты систем дистанционного банковского обслуживания детальными инструкциями, описывающими процедуры выполнения операций или транзакций?	обязательный							0,0364	
М7.23	Определены ли в документах организации и выполняются ли процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену их программных и (или) аппаратных частей?	обязательный							0,0368	
М7.24	Определена ли в документах организации, согласована ли со службой либо лицом, отвечающим в организации за обеспечение ИБ, и выполняется ли процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации?	обязательный							0,0392	
М7.25	Определена ли в документах организации, согласована ли со службой либо лицом, отвечающим в организации за обеспечение ИБ, и выполняется ли процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации?	обязательный							0,0392	
Итоговая оценка группового показателя М7										

Групповой показатель М8 “Обеспечение информационной безопасности банковских информационных технологических процессов”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М8.1	Проведена ли в организации классификация неплатежной информации?	рекомендуемый							0,0852	
М8.2	Проводится ли классификация неплатежной информации в соответствии со степенью тяжести последствий потери ее свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности?	рекомендуемый							0,0779	
М8.3	Определен ли документально набор требований по защите каждого из типов неплатежных информационных активов (типов неплатежной информации), полученных в результате классификации?	обязательный							0,0970	
М8.4	Возложены ли обязанности по администрированию средств защиты неплатежной информации приказами или распоряжениями по организации на администраторов ИБ с отражением этих обязанностей в должностных инструкциях?	рекомендуемый							0,0814	
М8.5	Определен ли документально порядок контроля функционирования со стороны лиц, отвечающих за ИБ, для каждой АБС организации?	обязательный							0,0777	
М8.6	Определены ли в документах организации банковские информационные технологические процессы, согласованы ли эти документы со службой ИБ организации?	обязательный							0,0740	
М8.7	Реализованы ли банковские информационные технологические процессы в рамках созданных для этих целей АБС?	обязательный							0,0639	
М8.8	Изолированы ли серверы, офисные ЭВМ и другое оборудование, не входящее в состав АБС, реализующих банковские информационные технологические процессы, от указанных АБС на уровне локальных вычислительных сетей способом, согласованным со службой либо лицом, отвечающим в организации за ИБ?	рекомендуемый							0,0758	
М8.9	Определены ли документально перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских информационных технологических процессов?	обязательный							0,0646	
М8.10	Соответствует ли состав установленного и используемого в ЭВМ и АБС программного обеспечения определенному перечню?	обязательный							0,0646	
М8.11	Контролируется ли выполнение требований частных показателей М8.9, М8.10 с документированием результатов контроля?	обязательный							0,0676	
М8.12	Регламентирована ли в документах организации, согласована ли со службой ИБ либо лицом, отвечающим за обеспечение ИБ, и выполняется ли процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ неплатежной информации?	обязательный							0,0889	
М8.13	Регламентирована ли в документах организации, согласована ли со службой ИБ либо лицом, отвечающим за обеспечение ИБ, и выполняется ли процедура восстановления всех реализованных программно-техническими средствами и организационными мерами функций по обеспечению ИБ неплатежной информации?	обязательный							0,0814	
Итоговая оценка группового показателя М8										

Групповой показатель М9 “Общие требования по обработке персональных данных в организации БС РФ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ[1]	Вычисленное значение показателя ИБ[2]
			0	0,25	0,5	0,75	1	н/о		
М9.1	Определены ли в организации, зафиксированы ли документально и утверждены ли руководством организации цели обработки персональных данных?	обязательный								
М9.2	Определена ли в организации необходимость уведомления Уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных?	обязательный								
М9.3	Определены ли в организации для каждой цели обработки персональных данных, зафиксированы ли документально и утверждены ли руководством организации: — объем и содержание персональных данных; — сроки обработки, в том числе сроки хранения персональных данных; — необходимость получения согласия субъектов персональных данных?	обязательный								
М9.4	Проводится ли в организации классификация персональных данных в соответствии со степенью тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных?	рекомендуемый								
М9.5	Выделяются ли при проведении классификации персональных данных следующие категории: — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к специальным категориям персональных данных; — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к биометрическим персональным данным; — персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным; — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к общедоступным или обезличенным персональным данным?	рекомендуемый								
М9.6	Осуществляется ли организацией передача персональных данных третьему лицу с согласия субъекта персональных данных? *В том случае, если организация поручает обработку персональных данных третьему лицу на основании договора* — включается ли в такой договор обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке?	обязательный								

[1] Графа не заполняется.

[2] Вычисленное значение показателя ИБ равно оценке соответствующего частного показателя (столбцы 4–9 таблицы).

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ[1]	Вычисленное значение показателя ИБ[2]
			0	0,25	0,5	0,75	1	н/о		
М9.7	Прекращается ли в организации обработка персональных данных и уничтожаются ли собранные персональные данные в следующих случаях и в сроки, установленные законодательством РФ: — по достижении целей обработки или при утрате необходимости в их достижении; — по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных — если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; — при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ; — при невозможности устранения оператором допущенных нарушений при обработке персональных данных? *Примечание: если иное установлено законодательством РФ, показателю присваивается оценка "н/о".*	обязательный								
М9.8	Определен ли в организации и зафиксирован ли документально порядок уничтожения персональных данных (в том числе и материальных носителей персональных данных)?	обязательный								
М9.9	Определен ли в организации и зафиксирован ли документально порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных?	обязательный								
М9.10	Определен ли в организации и зафиксирован ли документально порядок действий в случае запросов Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных?	обязательный								
М9.11	Определен ли в организации и зафиксирован ли документально подход к отнесению АБС к информационным системам персональных данных (ИСПДн)?	обязательный								
М9.12	Определен ли в организации и зафиксирован ли документально перечень ИСПДн, в который включены как минимум АБС, целью создания и использования которых является обработка персональных данных и не включены АБС, реализующие банковские платежные технологические процессы?	обязательный								
М9.13	Определены ли для каждой ИСПДн организации и зафиксированы ли документально: — цель обработки персональных данных; — объем и содержание обрабатываемых персональных данных; — перечень действий с персональными данными и способы их обработки?	обязательный								
М9.14	Соответствуют ли целям обработки объем и содержание персональных данных в ИСПДн, а также перечень действий и способы обработки персональных данных?	обязательный								
М9.15	Документированы ли в организации банковские информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн?	обязательный								
М9.16	Исключена ли при обработке ПДн в ИСПДн фиксация на одном материальном носителе и персональных данных, и иных видов информационных активов, а также персональных данных, цели обработки которых заведомо несовместимы?	рекомендуемый								

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ[1]	Вычисленное значение показателя ИБ[2]
М9.17	Используется ли при обработке ПДн в ИСПДн для каждой категории персональных данных отдельный материальный носитель? *Примечание: если в ИСПДн обрабатываются ПДн только одной категории, показателю присваивается оценка "н/о".*	рекомендуемый								
М9.18	Определен ли в организации и зафиксирован ли документально перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн либо имеющих доступ к персональным данным? Допускается указание работников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью на основании требований раздела 7.2 СТО БР ИББС-1.0. Возможно существование перечня (списка) в электронном виде при условии предоставления работникам прав доступа в ИСПДн только на основании распорядительного документа в документально зафиксированном в организации порядке.	обязательный								
М9.19	Осуществляется ли доступ работников организации к персональным данным (обработка персональных данных работниками) только для выполнения их должностных обязанностей?	обязательный								
М9.20	Проинформированы ли работники организации, осуществляющие обработку персональных данных в ИСПДн, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также ознакомлены ли работники под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей?	обязательный								
М9.21	Определен ли в организации и зафиксирован ли документально порядок доступа работников организации или иных лиц в помещения, в которых ведется обработка персональных данных?	обязательный								
М9.22	Определен ли в организации и зафиксирован ли документально порядок хранения материальных носителей персональных данных, устанавливающий: — места хранения материальных носителей персональных данных; — требования по обеспечению безопасности персональных данных при хранении их носителей; — работников, ответственных за реализацию требований по обеспечению безопасности персональных данных; — порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных?	обязательный								
М9.23	Соблюдаются ли требования, установленные "Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. № 687, при обработке в организации персональных данных на бумажных носителях, в частности, при использовании в организации БС РФ типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных?	обязательный								
Итоговая оценка группового показателя М9										

Групповой показатель М10 “Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М10.1	Отнесены ли все ИСПДн организации к специальным в соответствии с пунктом 8 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 “Об утверждении Порядка проведения классификации информационных систем персональных данных”?	обязательный							0,2	
М10.2	Определены ли в организации и зафиксированы ли документально критерии классификации ИСПДн, а также порядок проведения классификации ИСПДн?	обязательный							0,2	
М10.3	Проводится ли классификация на основе категорий обрабатываемых в ИСПДн персональных данных?	обязательный							0,2	
М10.4	Определены ли документально и утверждены ли руководством результаты классификации ИСПДн?	обязательный							0,2	
М10.5	Определен ли для каждого класса ИСПДн набор требований по обеспечению безопасности персональных данных на основе требований 7-го и 8-го разделов СТО БР ИББС-1.0, а также при необходимости на основе результатов оценки рисков нарушения безопасности персональных данных?	обязательный							0,2	
Итоговая оценка группового показателя М10										

