СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-2014

Дата введения: 2014-06-01

Издание официальное

Москва
2014

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 17 мая 2014 года № Р-399.

2. ВЗАМЕН СТО БР ИББС-1.2-2010.

Содержание

Введение

Стандартом Банка России СТО БР ИББС-1.0-2014 “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 регулярного аудита ИБ и самооценки ИБ.

Настоящий стандарт устанавливает способы определения степени выполнения требований стандарта Банка России СТО БР ИББС-1.0-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения”, а также итогового уровня соответствия ИБ требованиям стандарта Банка России СТО БР ИББС-1.0-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” при проведении аудита ИБ 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-1.0-2014

Дата введения: 2014-06-01

1. Область применения

Настоящий стандарт распространяется на организации БС РФ, а также на организации, проводящие оценку соответствия ИБ организации БС РФ требованиям стандарта Банка России СТО БР ИББС-1.0-2014 “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 соответствия ИБ.

Положения настоящего стандарта применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена 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 ИБ организации БС РФ требованиям СТО БР ИББС-1.0.

3.3. **Проверяемая организация**: Организация БС РФ, обеспечение ИБ 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;
ЭП — электронная подпись;
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;
$EV^1_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту 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, 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;
M_{ij} — 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 соответствия обеспечения ИБ организации БС РФ 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;
— определения итогового уровня соответствия ИБ организации требованиям СТО БР ИББС-1.0.

6. Показатели информационной безопасности. Способы оценивания показателей

6.1. Для оценки степени соответствия обеспечения 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.

6.2. Частные показатели разделены на два типа. К первому типу относятся частные показатели, отражающие требования СТО БР ИББС-1.0, выполнение которых обязательно в организации. Ко второму типу относятся частные показатели, отражающие положения СТО БР ИББС-1.0, выполнение которых рекомендуется в организации. Информация о принадлежности частных показателей к указанным типам определена в формах приложения А.

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

6.4. Оценка EV_{Mij} частного показателя формируется на основании выявленной проверяющей 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 (первый тип), 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 зафиксировано документами организации, то данный частный показатель определяется как неоцениваемый (должна быть заполнена графа “н/о” — нет оценки) и не учитывается в формировании дальнейших результатов оценки.

6.6. Для частных показателей, выполнение которых рекомендуется (второй тип), 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.

6.7. При проведении оценки частных показателей, для которых оценивается как степень их установления (определения) в организации БС РФ, так и степень выполнения (частный показатель категории проверки 1), используется 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 (определены) во внутренних документах проверяемой организации
0,25	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации, но не выполняются
0,5	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации, но выполняются в неполном объеме

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0,75	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации и выполняются почти в полном объеме
1	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации и выполняются в полном объеме

6.8. При проведении оценки частных показателей, для которых оценивается только степень документированности (частный показатель категории проверки 2), используется 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 документах проверяемой организации
1	Требования частного показателя ИБ полностью установлены во внутренних документах проверяемой организации

6.9. При проведении оценки частных показателей, для которых оценивается только степень выполнения (частный показатель категории проверки 3), используется 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 оценки соответствия ИБ (например, ограниченная выборка АБС), 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, в качестве основных источников которых рекомендуется использовать:

- внутренние 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 проверяющей группы за деятельностью сотрудников проверяемой организации.

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

Полученные свидетельства оценки соответствия ИБ и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств оценки соответствия ИБ, пример которых приведен в приложении Б. При заполнении листов для сбора свидетельств оценки соответствия ИБ необходимо указать ссылки на соответствующие внутренние документы проверяемой организации, результаты опроса сотрудников проверяемой организации, а также результаты наблюдений членов проверяющей группы. Результаты опроса и на-

блюдений должны быть подтверждены подписью опрашиваемого сотрудника организации и члена проверяющей группы соответственно.

6.12. Оценка группового показателя (EV_{Mi}) вычисляется из оценок входящих в него частных показателей (EV_{Mij}):

$$EV_{Mi} = \frac{\sum_{j} EV_{Mij}}{j}.$$

6.13. 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 $EV_{БИТП}$, $EV_{БПТП}$, $EV_{ООПД}$, $EV^{1}_{ОЗПД}$, $EV^{2}_{ОЗПД}$, EV_{1}, EV_{2} и EV_{3} (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;
- обеспечения 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

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
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) 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. Оценивание частных показателей в рамках групповых показателей M1—M7 для направления банковского платежного технологического процесса следует осуществлять с учетом актуальных результатов последней по времени проведения оценки выполнения организацией требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств” (далее — Положение Банка России от 9 июня 2012 года № 382-П) и используемых для вычисления обобщающего показателя $EV1_{ПС}$, установленного Положением Банка России от 9 июня 2012 года № 382-П.

Таблица соответствия частных показателей и требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в приложении 2 к Положению Банка России от 9 июня 2012 года № 382-П и учитываемых при оценивании частных показателей, приведена в приложении В.

Для проведения оценивания частных показателей с учетом результатов оценки выполнения организацией требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П, следует использовать подход, установленный в п. 6.7, 6.8 и 6.9 настоящей методики, с учетом того, что оценка частного показателя не может превышать минимальную оценку выполнения требований, установленных Положением Банка России от 9 июня 2012 года № 382-П, соответствующих оцениваемому частному показателю.

7.7. Итоговая оценка EV_1, отражающая степень выполнения требований СТО БР ИББС-1.0 по направлению “текущий уровень ИБ организации”, вычисляется по формуле:

$$EV_1 = \min(EV_{БИТП}, EV_{БПТП}, EV^2_{ОЗПД}, EV_{ООПД}), \text{ где:}$$

$EV_{БИТП}$ — 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.

7.8. Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс, вычисляется по формуле, в которой оценки

групповых показателей М1÷М6 выбираются по результатам их оценивания, применительно к банковскому платежному технологическому процессу и с учетом результатов оценки выполнения организацией требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П:

$$EV_{БПТП} = k^1_{БПТП} \frac{\sum_i EV_{Mi} + EV_{M7}}{7}, \; i = 1 \div 6,$$

где $k^1_{БПТП}$ — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

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:

$$EV_{БИТП} = k^1_{БИТП} \frac{\sum_i EV_{Mi} + EV_{M8}}{7}, \; i = 1 \div 6,$$

где $k^1_{БИТП}$ — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, 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:

$$EV^1_{ОЗПД} = k^1_{ОЗПД_1} \frac{\sum_i EV_{Mi} + EV_{M8} + EV_{M10}}{7}, \; i = 1 \div 5,$$

где $k^1_{ОЗПД_1}$ — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, 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:

$$EV^2_{ОЗПД} = k^1_{ОЗПД_2} \frac{\sum_i EV_{Mi} + EV_{M8} + EV_{M10}}{8}, \; i = 1 \div 6,$$

где $k^1_{ОЗПД_2}$ — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

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

$$EV_{ООПД} = k^1_{ООПД} \cdot EV_{M9},$$

где $k_{ООПД}$ — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

7.9. 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.

7.10. 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 БС РФ;
- 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 БС РФ 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 ИБ;
- организация обеспечения непрерывности бизнеса и его восстановления после прерываний;
- мониторинг ИБ и контроль защитных мер;
- проведение самооценки ИБ;
- проведение внешнего аудита ИБ;
- анализ функционирования СОИБ;
- анализ СОИБ со стороны руководства организации БС РФ;
- 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 БС РФ	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 БС РФ 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 ИБ	п. 8.10
M20	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний	п. 8.11
M21	Мониторинг ИБ и контроль защитных мер	п. 8.12

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
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 БС РФ	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) 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. Оценивание частных показателей в рамках групповых показателей M11÷M27 следует осуществлять с учетом результатов оценки выполнения организацией требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П и используемых для вычисления обобщающего показателя $EV2_{ПС}$, установленного Положением Банка России от 9 июня 2012 года № 382-П.

Таблица соответствия частных показателей и требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в приложении 2 к Положению Банка России от 9 июня 2012 года № 382-П и учитываемых при оценивании частных показателей, приведена в приложении В.

Для проведения оценивания частных показателей с учетом результатов оценки выполнения организацией требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П, следует использовать подход, установленный в п. 6.7, 6.8 и 6.9 настоящего стандарта, с учетом того, что оценка частного показателя не может превышать минимальную оценку выполнения требований, установленных Положением Банка России от 9 июня 2012 года № 382-П, соответствующих оцениваемому частному показателю.

8.6. Итоговая оценка EV_2, отражающая степени выполнения требований СТО БР ИББС-1.0 по направлению “менеджмент ИБ организации”, вычисляется по формуле:

$$EV_2 = k_2 \frac{\sum_{i=11}^{27} EV_{Mi}}{17},$$

где k_2 — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

8.7. 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.

8.8. 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 БС РФ по поддержке функционирования службы ИБ организации;

— деятельность руководства организации БС РФ по принятию решений о реализации и эксплуатации СОИБ;
— деятельность руководства организации БС РФ по поддержке планирования СОИБ;
— деятельность руководства организации БС РФ по поддержке реализации СОИБ;
— деятельность руководства организации БС РФ по поддержке проверки СОИБ;
— деятельность руководства организации БС РФ по анализу СОИБ;
— деятельность руководства организации БС РФ 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	п. 8.3, 8.4, 8.5, 8.6, 8.8
M31	Оценка деятельности руководства организации по поддержке реализации СОИБ	п. 8.9, 8.10, 8.11
M32	Оценка деятельности руководства организации по поддержке проверки СОИБ	п. 8.12, 8.13, 8.14, 8.15
M33	Оценка деятельность руководства организации по анализу СОИБ	п. 8.16
M34	Оценка деятельности руководства организации по поддержке совершенствования СОИБ	п. 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) приведены в приложении А.

Частные показатели по направлению оценки "уровень осознания ИБ организации" оцениваются с учетом результатов оценки выполнения организацией БС РФ требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П и используемых для вычисления обобщающего показателя $EV2_{ПС}$, установленного Положением Банка России от 9 июня 2012 года № 382-П, в соответствии с подходом, установленным п. 8.5 настоящего стандарта.