Групповой показатель М11 “Организация и функционирование службы ИБ организации БС РФ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М11.1	Сформирована ли руководством служба ИБ (назначено ли уполномоченное лицо) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный							0,0816	
М11.2	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный							0,0753	
М11.3	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный							0,0750	
М11.4	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый							0,0530	
М11.5	Сформированы ли для организаций, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	рекомендуемый							0,0615	
М11.6	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации?	обязательный							0,0694	
М11.7	Наделена ли служба ИБ (уполномоченное лицо) полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации?	обязательный							0,0725	
М11.8	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0725	
М11.9	Наделена ли служба ИБ (уполномоченное лицо) полномочиями определять требования к мерам обеспечения ИБ организации?	обязательный							0,0781	
М11.10	Наделена ли служба ИБ (уполномоченное лицо) полномочиями контролировать работников организации в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам?	обязательный							0,0725	
М11.11	Наделена ли служба ИБ (уполномоченное лицо) полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный							0,0725	
М11.12	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации)?	обязательный							0,0787	
М11.13	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?	обязательный							0,0587	
М11.14	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации?	обязательный							0,0787	
Итоговая оценка группового показателя М11										

Групповой показатель М12 “Определение/коррекция области действия СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М12.1	Определена ли в документах организации и корректируется ли опись структурированных по классам защищаемых информационных активов (типов информационных активов — типов информации)?	обязательный							0,1956	
М12.2	Проводится ли классификация информационных активов по типам на основании оценок ценности информационных активов для интересов (целей) организации, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов?	рекомендуемый							0,1614	
М12.3	Содержит ли опись информационных активов информацию о принадлежности конкретного информационного актива к выделенным типам информационных активов (в случае наличия в организации классификации информационных активов)?	обязательный							0,1352	
М12.4	Содержит ли опись информационных активов (типов информационных активов) перечень их объектов среды, покрывающий все уровни информационной инфраструктуры организации, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный							0,1098	
М12.5	Определены ли в документах организации процедуры анализа и пересмотра области действия СОИБ (в частности, процедуры пересмотра при изменении перечня информационных активов организации или типов информационных активов)?	обязательный							0,1276	
М12.6	Определены ли в документах организации роли по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,1352	
М12.7	Назначены ли в организации ответственные за выполнение ролей по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,1352	
Итоговая оценка группового показателя М12										

Групповой показатель М13 “Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М13.1	Принята ли в организации и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный							0,1154	
М13.2	Определены ли в организации критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный							0,1070	
М13.3	Определяет ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ организации способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания: — степени возможности реализации угроз ИБ выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированных в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов организации (типов информационных активов); — степени тяжести последствий от потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности для рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0854	
М13.4	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный							0,0854	
М13.5	Проводится ли оценка рисков нарушения ИБ для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ?	обязательный							0,0676	
М13.6	Создан ли и поддерживается ли в актуальном состоянии единый информационный ресурс (база данных), содержащий информацию об инцидентах ИБ?	рекомендуемый							0,0688	
М13.7	Соотносятся ли величины рисков, полученные в результате оценивания рисков нарушения ИБ, с уровнем допустимого риска, принятого в организации?	обязательный							0,0766	
М13.8	Определен ли в документах организации перечень недопустимых рисков нарушения ИБ, сформированный на основе сравнения полученных в результате оценивания рисков нарушения ИБ величин рисков с уровнем допустимого риска, принятого в организации?	обязательный							0,0766	
М13.9	Определены ли в документах организации роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный							0,0782	
М13.10	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный							0,0782	
М13.11	Определены ли в документах организации роли по оценке рисков нарушения ИБ?	обязательный							0,0782	
М13.12	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный							0,0826	
Итоговая оценка группового показателя М13										

Групповой показатель М14 “Разработка планов обработки рисков нарушения ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М14.1	Определен ли в документах организации по каждому из недопустимых рисков нарушения ИБ план, определяющий один из возможных способов обработки риска: – перенос риска на сторонние организации (например, путем страхования указанного риска); – уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска); – осознанное принятие риска; – формирование требований ИБ, снижающих риск до допустимого уровня, и формирование планов по их реализации?	обязательный							0,1814	
М14.2	Согласованы ли планы обработки рисков нарушения ИБ с руководителем службы ИБ либо лицом, отвечающим в организации за обеспечение ИБ?	обязательный							0,1814	
М14.3	Утверждены ли руководством организации планы обработки рисков нарушения ИБ?	обязательный							0,1814	
М14.4	Содержат ли планы реализации требований ИБ последовательность и сроки реализации и внедрения организационных, технических и иных защитных мер?	обязательный							0,1702	
М14.5	Определены ли в документах организации роли по разработке планов обработки рисков нарушения ИБ?	обязательный							0,1428	
М14.6	Назначены ли ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный							0,1428	
Итоговая оценка группового показателя М14										

Групповой показатель М15 “Определение/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М15.1	Проводятся ли разработка и коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ в организации, с учетом рекомендаций по стандартизации Банка России РС БР ИББС-2.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0”?	рекомендуемый							0,0406	
М15.2	Разработана ли политика ИБ организации? Утверждена ли политика ИБ руководством?	обязательный							0,0628	
М15.3	Корректируется ли политика ИБ организации?	обязательный							0,0557	
М15.4	Разработаны ли частные политики ИБ организации?	обязательный							0,0580	
М15.5	Корректируются ли частные политики ИБ организации?	обязательный							0,0557	
М15.6	Разработаны ли в организации документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ?	обязательный							0,0510	
М15.7	Корректируются ли в организации документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ?	обязательный							0,0489	
М15.8	Определены ли в организации перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ?	обязательный							0,0407	
М15.9	Определены ли в политике ИБ (частных политиках ИБ) организации: — цели и задачи обеспечения ИБ; — основные области обеспечения ИБ; — типы основных защищаемых информационных активов; — модели угроз и нарушителей; — совокупность правил, требований и руководящих принципов в области ИБ; — основные требования к обеспечению ИБ; — принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; — основные принципы повышения уровня осознания и осведомленности в области ИБ; — принципы реализации и контроля выполнения требований политики ИБ?	обязательный								0,0510	
М15.10	Корректируются ли в политике ИБ (частных политиках ИБ) организации: — цели и задачи обеспечения ИБ; — основные области обеспечения ИБ; — типы основных защищаемых информационных активов; — модели угроз и нарушителей; — совокупность правил, требований и руководящих принципов в области ИБ; — основные требования к обеспечению ИБ; — принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; — основные принципы повышения уровня осознания и осведомленности в области ИБ; — принципы реализации и контроля выполнения требований политики ИБ?	обязательный								0,0486	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М15.11	Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства Российской Федерации; — комплекса БР ИББС, в частности, требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0519	
М15.12	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства Российской Федерации; — комплекса БР ИББС, в частности, требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0510	
М15.13	Содержит ли совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, требования по обеспечению ИБ всех выявленных информационных активов (типов информационных активов), находящихся в области действия СОИБ организации?	обязательный							0,0501	
М15.14	Не противоречат ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положениям политики ИБ и частных политик ИБ?	обязательный							0,0510	
М15.15	Детализируют ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положения политики ИБ и частных политик ИБ?	обязательный							0,0426	
М15.16	Утвержден ли руководством организации порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации (в случае наличия в структурных подразделениях организации работников, ответственных за обеспечение ИБ)?	обязательный							0,0354	
М15.17	Определены ли в составе документов, регламентирующих деятельность в области обеспечения ИБ, перечень свидетельств выполнения указанной деятельности и ответственность работников организации за выполнение этой деятельности?	обязательный							0,0426	
М15.18	Определены ли в документах организации процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный							0,0443	
М15.19	Определен ли в документах организации порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0406	
М15.20	Определены ли в документах организации роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0382	
М15.21	Назначены ли ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0393	
Итоговая оценка группового показателя М15										

Групповой показатель М16 “Принятие руководством организации БС РФ решений о реализации и эксплуатации СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М16.1	Оформлены ли документально и утверждены ли руководством решения о реализации и эксплуатации СОИБ, в частности, решения: — об анализе и принятии остаточных рисков нарушения ИБ; — о планировании этапов внедрения СОИБ, в частности, требований ИБ, изложенных в 7-м и 8-м разделах СТО БР ИББС-1.0; — о распределении ролей в области обеспечения ИБ организации; — о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований 7-го и 8-го разделов СТО БР ИББС-1.0 и снижение рисков ИБ; — о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ?	обязательный								0,2752	
М16.2	Утверждены ли руководством все планы внедрения СОИБ, в частности, планы реализации требований 7-го и 8-го разделов СТО БР ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых документально зафиксированы: — последовательность выполнения мероприятий в рамках указанных планов; — сроки начала и окончания запланированных мероприятий; — должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия?	обязательный							0,2812	
М16.3	Определен ли документально порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации?	обязательный							0,2096	
М16.4	Оформлены ли документально решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,2340	
Итоговая оценка группового показателя М16										