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 EV_3, отражающая степень выполнения требований СТО БР ИББС-1.0 по направлению "уровень осознания ИБ организации", вычисляется по формуле:

$$EV_3 = k_3 \frac{\sum_{i=28}^{34} EV_{Mi}}{7},$$

где k_3 — корректирующий коэффициент, определяемый по правилам, установленным в разделе 10.

9.6. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M28÷M34, 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. Правила определения корректирующих коэффициентов

Корректирующие коэффициенты $k^1_{БПТП}$, $k^1_{БИТП}$, $k^1_{ОЗПД_1}$, $k^1_{ОЗПД_2}$, $k^1_{ООПД}$, k_2 и k_3 определяются в зависимости от количества частных показателей, участвующих в вычислении оценок $EV_{БИТП}$, $EV_{БПТП}$, $EV_{ООПД}$, $EV^1_{ОЗПД}$, $EV^2_{ОЗПД}$, EV_1 и EV_2 соответственно, оценки которых равны 0 (полностью не выполняются) согласно правилам, установленным в таблице 7.

Таблица 7. Правила определения корректирующих коэффициентов

Корректирующий коэффициент	Количество частных показателей, оценки которых равны нулю (полностью не выполняются)		
$k^1_{БПТП}$	0	1–20	более 20
$k^1_{БИТП}$	0	1–20	более 20
$k^1_{ОЗПД_1}$	0	1–20	более 20
$k^1_{ОЗПД_2}$	0	1–20	более 20
$k^1_{ООПД}$	0	1–8	более 8
k_2	0	1–25	более 25
k_3	0	1–10	более 10
Значение корректирующего коэффициента	1	0,85	0,7

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 заключения по результатам оценки соответствия ИБ.

11.4. Значения R, соответствующие четвертому и пятому уровню, 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.

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

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

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

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

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

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

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

Первому уровню соответствует 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-1.0-2014".

"Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2014" 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-1.0-2014" как минимум следует включать следующие оценки:

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

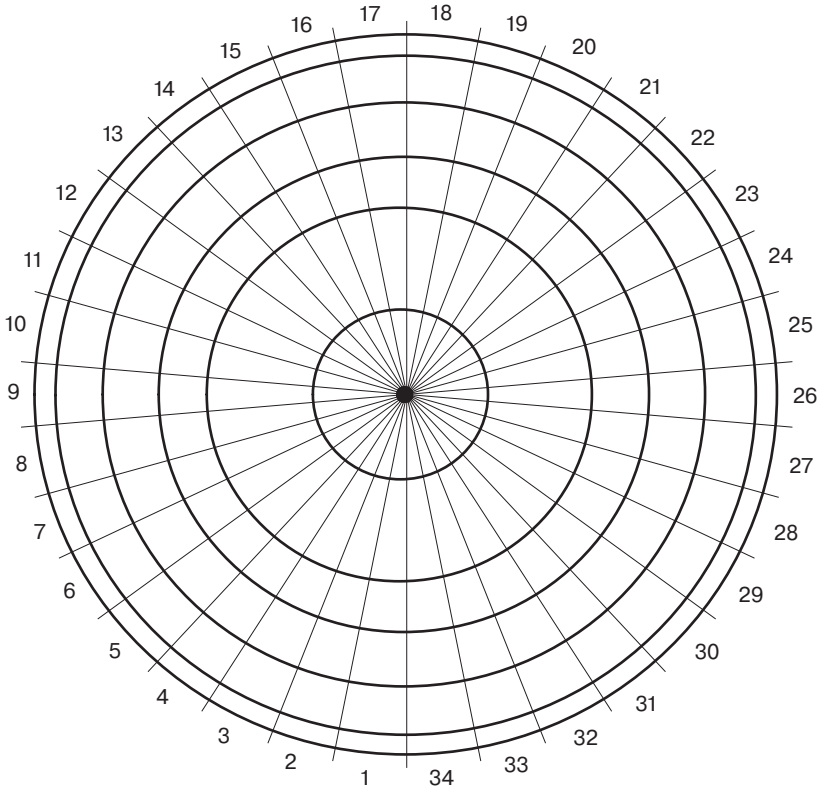
$EV^{I}_{озпд}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;