Групповой показатель М17 “Организация реализации планов внедрения СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М17.1	Определены ли в документах организации и выполняются ли проектирование/приобретение/развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер (СИБ), предусмотренных планами реализации требований ИБ?	обязательный							0,2540	
М17.2	Реализуются ли при построении элементов СИБ (применительно к конкретной области или сфере деятельности организации) защитные меры, применяемые к объектам среды, в соответствии с существующими в организации требованиями обеспечения ИБ, сформулированными в политике ИБ и других внутренних документах организации?	обязательный							0,2688	
М17.3	Определены ли в документах организации роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный							0,2412	
М17.4	Назначены ли ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный							0,2360	
Итоговая оценка группового показателя М17										

Групповой показатель М18 “Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М18.1	Организована ли документально оформленная работа с персоналом организации в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов? Утверждена ли руководством указанная работа?	обязательный							0,1898	
М18.2	Установлены ли в планах обучения и повышения осведомленности требования к периодичности обучения и повышения осведомленности?	обязательный							0,1378	
М18.3	Включена ли в программы обучения и повышения осведомленности информация: — по существующим политикам ИБ; — по применяемым в организации защитным мерам; — по правильному использованию защитных мер в соответствии с внутренними документами организации; — о значимости и важности деятельности работников для обеспечения ИБ организации?	обязательный							0,1536	
М18.4	Определен ли в организации перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ, в частности: — документы (журналы), подтверждающие прохождение руководителями и работниками организации обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых; — документы, содержащие результаты проверок обучения работников организации; — документы, содержащие результаты проверок осведомленности в области ИБ в организации?	обязательный							0,1184	
М18.5	Организуется ли для работника, получившего новую роль, обучение или инструктаж в области ИБ, соответствующий полученной роли?	обязательный							0,1396	
М18.6	Определены ли в документах организации роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1290	
М18.7	Назначены ли ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1338	
Итоговая оценка группового показателя М18										

Групповой показатель М19 “Организация обнаружения и реагирования на инциденты безопасности”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М19.1	Существуют ли в организации документы, регламентирующие процедуры обработки инцидентов, включающие: — процедуры обнаружения инцидентов ИБ; — процедуры информирования об инцидентах; — процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ; — процедуры реагирования на инцидент; — процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ)?	обязательный							0,1372	
М19.2	Сформирована и поддерживается ли в актуальном состоянии централизованная база инцидентов ИБ?	рекомендуемый							0,1152	
М19.3	Определены ли в документах организации процедуры по хранению информации: — об инцидентах ИБ; — о практиках анализа инцидентов ИБ; — о результатах реагирования на инциденты ИБ?	обязательный							0,1152	
М19.4	Определен ли в документах организации порядок действий работников организации при обнаружении нетипичных событий, связанных с ИБ, и порядок информирования о данных событиях?	обязательный							0,1124	
М19.5	Осведомлены ли работники организации о порядке действий при обнаружении нетипичных событий, связанных с ИБ, и порядке информирования о данных событиях?	обязательный							0,1124	
М19.6	Учитывают ли процедуры расследования инцидентов действующее законодательство Российской Федерации, положения нормативных актов Банка России, а также внутренних документов организации в области ИБ?	обязательный							0,0948	
М19.7	Принимаются и выполняются ли в организации документально оформленные решения по всем выявленным инцидентам ИБ?	обязательный							0,1076	
М19.8	Определены ли в документах организации роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1026	
М19.9	Назначены ли ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1026	
Итоговая оценка группового показателя М19										

Групповой показатель М20 “Организация обеспечения непрерывности бизнеса и его восстановления после прерываний”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М20.1	Выделены ли в описи защищаемых информационных активов организации активы, существенные для обеспечения непрерывности бизнеса организации?	обязательный							0,0876	
М20.2	Определены ли документально в организации требования обеспечения ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0888	
М20.3	Определен ли в документах организации план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации, в состав которого включены: — условия активизации плана; — порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персонала); — процедуры восстановления; — процедуры тестирования и проверки плана; — план обучения и повышения осведомленности работников организации; — обязанности работников организации с указанием ответственных за выполнение каждого из положений плана?	обязательный							0,0907	
М20.4	Основывается ли разработка планов обеспечения непрерывности бизнеса и его восстановления после прерываний на документально оформленных результатах оценки рисков нарушения ИБ организации применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0673	
М20.5	Определены ли документально, реализованы и эксплуатируются ли защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0801	
М20.6	Основываются ли реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания на соответствующих требованиях обеспечения ИБ?	обязательный							0,0758	
М20.7	Согласован ли план обеспечения непрерывности бизнеса и его восстановления после прерываний с существующими в организации процедурами обработки инцидентов ИБ?	обязательный							0,0593	
М20.8	Определено ли в документах организации и выполняется ли периодическое тестирование плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0550	
М20.9	Составлен ли сценарий тестирования плана обеспечения непрерывности бизнеса и его восстановления после прерывания с учетом существующей в организации модели угроз и нарушителей, а также результатов оценки рисков?	обязательный							0,0587	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М20.10	Проводится ли при необходимости корректировка плана обеспечения непрерывности бизнеса и его восстановления после прерывания по результатам тестирования?	обязательный							0,0699	
М20.11	Реализована ли в организации программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний?	обязательный							0,0593	
М20.12	Определены ли в документах организации и выполняются ли процедуры регулярного пересмотра и обновления плана обеспечения непрерывности бизнеса и его восстановления после прерывания (для обеспечения уверенности в их эффективности), учитывающие изменения в приоритетах, целях и интересах бизнеса организации; пересмотр моделей угроз; оценку рисков нарушения ИБ?	обязательный							0,0717	
М20.13	Определены ли в документах организации роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0679	
М20.14	Назначены ли ответственные за выполнение ролей по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0679	
Итоговая оценка группового показателя М20										

Групповой показатель М21 "Мониторинг и контроль защитных мер"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М21.1	Определены ли в документах организации процедуры мониторинга СОИБ и контроля защитных мер (включая контроль параметров конфигурации и настроек средств и механизмов защиты), которые охватывают все реализованные и эксплуатируемые защитные меры, входящие в СИБ, и проводятся персоналом организации, ответственным за обеспечение ИБ?	обязательный							0,1482	
М21.2	Фиксируются ли документально результаты выполнения процедур мониторинга СОИБ и контроля защитных мер?	обязательный							0,1352	
М21.3	Определены ли в документах организации и выполняются ли процедуры сбора и хранения информации о действиях работников организации, событиях и параметрах, имеющих отношение к функционированию защитных мер?	обязательный							0,1068	
М21.4	Включается ли в базу данных инцидентов информация обо всех инцидентах ИБ, выявленных в процессе мониторинга СОИБ и контроля защитных мер?	обязательный							0,1352	
М21.5	Подвергаются ли процедуры мониторинга СОИБ и контроля защитных мер регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ?	обязательный							0,1312	
М21.6	Определен ли в документах организации порядок пересмотра процедур мониторинга СОИБ и контроля защитных мер?	обязательный							0,1066	
М21.7	Определены ли в документах организации роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,1184	
М21.8	Назначены ли ответственные за выполнение ролей, связанных с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,1184	
Итоговая оценка группового показателя М21										

Групповой показатель М22 “Проведение самооценки ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М22.1	Проводится ли самооценка ИБ в соответствии с настоящим стандартом?	обязательный							0,1340	
М22.2	Организован ли порядок проведения самооценки ИБ в соответствии с рекомендациями по стандартизации Банка России РС БР ИББС-2.1 “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”?	рекомендуемый							0,1118	
М22.3	Определена ли в документах организации и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный							0,1026	
М22.4	Определены ли в документах организации: — порядок формирования, сбора и хранения свидетельств самооценки ИБ; — периодичность проведения самооценки ИБ; — порядок хранения и использования результатов самооценки ИБ?	обязательный							0,1098	
М22.5	Оформлен ли в документах организации для каждой проводимой в организации самооценки ИБ план ее проведения, определяющий: — цель самооценки ИБ; — объекты и деятельность, подвергающиеся самооценке ИБ; — порядок и сроки выполнения мероприятий самооценки ИБ; — распределение ролей среди работников организации, связанных с проведением самооценки ИБ?	обязательный							0,0978	
М22.6	Подготавливаются ли по результатам самооценок ИБ отчеты?	обязательный							0,1150	
М22.7	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации?	обязательный							0,1262	
М22.8	Определены ли в документах организации роли, связанные с выполнением программы самооценок ИБ?	обязательный							0,1014	
М22.9	Назначены ли ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный							0,1014	
Итоговая оценка группового показателя М22										

Групповой показатель М23 "Проведение аудита ИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М23.1	Проводится ли аудит ИБ организации в соответствии с требованиями стандарта Банка России СТО БР ИББС-1.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности” и настоящего стандарта?	обязательный							0,1192	
М23.2	Определена ли в документах организации и реализуется ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки?	обязательный							0,0974	
М23.3	Оформлен ли в документах организации для каждого проводимого в организации аудита ИБ план аудита, определяющий: — цель аудита ИБ; — критерии аудита ИБ; — область аудита ИБ; — дату и продолжительность проведения аудита ИБ; — состав аудиторской группы; — описание деятельности и мероприятий по проведению аудита ИБ; — распределение ресурсов при проведении аудита ИБ?	обязательный							0,1112	
М23.4	Оформлены ли договоры с аудиторскими организациями и определены ли в соответствующих документах: — порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ; — порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ; — порядок взаимодействия аудиторской группы и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству; — порядок организации опроса работников; — порядок организации наблюдения за деятельностью работников организации со стороны представителей аудиторской организации?	обязательный							0,1246	
М23.5	Подготавливаются ли по результатам аудитов ИБ отчеты?	обязательный							0,1186	
М23.6	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации?	обязательный							0,1312	
М23.7	Определен ли в документах организации порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности, отчетов аудитов?	обязательный							0,0886	
М23.8	Определены ли в документах организации роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный							0,1046	
М23.9	Назначены ли ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный							0,1046	
Итоговая оценка группового показателя М23										