$EV_{м6}$ — 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 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-1.0-2014" 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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М1.1	Выделены ли в организации БС РФ роли ее работников?	обязательный	категория 1						
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?	рекомендуемый	категория 1						
М1.3	Осуществляется ли формирование и назначение ролей работников организации БС РФ с учетом соблюдения принципа предоставления минимальных прав и полномочий, необходимых для выполнения служебных обязанностей?	обязательный	категория 1						
М1.4	Персонифицированы ли роли в организации БС РФ с установлением ответственности за их выполнение?	обязательный	категория 2						
М1.5	Зафиксирована ли в должностных инструкциях или в организационно-распорядительных документах организации БС РФ ответственность за выполнение ролей?	обязательный	категория 2						
М1.6	Отсутствуют ли в организации БС РФ роли, совмещающие функции разработки и сопровождения АБС/ПО?	обязательный	категория 1						
М1.7	Отсутствуют ли в организации БС РФ роли, совмещающие функции разработки и эксплуатации АБС/ПО?	обязательный	категория 1						
М1.8	Отсутствуют ли в организации БС РФ роли, совмещающие функции сопровождения и эксплуатации АБС/ПО?	обязательный	категория 1						
М1.9	Отсутствуют ли в организации БС РФ роли, совмещающие функции администратора и администратора информационной безопасности?	обязательный	категория 1						
М1.10	Отсутствуют ли в организации БС РФ роли, совмещающие функции по выполнению операций в АБС и контроля их выполнения?	обязательный	категория 1						
М1.11	Определены ли в организации БС РФ, выполняются ли и регистрируются ли процедуры контроля деятельности работников, обладающих совокупностью полномочий, определяемых их ролями, позволяющими получить контроль над защищаемым информационным активом организации БС РФ?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М1.12	Определены ли, выполняются ли и регистрируются ли в организации БС РФ 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	категория 1						
М1.13	Предусматривают ли указанные в частном показателе М1.12 процедуры фиксацию результатов проводимых проверок?	обязательный	категория 2						
М1.14	Определены ли, выполняются ли и регистрируются, выполняются и регистрируются ли в организации БС РФ процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников?	рекомендуемый	категория 1						
М1.15	Предусматривают ли указанные в частном показателе М1.14 процедуры фиксацию результатов проводимых проверок?	рекомендуемый	категория 2						
М1.16	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры внеплановой проверки работников при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии?	рекомендуемый	категория 1						
М1.17	Предусматривают ли указанные в частном показателе М1.16 процедуры фиксацию результатов проводимых проверок?	рекомендуемый	категория 2						
М1.18	Обязаны ли все работники организации БС РФ давать письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов?	обязательный	категория 3						
М1.19	Регламентируются ли положениями, включенными в договоры (соглашения) с внешними организациями и клиентами, требования по ИБ?	обязательный	категория 2						
М1.20	Определены ли в трудовых контрактах (соглашениях, договорах) и (или) должностных инструкциях обязанности персонала по выполнению требований ИБ?	обязательный	категория 2						
М1.21	Приравнивается ли невыполнение работниками организации БС РФ требований ИБ к невыполнению должностных обязанностей и приводит ли как минимум к дисциплинарной ответственности?	обязательный	категория 1						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М2.1	Рассматриваются ли в части вопросов обеспечения ИБ следующие стадии модели ЖЦ АБС: — разработка технических заданий; — проектирование; — создание и тестирование; —приемка и ввод в действие; — эксплуатация; — сопровождение и модернизации; — снятие с эксплуатации?	обязательный	категория 1						
М2.2	Осуществляется ли выполнение работ на всех стадиях жизненного цикла АБС в части вопросов обеспечения ИБ по согласованию и под контролем службы ИБ?	обязательный	категория 1						
М2.3	Имеют ли организации, привлекаемые на договорной основе для обеспечения ИБ на стадиях ЖЦ АБС, лицензии на деятельность по технической защите конфиденциальной информации в соответствии с законодательством РФ?	обязательный	категория 3						
М2.4	Включаются ли требования к обеспечению информационной безопасности, установленные и используемые организацией БС РФ для обеспечения ИБ в рамках технологических процессов организации БС РФ, в технические задания на разработку или модернизацию АБС?	обязательный	категория 3						
М2.5	Обеспечивается ли в организации БС РФ реализация запрета использования защищаемой информации в качестве тестовых данных, анонимность данных и контроль адекватности предоставления и разграничения доступа на стадии создания и тестирования АБС и (или) их компонентов?	обязательный	категория 1						
М2.6	Снабжены ли эксплуатируемые АБС и (или) их компоненты документацией, содержащей описание реализованных в АБС защитных мер, в том числе описание состава и требований к реализации организационных защитных мер, состава и требований к эксплуатации технических защитных мер?	обязательный	категория 2						
М2.7	Проводится ли организацией БС РФ анализ принятия разработчиком АБС защитных мер, направленных на обеспечение безопасности разработки АБС и безопасности ее поставки?	рекомендуемый	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М2.8	Реализуется ли при взаимодействии организации БС РФ 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 БС РФ приобретает полный комплект документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика; 3) руководство организации БС РФ оценивает и фиксирует допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов?	обязательный	категория 3						
М2.9	Учитывается ли при разработке технических заданий на системы дистанционного банковского обслуживания, что защита данных должна обеспечиваться в условиях: — попыток несанкционированного доступа к информации анонимных, неавторизованных злоумышленников с использованием сетей общего пользования; — возможности ошибок авторизованных пользователей систем; — возможности ненамеренного или неадекватного использования защищаемой информации авторизованными пользователями?	обязательный	категория 3						
М2.10	Определены ли в организации БС РФ, выполняются ли и регистрируются ли на стадии эксплуатации АБС процедуры: — контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер; — контроля отсутствия уязвимостей в оборудовании и программном обеспечении АБС; — контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер; — контроля необходимого обновления программного обеспечения АБС, включая программное обеспечение технических защитных мер?	обязательный	категория 1						
М2.11	Определены ли, выполняются ли, регистрируются ли и контролируется ли на стадии эксплуатации АБС процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ?	обязательный	категория 1						
М2.12	Определены ли, выполняются ли и регистрируются ли на стадии эксплуатации АБС процедуры контроля состава устанавливаемого и (или) используемого ПО АБС?	обязательный	категория 1						
М2.13	Выделены ли и назначены ли роли, связанные с эксплуатацией и контролем эксплуатации АБС и применяемых технических защитных мер, в том числе с внесением изменений в параметры их настройки?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М2.14	Определены ли, выполняются ли для всех АБС процедуры контроля ее эксплуатации со стороны службы ИБ, регистрируется ли процесс и результаты их выполнения?	обязательный	категория 1						
М2.15	Определены ли, выполняются ли и контролируются ли на стадии эксплуатации АБС процедуры, необходимые для обеспечения сохранности носителей защищаемой информации?	обязательный	категория 1						
М2.16	Определены ли, выполняются ли и регистрируются ли в организации БС РФ 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	категория 1						
М2.17	Определены ли, выполняются ли и регистрируются ли на стадии сопровождения (модернизации) АБС, отнесенных решением организацией БС РФ к критичным, в том числе АБС, задействованных в реализации банковского платежного технологического процесса, и в ИСПДн, процедуры фиксации внесенных изменений?	обязательный	категория 1						
М2.18	Определены ли, выполняются ли и регистрируются ли на стадии сопровождения (модернизации) АБС, отнесенных решением организацией БС РФ к критичным, в том числе АБС, задействованных в реализации банковского платежного технологического процесса, и в ИСПДн, процедуры проверки функциональности АБС, в том числе применяемых мер защиты информации, после внесения изменений?	обязательный	категория 1						
М2.19	Определены ли, выполняются ли, регулируются ли и выполняются ли на стадии снятия с эксплуатации процедуры, обеспечивающие удаление информации с использованием алгоритмов и (или) методов, обеспечивающих невозможность восстановления удаленной информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой техническими защитными мерами, 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 законодательством РФ, нормативными актами Банка России и (или) договорными документами)?	обязательный	категория 1						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры выявления, учета и классификации (отнесение к одному из типов) информационных активов?	обязательный	категория 1						
М3.2	Учтены ли и зафиксированы ли права доступа работников и клиентов организации БС РФ к информационным активам и (или) их типам?	обязательный	категория 1						
М3.3	Применяются ли в составе АБС встроенные защитные меры от НСД и НРД?	обязательный	категория 1						
М3.4	Применяются ли в составе АБС сертифицированные по требованиям безопасности информации средства защиты информации?	рекомендуемый	категория 3						
М3.5	Обеспечивается ли защитными мерами от НСД сокрытие вводимых субъектами доступа аутентификационных данных на устройствах отображения информации?	обязательный	категория 3						
М3.6	Препятствует ли размещение устройств отображения информации АБС ее несанкционированному просмотру?	обязательный	категория 3						
М3.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС РФ, и программных процессов (сервисов)?	обязательный	категория 1						
М3.8	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры разграничения доступа к информационным активам на основе ролевого метода с определением для каждой роли полномочий по доступу к информационным активам?	обязательный	категория 1						
М3.9	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления предоставлением/отзывом и блокированием доступа, в том числе доступа, осуществляемого через внешние информационно-телекоммуникационные сети?	обязательный	категория 1						
М3.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации?	обязательный	категория 1						
М3.11	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления идентификационными данными, аутентификационными данными и средствами аутентификации?	обязательный	категория 1						
М3.12	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления учетными записями субъектов доступа?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.13	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры выявления и блокирования неуспешных попыток доступа?	обязательный	категория 1						
М3.14	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации для продолжения работы?	обязательный	категория 1						
М3.15	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры ограничения действий пользователей по изменению настроек их автоматизированных мест (использование ограничений на изменение BIOS)?	обязательный	категория 1						
М3.16	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления составом разрешенных действий до выполнения идентификации и аутентификации?	обязательный	категория 1						
М3.17	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры ограничения действий пользователей по изменению параметров настроек АБС и реализации контроля действий эксплуатационного персонала по изменению параметров настроек АБС?	обязательный	категория 1						
М3.18	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин?	обязательный	категория 1						
М3.19	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры использования технологий беспроводного доступа к информации в случае их применения и защиты внутренних беспроводных соединений?	обязательный	категория 1						
М3.20	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры использования мобильных устройств для доступа к информации в случае их применения?	обязательный	категория 1						
М3.21	Исключают ли процедуры управления доступом возможность “самосанкционирования”?	обязательный	категория 1						
М3.22	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ правила и процедуры мониторинга ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции?	обязательный	категория 1						
М3.23	Определены ли действия и операции, подлежащие регистрации?	обязательный	категория 2						