Групповой показатель М24 “Анализ функционирования СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М24.1	Проводится ли в организации анализ функционирования СОИБ, использующий в том числе: – результаты мониторинга СОИБ и контроля защитных мер; – сведения об инцидентах ИБ; – результаты проведения аудитов ИБ, самооценок ИБ; – данные об угрозах, возможных нарушителях и уязвимостях ИБ; – данные об изменениях внутри организации, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации; – данные об изменениях вне организации, например, данные об изменениях в законодательстве Российской Федерации, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах организации?	обязательный								0,1274	
М24.2	Проводится ли анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации, требованиям законодательства РФ, требованиям стандартов Банка России, контрактным требованиям организации?	обязательный							0,1058	
М24.3	Проводится ли анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в организации, требованиям политик ИБ организации?	обязательный							0,1002	
М24.4	Проводится ли оценка рисков в области ИБ организации, включая оценку уровня остаточного и допустимого рисков?	обязательный							0,0946	
М24.5	Проводится ли проверка адекватности модели угроз организации существующим угрозам ИБ?	обязательный							0,0946	
М24.6	Проводится ли оценка адекватности используемых защитных мер требованиям внутренних документов организации и результатам оценки рисков?	обязательный							0,0930	
М24.7	Проводится ли анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер?	обязательный							0,0822	
М24.8	Документируются ли результаты анализа функционирования СОИБ?	обязательный							0,1026	
М24.9	Определены ли в документах организации роли, связанные с процедурами анализа функционирования СОИБ?	обязательный							0,0998	
М24.10	Назначены ли ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный							0,0998	
Итоговая оценка группового показателя М24										

Групповой показатель М25 “Анализ СОИБ со стороны руководства организации БС РФ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М25.1	Утвержден ли в организации перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный							0,1376	
М25.2	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: — мониторинга СОИБ и контроля защитных мер; — анализа функционирования СОИБ; — аудитов ИБ; — самооценок ИБ?	обязательный							0,1464	
М25.3	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию: — о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; — о новых выявленных уязвимостях и угрозах ИБ; — о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством; — об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России; — о выявленных инцидентах ИБ?	обязательный							0,1318	
М25.4	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков?	обязательный							0,1154	
М25.5	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1228	
М25.6	Определен ли в организации и утвержден ли руководством план выполнения деятельности по контролю и анализу СОИБ, содержащий, в частности, положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации?	обязательный							0,1104	
М25.7	Определены ли в документах организации роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
М25.8	Назначены ли ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
Итоговая оценка группового показателя М25										

Групповой показатель М26 “Принятие решений по тактическим улучшениям СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М26.1	Рассматриваются ли при принятии решений, связанных с тактическими улучшениями СОИБ, документально оформленные результаты: – аудитов ИБ; – самооценок ИБ; – мониторинга СОИБ и контроля защитных мер; – анализа функционирования СОИБ; – обработки инцидентов ИБ; – выявления новых угроз и уязвимостей ИБ; – оценки рисков; – анализа перечня защитных мер, возможных для применения; – стратегических улучшений СОИБ; – анализа СОИБ со стороны руководства; – анализа успешных практик в области ИБ (собственных или других организаций)?	обязательный								0,1354	
М26.2	Оформляются ли документально решения по тактическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо направления тактических улучшений СОИБ?	обязательный							0,1354	
М26.3	Формируются ли направления тактических улучшений СОИБ в виде корректирующих и превентивных действий?	обязательный							0,1216	
М26.4	Определены ли в документах организации планы реализации тактических улучшений СОИБ?	обязательный							0,1354	
М26.5	Существуют ли в организации документы, в которых фиксируются результаты выполнения планов реализации тактических улучшений СОИБ?	обязательный							0,1272	
М26.6	Санкционирует и контролирует ли руководство службы ИБ организации деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный							0,1300	
М26.7	Определены ли в документах организации и выполняются ли процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ? Фиксируются ли результаты выполнения указанных процедур?	обязательный							0,0934	
М26.8	Назначаются ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный							0,1216	
Итоговая оценка группового показателя М26										

Групповой показатель М27 “Принятие решений по стратегическим улучшениям СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М27.1	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, документально оформленные результаты: — аудитов ИБ; — самооценок ИБ; — мониторинга СОИБ и контроля защитных мер; — анализа функционирования СОИБ; — обработки инцидентов ИБ; — выявления новых информационных активов организации или их типов; — выявления новых угроз и уязвимостей ИБ; — оценки рисков; — пересмотра основных рисков ИБ; — анализа СОИБ со стороны руководства; — анализа успешных практик в области ИБ (собственных или других организаций)?	обязательный								0,1130	
М27.2	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, изменения интересов, целей и задач бизнеса организации, контрактных обязательств организации, а также изменения в законодательстве РФ и нормативных актах Банка России?	обязательный							0,1058	
М27.3	Оформляются ли документально решения по стратегическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо направления стратегических улучшений СОИБ?	обязательный							0,0984	
М27.4	Формируются ли направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например: — уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ (частных политик ИБ) организации; — изменения в области действия СОИБ; — уточнение описи типов информационных активов; — пересмотр моделей угроз и нарушителей; — изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ?	обязательный							0,0984	
М27.5	Определены ли в документах организации планы реализации стратегических улучшений СОИБ?	обязательный							0,1016	
М27.6	Существуют ли в организации документы, в которых фиксируются результаты выполнения планов реализации стратегических улучшений СОИБ?	обязательный							0,0962	
М27.7	Санкционирует и контролирует ли руководство организации деятельность, связанную с реализацией стратегических улучшений СОИБ?	обязательный							0,1108	
М27.8	В случае стратегических улучшений СОИБ выполняется ли деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов, в частности, выполняются ли: — выработка планов тактических улучшений СОИБ; — уточнение планов обработки рисков; — уточнение программы внедрения защитных мер; — уточнение процедур использования защитных мер?	обязательный							0,1058	
М27.9	Определены ли в документах организации и выполняются ли процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ? Фиксируются ли документально результаты выполнения указанных процедур?	обязательный							0,0822	
М27.10	Назначаются ли ответственные за реализацию решений по стратегическим улучшениям СОИБ?	обязательный							0,0878	
Итоговая оценка группового показателя М27										

Групповой показатель М28 “Оценка деятельности руководства организации БС РФ по поддержке функционирования службы ИБ организации БС РФ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М28.1 (аналог М11.1)	Сформирована ли руководством служба ИБ (назначено ли уполномоченное лицо) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный							0,0816	
М28.2 (аналог М11.2)	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный							0,0753	
М28.3 (аналог М11.3)	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный							0,0750	
М28.4 (аналог М11.4)	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый							0,0530	
М28.5 (аналог М11.5)	Сформированы ли для организаций, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	рекомендуемый							0,0615	
М28.6 (аналог М11.6)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации?	обязательный							0,0694	
М28.7 (аналог М11.7)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации?	обязательный							0,0725	
М28.8 (аналог М11.8)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0725	
М28.9 (аналог М11.9)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями определять требования к мерам обеспечения ИБ организации?	обязательный							0,0781	
М28.10 (аналог М11.10)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями контролировать работников организации в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам?	обязательный							0,0725	
М28.11 (аналог М11.11)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный							0,0725	
М28.12 (аналог М11.12)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации)?	обязательный							0,0787	
М28.13 (аналог М11.13)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?	обязательный							0,0587	
М28.14 (аналог М11.14)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации?	обязательный							0,0787	
Итоговая оценка группового показателя М28										

Групповой показатель М29 “Оценка деятельности руководства организации БС РФ по принятию решений о реализации и эксплуатации СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М29.1 (аналог М16.1)	Оформлены ли документально и утверждены ли руководством решения о реализации и эксплуатации СОИБ, в частности, решения: — об анализе и принятии остаточных рисков нарушения ИБ; — о планировании этапов внедрения СОИБ, в частности, требований ИБ, изложенных в 7-м и 8-м разделах СТО БР ИББС-1.0; — о распределении ролей в области обеспечения ИБ организации; — о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований 7-го и 8-го разделов СТО БР ИББС-1.0 и снижение рисков ИБ; — о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ?	обязательный								0,2752	
М29.2 (аналог М16.2)	Утверждены ли руководством все планы внедрения СОИБ, в частности, планы реализации требований 7-го и 8-го разделов СТО БР ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых документально зафиксированы: — последовательность выполнения мероприятий в рамках указанных планов; — сроки начала и окончания запланированных мероприятий; — должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия?	обязательный							0,2812	
М29.3 (аналог М16.3)	Определен ли документально порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации?	обязательный							0,2096	
М29.4 (аналог М16.4)	Оформлены ли документально решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,2340	
Итоговая оценка группового показателя М29										

Групповой показатель М30 “Оценка деятельности руководства организации БС РФ по поддержке планирования СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М30.1 (аналог М12.1)	Определена ли в документах организации и корректируется ли опись структурированных по классам защищаемых информационных активов (типов информационных активов — типов информации)?	обязательный							0,0386	
М30.2 (аналог М12.6)	Определены ли в документах организации роли по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,0364	
М30.3 (аналог М12.7)	Назначены ли в организации ответственные за выполнение ролей по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,0364	
М30.4 (аналог М13.1)	Принята ли в организации и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный							0,0386	
М30.5 (аналог М13.2)	Определены ли в организации критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный							0,0386	
М30.6 (аналог М13.4)	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный							0,0345	
М30.7 (аналог М13.9)	Определены ли в документах организации роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный							0,0364	
М30.8 (аналог М13.10)	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный							0,0364	
М30.9 (аналог М13.11)	Определены ли в документах организации роли по оценке рисков нарушения ИБ?	обязательный							0,0345	
М30.10 (аналог М13.12)	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный							0,0345	
М30.11 (аналог М14.3)	Утверждены ли руководством организации планы обработки рисков нарушения ИБ?	обязательный							0,0364	
М30.12 (аналог М14.5)	Определены ли в документах организации роли по разработке планов обработки рисков нарушения ИБ?	обязательный							0,0345	
М30.13 (аналог М14.6)	Назначены ли ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный							0,0364	
М30.14 (аналог М15.2)	Разработана ли политика ИБ организации? Утверждена ли политика ИБ руководством?	обязательный							0,0408	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М30.15 (аналог М15.3)	Корректируется ли политика ИБ организации?	обязательный							0,0386	
М30.16 (аналог М15.4)	Разработаны ли частные политики ИБ организации?	обязательный							0,0408	
М30.17 (аналог М15.5)	Корректируются ли частные политики ИБ организации?	обязательный							0,0364	
М30.18 (аналог М15.9)	Определены ли в политике ИБ (частных политиках ИБ) организации: — цели и задачи обеспечения ИБ; основные области обеспечения ИБ; — типы основных защищаемых информационных активов; — модели угроз и нарушителей; — совокупность правил, требований и руководящих принципов в области ИБ; — основные требования к обеспечению ИБ; — принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; — основные принципы повышения уровня осознания и осведомленности в области ИБ; — принципы реализации и контроля выполнения требований политики ИБ?	обязательный								0,0386	
М30.19 (аналог М15.10)	Корректируются ли в политике ИБ (частных политиках ИБ) организации: — цели и задачи обеспечения ИБ; основные области обеспечения ИБ; — типы основных защищаемых информационных активов; — модели угроз и нарушителей; — совокупность правил, требований и руководящих принципов в области ИБ; — основные требования к обеспечению ИБ; — принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; — основные принципы повышения уровня осознания и осведомленности в области ИБ; — принципы реализации и контроля выполнения требований политики ИБ?	обязательный								0,0364	
М30.20 (аналог М15.11)	Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства Российской Федерации; — комплекса БР ИББС, в частности, требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0408	
М30.21 (аналог М15.12)	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства Российской Федерации; — комплекса БР ИББС, в частности, требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0386	

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М30.22 (аналог М15.16)	**Утвержден ли руководством организации порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации (в случае наличия в структурных подразделениях организации работников, ответственных за обеспечение ИБ)?**	**обязательный**							**0,0345**	
М30.23 (аналог М15.18)	**Определены ли в документах организации процедуры выделения и распределения ролей в области обеспечения ИБ?**	**обязательный**							**0,0345**	
М30.24 (аналог М15.20)	**Определены ли в документах организации роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?**	**обязательный**							**0,0386**	
М30.25 (аналог М15.21)	**Назначены ли ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?**	**обязательный**							**0,0364**	
М30.26 (аналог М17.3)	**Определены ли в документах организации роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?**	**обязательный**							**0,0364**	
М30.27 (аналог М17.4)	**Назначены ли ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?**	**обязательный**							**0,0364**	
Итоговая оценка группового показателя М30										

Групповой показатель М31 “Оценка деятельности руководства организации БС РФ по поддержке реализации СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М31.1 (аналог М18.1)	Организована ли документально оформленная работа с персоналом организации в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов? Утверждена ли руководством указанная работа?	обязательный							0,1442	
М31.2 (аналог М18.6)	Определены ли в документах организации роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1024	
М31.3 (аналог М18.7)	Назначены ли ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1024	
М31.4 (аналог М19.8)	Определены ли в документах организации роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1404	
М31.5 (аналог М19.9)	Назначены ли ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1268	
М31.6 (аналог М20.3)	Определен ли в документах организации план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации, в состав которого включены: — условия активизации плана; — порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персонала); — процедуры восстановления; — процедуры тестирования и проверки плана; — план обучения и повышения осведомленности работников организации; — обязанности работников организации с указанием ответственных за выполнение каждого из положений плана?	обязательный							0,1442	
М31.7 (аналог М20.13)	Определены ли в документах организации роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1198	
М31.8 (аналог М20.14)	Назначены ли ответственные за выполнение ролей по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1198	
Итоговая оценка группового показателя М31										

Групповой показатель М32 “Оценка деятельности руководства организации БС РФ по поддержке проверки СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М32.1 (аналог М21.7)	Определены ли в документах организации роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,0921	
М32.2 (аналог М21.8)	Назначены ли ответственные за выполнение ролей, связанных с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,0921	
М32.3 (аналог М22.3)	Определена ли в документах организации и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный							0,0848	
М32.4 (аналог М22.7)	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации?	обязательный							0,0943	
М32.5 (аналог М22.8)	Определены ли в документах организации роли, связанные с выполнением программы самооценок ИБ?	обязательный							0,0734	
М32.6 (аналог М22.9)	Назначены ли ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный							0,0734	
М32.7 (аналог М23.2)	Определена ли в документах организации и реализована ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки?	обязательный							0,0808	
М32.8 (аналог М23.6)	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации?	обязательный							0,0969	
М32.9 (аналог М23.8)	Определены ли в документах организации роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный							0,0805	
М32.10 (аналог М23.9)	Назначены ли ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный							0,0805	
М32.11 (аналог М24.9)	Определены ли в документах организации роли, связанные с процедурами анализа функционирования СОИБ?	обязательный							0,0756	
М32.12 (аналог М24.10)	Назначены ли ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный							0,0756	
Итоговая оценка группового показателя М32										

Групповой показатель М33 “Оценка деятельности руководства организации БС РФ по анализу СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М33.1 (аналог М25.1)	Утвержден ли в организации перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный							0,1376	
М33.2 (аналог М25.2)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: — мониторинга СОИБ и контроля защитных мер; — анализа функционирования СОИБ; — аудитов ИБ; — самооценок ИБ?	обязательный							0,1464	
М33.3 (аналог М25.3)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию: — о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; — о новых выявленных уязвимостях и угрозах ИБ; — о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством; — об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России; — о выявленных инцидентах ИБ?	обязательный							0,1338	
М33.4 (аналог М25.4)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков?	обязательный							0,1154	
М33.5 (аналог М25.5)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1228	
М33.6 (аналог М25.6)	Определен ли в организации и утвержден ли руководством план выполнения деятельности по контролю и анализу СОИБ, содержащий, в частности, положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации?	обязательный							0,1104	
М33.7 (аналог М25.7)	Определены ли в документах организации роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
М33.8 (аналог М25.8)	Назначены ли ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
Итоговая оценка группового показателя М33										

Групповой показатель М34 "Оценка деятельности руководства по поддержке совершенствования СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М34.1 (аналог М26.6)	Санкционирует и контролирует ли руководство службы ИБ организации деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный							0,2560	
М34.2 (аналог М26.8)	Назначаются ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный							0,2248	
М34.3 (аналог М27.7)	Санкционирует и контролирует ли руководство организации деятельность, связанную с реализацией стратегических улучшений СОИБ?	обязательный							0,2816	
М34.4 (аналог М27.10)	Назначаются ли ответственные за реализацию решений по стратегическим улучшениям СОИБ?	обязательный							0,2376	
Итоговая оценка группового показателя М34										

Приложение Б
(обязательное)

Форма листов для сбора свидетельств аудита ИБ

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

_____
(подпись)

_____
(подпись)

_____
(подпись)

Приложение В
(обязательное)

Уточняющие вопросы частных показателей ИБ для оценки степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в ИСПДн