М3.24	Определены ли состав и содержание данных о действиях и операциях, подлежащих регистрации, сроки их хранения?	обязательный	категория 2						
М3.25	Обеспечено ли резервирование необходимого объема памяти для записи данных?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.26	Обеспечено ли реагирование на сбои при регистрации действий и операций, в том числе на аппаратные и программные ошибки, сбои в технических средствах сбора данных?	обязательный	категория 1						
М3.27	Обеспечена ли генерация временных меток для регистрируемых действий и операций и синхронизация системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных?	обязательный	категория 3						
М3.28	Реализовано ли в организации БС РФ ведение журналов действия и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов и АБС с целью их использования при реагировании на инциденты ИБ?	обязательный	категория 1						
М3.29	Обеспечено ли хранение данных о действиях и операциях не менее трех лет (если иные сроки хранения не установлены законодательством РФ, нормативными актами Банка России)?	рекомендуемый	категория 3						
М3.30	Обеспечено ли хранение данных, полученных в результате выполнения банковского платежного технологического процесса, не менее пяти лет (если иные сроки хранения не установлены законодательством РФ, нормативными актами Банка России)?	рекомендуемый	категория 3						
М3.31	Используются ли для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях специализированные программные и (или) технические средства?	обязательный	категория 3						
М3.32	Зафиксированы ли критерии выявления неправомерных или подозрительных действий и операций, используемые при проведении процедур мониторинга ИБ и анализа данных о действиях и операциях?	обязательный	категория 2						
М3.33	Применяются ли процедуры мониторинга ИБ и анализа данных о действиях и операциях, использующие зафиксированные критерии выявления неправомерных или подозрительных действий и операций, на регулярной основе, например ежедневно, ко всем выполненным операциям (транзакциям)?	обязательный	категория 3						
М3.34	Определено ли и контролируется ли в организации БС РФ выполнение требований: — к разделению сегментов вычислительных сетей, в том числе создаваемых с использованием технологии виртуализации; — к межсетевому экранированию; — к информационному взаимодействию между сегментами вычислительных сетей?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.35	Осуществляется ли разделение сегментов вычислительных сетей с целью обеспечения независимого выполнения банковских платежных технологических процессов организации БС РФ, а также банковских информационных технологических процессов организации БС РФ разной степени критичности, в том числе банковских информационных технологических процессов, в рамках которых осуществляется обработка персональных данных в ИСПДн?	обязательный	категория 1						
М3.36	Регламентированы ли и контролируются ли процедуры внесения изменений в конфигурацию сетевого оборудования, предусматривающие согласование вносимых изменений со службой ИБ?	обязательный	категория 2						
М3.37	Предоставлен ли работникам службы ИБ доступ к конфигурации сетевого оборудования без возможности внесения изменений?	рекомендуемый	категория 3						
М3.38	Определен ли, выполняется ли, регистрируется ли и контролируется ли порядок доступа к объектам среды информационных активов, в том числе в помещения, в которых размещаются объекты среды информационных активов?	обязательный	категория 1						
М3.39	Обеспечивают ли используемые в организации БС РФ 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	категория 3						
М3.40	Определен ли, выполняется ли и контролируется ли в организации БС РФ порядок использования съемных носителей информации?	обязательный	категория 1						
М3.41	Реализованы ли в системах дистанционного банковского обслуживания, используемых в организации БС РФ, защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций?	обязательный	категория 3						
М3.42	Придано ли протоколам операций, выполняемых посредством дистанционного банковского обслуживания, свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание?	обязательный	категория 1						
М3.43	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	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.44	Определены ли в организации БС РФ процедуры, определяющие действия работников и клиентов организации БС РФ 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	категория 2						
М3.45	Доведены ли до сведения работников и клиентов организации БС РФ процедуры, указанные в частном показателе М3.44?	обязательный	категория 3						
М3.46	Предусматривают ли указанные в частном показателе М3.44 процедуры регистрацию работниками и клиентами всех своих действий и их результатов?	обязательный	категория 3						
М3.47	Реализованы ли в системах дистанционного банковского обслуживания механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имени?	обязательный	категория 3						
М3.48	Применяются ли в организации БС РФ меры, направленные на обеспечение защиты от НСД, повреждения или нарушения целостности данных о действиях и операциях, а также меры по защите информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и работников организации БС РФ?	обязательный	категория 1						
М3.49	Регистрируются ли все попытки НСД к информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и сотрудников организации БС РФ?	обязательный	категория 1						
М3.50	Предоставляется ли доступ к данным о действиях и операциях только с целью выполнения служебных обязанностей?	обязательный	категория 1						
М3.51	Выполняются ли регламентированные процедуры соответствующего пересмотра прав доступа при увольнении или изменении должностных обязанностей работников организации БС РФ, имевших доступ к данным о действиях и операциях?	обязательный	категория 1						
М3.52	Используются ли сетевые протоколы, обеспечивающие защиту сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации при осуществлении доступа на участке телекоммуникационных каналов и линий связи, в том числе беспроводных, не контролируемых организацией БС РФ?	обязательный	категория 3						
М3.53	Осуществляется ли передача защищаемых данных по каналам связи, имеющим выход за пределы контролируемой организацией БС РФ зоны, только при условии обеспечения их защиты от раскрытия и модификации?	обязательный	категория 3						
М3.54	Осуществляется ли работа всех работников организации БС РФ АБС под уникальными и персонифицированными учетными записями?	обязательный	категория 3						
Итоговая оценка группового показателя М3									