Таблица 1. Уточняющие вопросы частных показателей ИБ

№ уточняющего вопроса	Пункт РС БР ИББС-2.3	Уточняющий вопрос	Частный показатель СТО БР ИББС-1.2
1	5.2	Отнесена ли каждая информационная система персональных данных (ИСПДн) организации к одному из следующих классов – ИСПДн-С, ИСПДн-Б, ИСПДн-И, ИСПДн-Д[1]?	М10.2, М10.3, М12.2, М12.3, М12.4
2	6.1.1	Реализуются ли требования по обеспечению безопасности персональных данных в ИСПДн комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации? Осуществляется ли реализация требований и (или) организуется ли выполнение требований по обеспечению безопасности персональных данных структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных, либо на договорной основе организацией – контрагентом организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации? *Допускается возложение ответственности за организацию работы по обеспечению безопасности персональных данных на существующее в организации подразделение (например, на службу ИБ).* Осуществляется ли реализация требований по обеспечению безопасности ПДн по согласованию и под контролем службы ИБ организации?	М2.1, М2.2, М2.3, М2.4
3	6.1.2	Включает ли создание ИСПДн организации разработку и согласование (утверждение) предусмотренной техническим заданием организационно-распорядительной, проектной и эксплуатационной документации на создаваемую систему (в документации должны быть отражены вопросы обеспечения безопасности обрабатываемых персональных данных)? Осуществляются ли разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн по согласованию и под контролем структурного подразделения или должностного лица (работника) организации, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации?	М2.1, М2.2, М2.3, М2.5, М2.6, М8.3, М8.5, М15.6, М15.7
4	6.1.3	Защищены ли от воздействий вредоносного кода все информационные активы, принадлежащие ИСПДн организации? Определены ли в организации и зафиксированы ли документально требования по обеспечению безопасности персональных данных средствами антивирусной защиты и порядок проведения контроля реализации этих требований в соответствии с требованиями пункта 7.5 СТО БР ИББС-1.0?	М4.1, М4.5
5	6.1.4	Определена ли в организации система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн?	М3.5, М3.6, М3.7, М3.8
6	6.1.5	Действуют ли работники, осуществляющие обработку персональных данных в ИСПДн, в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдают ли работники требования документов организации по обеспечению ИБ?	М1.1, М1.3, М1.4, М1.19, М16.1, М29.1

[1] Классы ИСПДн:

ИСПДн-С – ИСПДн обработки специальных категорий персональных данных;

ИСПДн-Б – ИСПДн обработки биометрических персональных данных;

ИСПДн-И – ИСПДн обработки персональных данных, не являющихся биометрическими и не относящихся к специальным категориям, доступ к которым должен быть ограничен;

ИСПДн-Д – ИСПДн обработки общедоступных и (или) обезличенных персональных данных.

№ уточняющего вопроса	Пункт РС БР ИББС-2.3	Уточняющий вопрос	Частный показатель СТО БР ИББС-1.2
7	6.1.6	Возложены ли приказами (распоряжениями) обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению ИБ ИСПДн организации, на администраторов информационной безопасности ИСПДн?	М1.1, М1.3, М1.4, М8.4, М8.5, М15.6, М15.7, М15.8
8	6.1.7	Определен ли порядок действий администратора информационной безопасности ИСПДн и персонала, занятых в процессе обработки персональных данных, инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн? Выполняются ли следующие требования к таким инструкциям (руководствам): – устанавливают требования к квалификации администратора информационной безопасности и персонала в области защиты информации, а также актуальный перечень защищаемых объектов и правила его обновления; – содержат в полном объеме актуальные (по времени) данные о полномочиях пользователей; – содержат данные о технологии обработки информации в объеме, необходимом для администратора информационной безопасности; – устанавливают порядок и периодичность анализа журналов регистрации событий (архивов журналов)? Определены ли в эксплуатационной документации на ИСПДн параметры конфигурации средств защиты и механизмов защиты информации от НСД, используемых в зоне ответственности администратора информационной безопасности? Установлены ли в эксплуатационной документации или регламентированы ли внутренним документом организации порядок и периодичность проверок установленных параметров конфигурации (при этом проверки должны проводиться не реже чем раз в год)?	М1.1, М1.3, М1.4, М1.13, М1.14, М2.5, М2.6, М2.11, М2.12, М3.2, М3.11, М3.12, М3.14, М3.15, М3.16, М3.17, М8.5, М8.12, М15.6, М15.7, М15.8, М21.1, М21.7, М21.8, М32.1, М32.2
9	6.1.8	Определен ли в организации и зафиксирован ли документально порядок доступа в помещения, в которых размещаются технические средства ИСПДн и хранятся носители персональных данных, предусматривающий контроль доступа в помещения посторонних лиц и наличие препятствий для несанкционированного проникновения в помещения? Разработан ли указанный порядок структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение режима физической безопасности организации БС РФ и согласован ли структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и со службой ИБ организации?	М3.18, М3.19, М3.20, М11.9, М28.9
10	6.1.9	Запрещено ли организационно-техническими мерами в помещениях, в которых размещаются технические средства ИСПДн, несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных, в том числе с использованием отчуждаемых носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки?	М15.6, М15.8, М21.1, М21.7, М32.1
11	6.2.1	Регламентируются ли в проектной и эксплуатационной документации процессы обработки персональных данных, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств?	М2.1, М8.6, М15.6, М15.7
12	6.2.2	Обеспечиваются ли идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов? Ограничено ли при наличии технической возможности количество последовательных неудачных попыток ввода пароля (от 3 до 5 попыток)? Блокируют ли при превышении указанного количества средства защиты и механизмы защиты возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности? Регламентируются ли порядок формирования и смены паролей, а также порядок контроля исполнения этих процедур разработчиком ИСПДн в эксплуатационной документации в инструкциях (руководствах) администраторов информационной безопасности?	М3.5, М3.6, М3.7, М3.8, М15.6, М15.8

№ уточняющего вопроса	Пункт РС БР ИББС-2.3	Уточняющий вопрос	Частный показатель СТО БР ИББС-1.2
13	6.2.3	Осуществляется ли передача персональных данных только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию со структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных?	М3.9, М5.1, М5.15, М5.23, М11.9, М28.9
14	6.3.2	Обеспечивается ли выполнение функций обеспечения безопасности персональных данных в ИСПДн средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО)?	М2.1, М3.4
15	6.3.3	Выполнены ли разработчиком ИСПДн на стадии ввода в действие настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий? Определен ли разработчиком ИСПДн порядок постоянного контроля фактического состояния настроек средств и механизмов обеспечения безопасности на предмет их соответствия установленным правилам? Согласован ли указанный порядок со структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных, и согласован ли со службой ИБ организации?	М3.4, М11.9, М21.1, М28.9
16	6.3.4	Выполняется ли в обязательном порядке регистрация входа в ИСПДн (выхода из ИСПДн) субъектов доступа? Указываются ли в журнале регистрации событий, который ведется в электронном виде ИСПДн, следующие параметры: – дата и время входа в систему (выхода из системы) субъекта доступа; – идентификатор субъекта, предъявленный при запросе доступа; – результат попытки входа: успешная или неуспешная (несанкционированная); – идентификатор (адрес) устройства (компьютера), используемого для входа в систему?	М3.11, М3.12
17	6.3.6	Определен ли в организации и зафиксирован ли документально порядок постановки на учет и снятия с учета машинных носителей, предназначенных для размещения персональных данных? Проводится ли снятие с учета машинных носителей, на которых были размещены персональные данные, по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения? Регламентируется ли разработчиком ИСПДн в эксплуатационной документации на ИСПДн процедура стирания информации в зависимости от применяемого средства гарантированного стирания? Осуществляется ли (при наличии технической возможности) очистка освобождаемых областей памяти на носителях, ранее использованных для хранения персональных данных?	М2.16, М2.17, М3.1, М3.11, М3.12, М8.1, М8.6, М8.7, М12.2, М12.3, М17.2
18	6.3.7	Определены ли в соответствии с требованиями пункта 7.9.7 СТО БР ИББС-1.0 и зафиксированы ли документально состав и назначение ПО ИСПДн?	М2.13, М2.14, М8.9, М8.10
19	6.3.8	Регламентирован ли порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО? Учтены ли эталонные копии ПО, регламентирован ли доступ к ним? Готовятся ли разработчиком ИСПДн соответствующие регламенты в виде инструкций, руководств и включаются ли в эксплуатационную документацию на ИСПДн?	М2.1, М2.13, М2.14, М15.6, М15.7, М15.8
20	6.3.9	Подлежат ли резервному копированию все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн? Предусматривают ли средства восстановления функций обеспечения безопасности персональных данных в ИСПДн ведение не менее двух независимых копий программных средств? Регламентирован ли порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий, разработчиком ИСПДн в эксплуатационной документации на ИСПДн?	М2.13, М2.14, М8.13, М20.3, М20.5