Групповой показатель М4 “Обеспечение информационной безопасности средствами антивирусной защиты”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного 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 БС РФ, если иное не предусмотрено технологическим процессом, средства антивирусной защиты?	обязательный	категория 1						
М4.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС?	обязательный	категория 1						
М4.3	Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных?	рекомендуемый	категория 1						
М4.4	Проводится ли антивирусная проверка съемных носителей информации перед их подключением к средствам вычислительной техники, задействованным в рамках осуществления банковских технологических процессов, на специально выделенном автономном средстве вычислительной техники?	рекомендуемый	категория 1						
М4.5	Разработаны ли и введены ли в действие инструкции и рекомендации по антивирусной защите, учитывающие особенности банковских технологических процессов?	обязательный	категория 2						
М4.6	Организована ли в организации БС РФ антивирусная фильтрация всего трафика электронного почтового обмена?	обязательный	категория 3						
М4.7	Организована ли в организации БС РФ эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей на: — рабочих станциях; — серверном оборудовании, в том числе серверах электронной почты; — технических средствах межсетевого экранирования?	обязательный	категория 1						
М4.8	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов?	обязательный	категория 1						
М4.9	Выполняется ли после установки или изменения программного обеспечения антивирусная проверка?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М4.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать: — 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	категория 1						
М4.11	Определены ли, выполняются ли и регистрируются ли процедуры контроля за отключением и обновлением антивирусных средств на всех технических средствах АБС?	обязательный	категория 1						
М4.12	Возложена ли обязанность по выполнению предписанных мер антивирусной защиты на каждого работника организации БС РФ, имеющего доступ к ЭВМ и (или) АБС, а ответственность за выполнение требований по антивирусной защите — на руководителей функциональных подразделений организации БС РФ?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М5.1	Принято ли документально руководством организации БС РФ решение об использовании сети Интернет для производственной и (или) собственной хозяйственной деятельности, в котором явно перечислены и зафиксированы цели использования сети Интернет?	обязательный	категория 2						
М5.2	Запрещается ли использование ресурсов сети Интернет в неустановленных целях?	обязательный	категория 2						
М5.3	Проведено ли в организации БС РФ выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей?	обязательный	категория 3						
М5.4	Проводится ли наделение работников организации БС РФ правами пользователя конкретного пакета, содержащего перечень сервисов и ресурсов сети Интернет, в соответствии с его должностными обязанностями, в частности в соответствии с назначенными ему ролями?	обязательный	категория 3						
М5.5	Регистрируется ли наделение работников организации БС РФ правами пользователя конкретного пакета, содержащего перечень сервисов и ресурсов сети Интернет, в соответствии с его должностными обязанностями, в частности в соответствии с назначенными ему ролями?	обязательный	категория 3						
М5.6	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры подключения и использования ресурсов сети Интернет?	обязательный	категория 1						
М5.7	Осуществляется ли передача защищаемых данных с использованием сети Интернет только при условии обеспечения их защиты от раскрытия и модификации?	обязательный	категория 1						
М5.8	Применяются ли в организации БС РФ в связи с повышенными рисками нарушения ИБ при взаимодействии с сетью Интернет защитные меры, в том числе межсетевые экраны, антивирусные средства, средства обнаружения вторжений, средства криптографической защиты информации, обеспечивающие, среди прочего, прием и передачу информации только в установленном формате и только по конкретной технологии?	обязательный	категория 1						
М5.9	Разработаны ли и введены ли в действие инструкции и рекомендации по использованию сети Интернет, учитывающие особенности банковских технологических процессов?	обязательный	категория 1						
М5.10	Определены ли и выполняются ли процедуры протоколирования посещения ресурсов сети Интернет работниками организации БС РФ?	обязательный	категория 1						
М5.11	Доступны ли данные о посещенных сотрудниками организации БС РФ ресурсов сети Интернет работникам службы ИБ?	обязательный	категория 3						
М5.12	Выполнено ли выделение и организована ли физическая изоляция от внутренних сетей тех ЭВМ, с помощью которых осуществляется непосредственное взаимодействие с сетью Интернет?	рекомендуемый	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М5.13	Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный	категория 3						
М5.14	Регистрируются ли регламентированным образом попытки подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный	категория 1						
М5.15	Все ли операции клиентов в течение сеанса работы с системами дистанционного банковского обслуживания, в том числе операции по переводу денежных средств, выполняются только после выполнения процедур идентификации, аутентификации и авторизации?	обязательный	категория 3						
М5.16	Обеспечивается ли закрытие текущей сессии и повторное выполнение процедур идентификации, аутентификации и авторизации в случаях нарушения или разрыва соединения при работе с системами дистанционного банковского обслуживания?	обязательный	категория 3						
М5.17	Используется ли специализированное клиентское программное обеспечение для доступа пользователей к системам дистанционного банковского обслуживания?	рекомендуемый	категория 3						