№ уточняющего вопроса	Пункт РС БР ИББС-2.3	Уточняющий вопрос	Частный показатель СТО БР ИББС-1.2
21	6.3.10	Осуществляется ли (в случае нештатной ситуации) восстановление функций обеспечения безопасности персональных данных в ИСПДн администратором ИСПДн с обязательным привлечением администратора информационной безопасности ИСПДн (при необходимости – с привлечением специалистов структурного подразделения или должностного лица (работника) организации, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации)? Регламентирована ли разработчиком ИСПДн в эксплуатационной документации на ИСПДн процедура восстановления?	М1.1, М1.3, М1.4, М2.5, М2.6, М2.13, М8.4, М8.5, М8.13, М20.2
22	6.3.11	Осуществляется ли подключение ИСПДн к ИСПДн другого класса или к сети Интернет с использованием средств межсетевого экранирования (межсетевых экранов), которые обеспечивают выполнение следующих функций: – фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов); – идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия; – регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана); – возможность проверки (контроля) целостности программной и информационной части средства межсетевого экранирования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования); – фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств; – восстановление свойств межсетевого экрана после сбоев и отказов оборудования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования); – возможность проведения регламентного тестирования реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования)?	М5.1, М5.15, М5.23
23	6.4.1	Выполняются ли для информационных систем обработки биометрических персональных данных требования, установленные Постановлением Правительства от 6 июля 2008 г. № 512 “Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных”?	М2.5, М2.6, М3.1, М3.3, М3.4, М3.7, М3.8, М3.9, М3.10, М3.11, М3.12, М6.3, М6.4, М8.1, М8.7, М11.9, М12.2, М12.3, М17.2, М28.9
24	6.5.2	Осуществляется ли идентификация по логическим именам информационных ресурсов (например, информационных массивов, баз данных, файлов, обрабатывающих их программ), содержащих персональные данные?	М3.4, М3.5
25	6.5.3	Осуществляется ли обязательный контроль доступа субъектов к защищаемым информационным ресурсам в соответствии с правами доступа указанных субъектов?	М3.2, М3.4, М3.5, М3.6, М3.7, М3.8
26	6.5.4	Выполняется ли в обязательном порядке регистрация печати материалов, содержащих персональные данные? Указываются ли в журнале регистрации событий, который ведется в электронном виде ИСПДн, следующие параметры: – дата и время печати; – спецификация устройства печати (логическое имя (номер) внешнего устройства); – полное наименование (вид, шифр, код) материала; – идентификатор субъекта доступа, запросившего печать материала; – объем фактически отпечатанного материала (количество страниц, листов, копий) и результат печати: успешная (весь объем) или неуспешная?	М3.11, М3.12

№ уточняющего вопроса	Пункт РС БР ИББС-2.3	Уточняющий вопрос	Частный показатель СТО БР ИББС-1.2
27	6.5.5	Выполняется ли обязательная регистрация запуска программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам? Указываются ли в журнале регистрации событий, который ведется в электронном виде ИСПДн, следующие параметры: – дата и время запуска; – имя (идентификатор) программы (процесса, задания); – идентификатор субъекта доступа, запросившего программу (процесс, задание); – результат попытки запуска: успешная или неуспешная (несанкционированная); – дата и время попытки доступа к защищаемому информационному ресурсу; – имя (идентификатор) защищаемого информационного ресурса; – вид запрашиваемой операции (например, чтение, запись, модификация, удаление); – результат попытки доступа: успешная или неуспешная (несанкционированная)?	М3.11, М3.12
28	6.5.6	Выполняется ли обязательная регистрация изменений полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов)? Указываются ли в журнале регистрации событий, который ведется в электронном виде ИСПДн, следующие параметры: – дата и время изменения; – содержание изменения с указанием идентификатора субъекта доступа, чьи полномочия подверглись изменению, или логического имени защищаемого информационного ресурса, чей статус изменился; – идентификатор администратора информационной безопасности, осуществившего изменение?	М3.11, М3.12
29	6.3.5 6.5.7	Не имеют ли ИСПДн субъектов доступа, обладающих полномочиями, а при возможности и техническими средствами по уничтожению и модификации информации, содержащейся в журналах регистрации событий, указанных в пунктах 6.3.4, 6.5.4–6.5.6 РС БР ИББС-2.3? Регламентирована ли очистка журналов регистрации событий, указанных в пунктах 6.3.4, 6.5.4–6.5.6 РС БР ИББС-2.3, разработчиком ИСПДн в эксплуатационной документации на ИСПДн? Проводится ли перед очисткой журналов регистрации событий, указанных в пунктах 6.3.4, 6.5.4–6.5.6 РС БР ИББС-2.3, архивирование содержащейся в них информации путем перемещения информации в соответствующий архив? Регистрируются ли операции по архивированию журнала регистрации событий, указанных в пунктах 6.3.4, 6.5.4–6.5.6 РС БР ИББС-2.3, с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий? Уничтожаются ли архивы журналов регистрации событий, указанных в пунктах 6.3.4, 6.5.4–6.5.6 РС БР ИББС-2.3, только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы не ранее чем через три года с момента появления последней записи в данной архивной копии?	М1.9, М3.11, М3.12, М8.4, М8.5, М15.6, М15.8
30	6.5.8	*В случае, если комплекс средств автоматизации ИСПДн представляет собой автономное, изолированное на физическом уровне в соответствии с эталонной моделью взаимодействия открытых систем – моделью OSI, автоматизированное рабочее место (АРМ) работника или работников* – исключены ли из ИСПДн программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения)? *В случае, если стандартные программные средства общего назначения (например, MS Office), не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО* – введен ли документально запрет использования отдельных компонент (средств разработки и отладки ПО) стандартных программных средств общего назначения (например, MS Office)?	М2.1, М2.13

№ уточняющего вопроса	Пункт РС БР ИББС-2.3	Уточняющий вопрос	Частный показатель СТО БР ИББС-1.2
31	6.5.9	*В случае, если комплекс средств автоматизации ИСПДн включает одно или несколько сетевых АРМ, сетевого оборудования и серверов* – располагаются ли технические и программные средства, предназначенные для разработки и отладки ПО либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения, в сегментах локальной вычислительной сети (ЛВС), изолированных (на уровне не выше сетевого в соответствии с эталонной моделью взаимодействия открытых систем – моделью OSI) от сегментов, задействованных в обработке персональных данных? Регламентированы ли разработчиком в эксплуатационной документации на ИСПДн параметры настроек технических и программных средств, обеспечивающих указанное разделение, а также процедура контроля этих параметров настроек? *В случае, если стандартные программные средства общего назначения (например, MS Office) не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО* – введен ли документально запрет использования отдельных компонент (средств разработки и отладки ПО) стандартных программных средств общего назначения (например, MS Office), использующихся в сегментах, задействованных в обработке персональных данных?	М2.7, М2.10, М8.8, М8.12
32	6.5.10	*В случае осуществления передачи персональных данных между подразделениями организации по телекоммуникационным каналам и линиям связи, не принадлежащим организации или не пролегающим только по территории организации* – осуществляется ли такая передача только при обеспечении защиты персональных данных с помощью организации виртуальных частных сетей (Virtual Private Network – VPN) или иных защитных мер, механизмов и средств, применение которых определяется структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных, и согласовывается со службой ИБ организации?	М3.4, М6.1
33	6.5.11	*В случае осуществления передачи персональных данных по телекоммуникационным каналам и линиям связи между подразделениями организации, с одной стороны, и внешними организациями, с другой стороны* – осуществляется ли такая передача с использованием сертифицированных СКЗИ или иных защитных механизмов, применение которых определяется структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных, и согласовывается со службой ИБ организации? *В случае использования СКЗИ* – выполняются ли требования нормативных правовых актов ФСБ России? *В случае обмена информацией с другой организацией* – определены ли соглашением сторон (в частности, условиями договора) правила использования СКЗИ? *В случае отсутствия указанной технической возможности* – осуществляется ли передача персональных данных в электронном виде на съемных носителях в порядке, согласованном со структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных, и со службой ИБ организации?	М3.4, М6.1, М11.9
34	6.5.12	Осуществляется ли подключение ИСПДн к ИСПДн другого класса или к сети Интернет с использованием средств межсетевого экранирования (межсетевых экранов), которые имеют подтвержденный сертификатом класс защиты не ниже четвертого при возможности информационного обмена между всеми компонентами защищаемой ИСПДн без использования компонентов других автоматизированных банковских систем организации (в иных случаях – не ниже третьего класса)? *Указанные классы защиты устанавливаются в соответствии с руководящим документом "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации",* утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 года.	М3.4, М5.1, М5.15, М5.23

Таблица 2. Таблица соответствия частных показателей и положений РС БР ИББС-2.3

СТО БР ИББС-1.2	Класс ИСПДн	РС БР ИББС-2.3
М1.1	ИСПДн-Д	6.1.5, 6.1.6, 6.1.7
	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.1.5, 6.1.6, 6.1.7, 6.3.10
М1.3	ИСПДн-Д	6.1.5, 6.1.6, 6.1.7
	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.1.5, 6.1.6, 6.1.7, 6.3.10
М1.4	ИСПДн-Д	6.1.5, 6.1.6, 6.1.7
	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.1.5, 6.1.6, 6.1.7, 6.3.10
М1.9	ИСПДн-И	6.3.5
	ИСПДн-Б	6.3.5
	ИСПДн-С	6.3.5, 6.5.7
М1.13	Все классы	6.1.7
М1.14	Все классы	6.1.7
М1.19	Все классы	6.1.5
М2.1	ИСПДн-Д	6.1.1, 6.1.2, 6.2.1
	ИСПДн-И, ИСПДн-Б	6.1.1, 6.1.2, 6.2.1, 6.3.2, 6.3.8
	ИСПДн-С	6.1.1, 6.1.2, 6.2.1, 6.3.2, 6.3.8, 6.5.8
М2.2	Все классы	6.1.1, 6.1.2
М2.3	Все классы	6.1.1, 6.1.2
М2.4	Все классы	6.1.1
М2.5	ИСПДн-Д	6.1.2, 6.1.7
	ИСПДн-И, ИСПДн-С	6.1.2, 6.1.7, 6.3.10
	ИСПДн-Б	6.1.2, 6.1.7, 6.3.10, 6.4.1
М2.6	ИСПДн-Д	6.1.2, 6.1.7
	ИСПДн-И, ИСПДн-С	6.1.2, 6.1.7, 6.3.10
	ИСПДн-Б	6.1.2, 6.1.7, 6.3.10, 6.4.1
М2.7	ИСПДн-С	6.5.9
М2.10	ИСПДн-С	6.5.9
М2.11	Все классы	6.1.7
М2.12	Все классы	6.1.7
М2.13	ИСПДн-И, ИСПДн-Б	6.3.7, 6.3.8, 6.3.9, 6.3.10
	ИСПДн-С	6.3.7, 6.3.8, 6.3.9, 6.3.10, 6.5.8
М2.14	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.7, 6.3.8, 6.3.9
М2.16	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.6
М2.17	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.6
М3.1	ИСПДн-И, ИСПДн-С	6.3.6
	ИСПДн-Б	6.3.6, 6.4.1
М3.2	ИСПДн-Д, ИСПДн-И, ИСПДн-Б	6.1.7
	ИСПДн-С	6.1.7, 6.5.3
М3.3	ИСПДН-Б	6.4.1
М3.4	ИСПДн-И	6.3.2, 6.3.3
	ИСПДн-Б	6.3.2, 6.3.3, 6.4.1
	ИСПДн-С	6.3.2, 6.3.3, 6.4.1, 6.5.2, 6.5.3, 6.5.10, 6.5.11, 6.5.12
М3.5	ИСПДн-Д, ИСПДн-И, ИСПДн-Б	6.1.4, 6.2.2
	ИСПДн-С	6.1.4, 6.2.2, 6.5.2, 6.5.3
М3.6	ИСПДн-Д, ИСПДн-И, ИСПДн-Б	6.1.4, 6.2.2
	ИСПДн-С	6.1.4, 6.2.2, 6.5.3
М3.7	ИСПДн-Д, ИСПДн-И	6.1.4, 6.2.2
	ИСПДн-Б	6.1.4, 6.2.2, 6.4.1
	ИСПДн-С	6.1.4, 6.2.2, 6.5.3
М3.8	ИСПДн-Д, ИСПДн-И	6.1.4, 6.2.2
	ИСПДн-Б	6.1.4, 6.2.2, 6.4.1
	ИСПДн-С	6.1.4, 6.2.2, 6.5.3

СТО БР ИББС-1.2	Класс ИСПДн	РС БР ИББС-2.3
М3.9	ИСПДн-Д, ИСПДн-И, ИСПДн-С	6.2.3
	ИСПДн-Б	6.2.3, 6.4.1
М3.10	ИСПДн-Б	6.4.1
М3.11	ИСПДн-Д	6.1.7
	ИСПДн-И	6.1.7, 6.3.4, 6.3.5, 6.3.6
	ИСПДн-Б	6.1.7, 6.3.4, 6.3.5, 6.3.6, 6.4.1
	ИСПДн-С	6.1.7, 6.3.4, 6.3.5, 6.3.6, 6.5.4, 6.5.5, 6.5.6, 6.5.7
М3.12	ИСПДн-Д	6.1.7
	ИСПДн-И	6.1.7, 6.3.4, 6.3.5, 6.3.6
	ИСПДн-Б	6.1.7, 6.3.4, 6.3.5, 6.3.6, 6.4.1
	ИСПДн-С	6.1.7, 6.3.4, 6.3.5, 6.3.6, 6.5.4, 6.5.5, 6.5.6, 6.5.7
М3.14	Все классы	6.1.7
М3.15	Все классы	6.1.7
М3.16	Все классы	6.1.7
М3.17	Все классы	6.1.7
М3.18	Все классы	6.1.8
М3.19	Все классы	6.1.8
М3.20	Все классы	6.1.8
М4.1	Все классы	6.1.3
М4.5	Все классы	6.1.3
М5.1	ИСПДн-Д	6.2.3
	ИСПДн-И, ИСПДн-Б	6.2.3, 6.3.11
	ИСПДн-С	6.2.3, 6.3.11, 6.5.12
М5.15	ИСПДн-Д	6.2.3
	ИСПДн-И, ИСПДн-Б	6.2.3, 6.3.11
	ИСПДн-С	6.2.3, 6.3.11, 6.5.12
М5.23	ИСПДн-Д	6.2.3
	ИСПДн-И, ИСПДн-Б	6.2.3, 6.3.11
	ИСПДн-С	6.2.3, 6.3.11, 6.5.12
М6.1	ИСПДн-С	6.5.10, 6.5.11
М6.3	ИСПДн-Б	6.4.1
М6.4	ИСПДн-Б	6.4.1
М8.1	ИСПДн-И, ИСПДн-С	6.3.6
	ИСПДн-Б	6.3.6, 6.4.1
М8.3	Все классы	6.1.2
М8.4	ИСПДн-Д	6.1.6
	ИСПДн-И, ИСПДн-Б	6.1.6, 6.3.5, 6.3.10
	ИСПДн-С	6.1.6, 6.3.5, 6.3.10, 6.5.7
М8.5	ИСПДн-Д	6.1.2, 6.1.6, 6.1.7
	ИСПДн-И, ИСПДн-Б	6.1.2, 6.1.6, 6.1.7, 6.3.5, 6.3.10
	ИСПДн-С	6.1.2, 6.1.6, 6.1.7, 6.3.5, 6.3.10, 6.5.7
М8.6	ИСПДн-Д	6.2.1
	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.2.1, 6.3.6
М8.7	ИСПДн-И, ИСПДн-С	6.3.6
	ИСПДн-Б	6.3.6, 6.4.1
М8.8	ИСПДн-С	6.5.9
М8.9	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.7
М8.10	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.7
М8.12	ИСПДн-Д, ИСПДн-И, ИСПДн-Б	6.1.7
	ИСПДн-С	6.1.7, 6.5.9
М8.13	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.9, 6.3.10
М10.2	Все классы	5.2
М10.3	Все классы	5.2

СТО БР ИББС-1.2	Класс ИСПДн	РС БР ИББС-2.3
М11.9	ИСПДн-Д, ИСПДн-И, ИСПДн-С	6.1.8, 6.2.3, 6.3.3
	ИСПДн-Б	6.1.8, 6.2.3, 6.3.3, 6.4.1
	ИСПДн-С	6.1.8, 6.2.3, 6.3.3, 6.5.11
М12.2	ИСПДн-Д	5.2
	ИСПДн-И, ИСПДн-С	5.2, 6.3.6
	ИСПДн-Б	5.2, 6.3.6, 6.4.1
М12.3	ИСПДн-Д	5.2
	ИСПДн-И, ИСПДн-С	5.2, 6.3.6
	ИСПДн-Б	5.2, 6.3.6, 6.4.1
М12.4	Все классы	5.2
М15.6	ИСПДн-Д	6.1.2, 6.1.6, 6.1.7, 6.1.9, 6.2.1, 6.2.2
	ИСПДн-И, ИСПДн-Б	6.1.2, 6.1.6, 6.1.7, 6.1.9, 6.2.1, 6.2.2, 6.3.5, 6.3.8
	ИСПДн-С	6.1.2, 6.1.6, 6.1.7, 6.1.9, 6.2.1, 6.2.2, 6.3.5, 6.3.8, 6.5.7
М15.7	ИСПДн-Д	6.1.2, 6.1.6, 6.1.7, 6.2.1
	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.1.2, 6.1.6, 6.1.7, 6.2.1, 6.3.8
М15.8	ИСПДн-Д	6.1.6, 6.1.7, 6.1.9, 6.2.2
	ИСПДн-И, ИСПДн-Б	6.1.6, 6.1.7, 6.1.9, 6.2.2, 6.3.5, 6.3.8
	ИСПДн-С	6.1.6, 6.1.7, 6.1.9, 6.2.2, 6.3.5, 6.3.8, 6.5.7
М16.1	Все классы	6.1.5
М17.2	ИСПДн-И, ИСПДн-С	6.3.6
	ИСПДн-Б	6.3.6, 6.4.1
М20.2	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.10
М20.3	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.9
М20.5	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.3.9
М21.1	ИСПДн-Д	6.1.7, 6.1.9
	ИСПДн-И, ИСПДн-Б, ИСПДн-С	6.1.7, 6.1.9, 6.3.3
М21.7	Все классы	6.1.7, 6.1.9
М21.8	Все классы	6.1.7
М28.9	ИСПДн-Д, ИСПДн-И, ИСПДн-С	6.1.8, 6.2.3, 6.3.3
	ИСПДн-Б	6.1.8, 6.2.3, 6.3.3, 6.4.1
	ИСПДн-С	6.1.8, 6.2.3, 6.3.3, 6.5.11
М29.1	Все классы	6.1.5
М32.1	Все классы	6.1.7, 6.1.9
М32.2	Все классы	6.1.7

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