М5.18	Определены ли состав и порядок применения мер защиты, применяемых для организации почтового обмена через сеть Интернет?	обязательный	категория 2						
М5.19	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 БС РФ) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски)?	рекомендуемый	категория 3						
М5.20	Осуществляется ли архивирование электронной почты с целью: — контроля информационных потоков, в том числе с целью предотвращение утечек информации; — использования архивов при проведении разбирательств по фактам утечек информации?	обязательный	категория 3						
М5.21	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ правила и процедуры доступа к информации архива и ее изменения, предусматривающие возможность доступа работников службы ИБ к информации архива?	обязательный	категория 1						
М5.22	Не применяется ли в организации БС РФ практика хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которой осуществляется непосредственное взаимодействие с сетью Интернет?	рекомендуемый	категория 3						
М5.23	Всегда ли наличие банковской информации на ЭВМ, с помощью которых осуществляется непосредственное взаимодействие с сетью Интернет, определяется бизнес-целями организации БС РФ и санкционируется ее руководством?	обязательный	категория 3						
М5.24	Определены ли состав и порядок применения мер защиты, применяемых при взаимодействии с сетью Интернет и позволяющие обеспечить противодействие атакам злоумышленников и распространению спама?	обязательный	категория 1						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М6.1	Проводится ли применение СКЗИ в организации БС РФ в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией БС РФ?	обязательный	категория 1						
М6.2	Имеют ли СКЗИ, применяемые для защиты персональных данных, класс не ниже КС2?	обязательный	категория 3						
М6.3	Проводятся ли работы по обеспечению безопасности информации с помощью СКЗИ в соответствии с действующими законодательством, нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России?	обязательный	категория 1						
М6.4	Утверждена ли частная политика, касающаяся применения СКЗИ в организации БС РФ?	рекомендуемый	категория 2						
М6.5	Допускают ли СКЗИ возможность встраивания в технологические процессы обработки электронных сообщений?	обязательный	категория 3						
М6.6	Обеспечивают ли СКЗИ взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов?	обязательный	категория 3						
М6.7	Обладают ли СКЗИ полным комплектом эксплуатационной документации, предоставляемым разработчиком, включающей описание ключевой системы, правил работы с ней и обоснование необходимого организационно-штатного обеспечения?	обязательный	категория 3						
М6.8	Сертифицированы ли СКЗИ уполномоченным государственным органом или имеют ли СКЗИ разрешение ФСБ России?	обязательный	категория 3						
М6.9	Осуществляется ли установка и ввод в эксплуатацию, а также эксплуатация СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам?	обязательный	категория 3						
М6.10	Поддерживается ли непрерывность процессов протоколирования работы СКЗИ в соответствии с технической документацией на СКЗИ при применении СКЗИ?	обязательный	категория 3						
М6.11	Поддерживается ли непрерывность процессов обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М6.12	Обеспечивается ли ИБ процессов изготовления криптографических ключей СКЗИ комплексом технологических, организационных, технических и программных мер и средств защиты, предусмотренных технической документацией на СКЗИ?	обязательный	категория 3						
М6.13	Реализованы ли процедуры мониторинга ИБ, регистрирующие все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и всех инцидентов ИБ?	рекомендуемый	категория 1						
М6.14	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	категория 1						
М6.15	Самостоятельно ли изготавливаются в организации БС РФ и (или) клиентом организации ключи СКЗИ?	рекомендуемый	категория 3						
М6.16	Регулируются ли заключаемыми договорами отношения, возникающие между организациями и их клиентами?	обязательный	категория 2						
Итоговая оценка группового показателя М6									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М7.1	Регламентирован (описан) ли в организации БС РФ банковский платежный технологический процесс?	обязательный	категория 2						
М7.2	Зафиксирован ли порядок обмена платежной информацией в договорах между участниками данного обмена?	обязательный	категория 2						
М7.3	Отсутствуют ли в организации БС РФ работники, обладающие полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведение несанкционированных операций по изменению состояния банковских счетов?	обязательный	категория 1						
М7.4	Контролируются (проверяются) ли и удостоверяются ли результаты технологических операций по обработке платежной информации лицами/автоматизированными процессами?	обязательный	категория 3						
М7.5	Осуществляется ли обработка платежной информации и контроль (проверка) результатов обработки разными работниками/автоматизированными процессами?	рекомендуемый	категория 3						
М7.6	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений?	обязательный	категория 1						
М7.7	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса доступ работника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации?	обязательный	категория 1						
М7.8	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации?	обязательный	категория 1						
М7.9	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса аутентификацию входящих электронных платежных сообщений?	обязательный	категория 1						
М7.10	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М7.11	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса возможность ввода платежной информации в АБС только для авторизованных пользователей?	обязательный	категория 1						
М7.12	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса контроль, направленный на исключение возможности совершения злоумышленных действий, в частности двойной ввод, сверка, установление ограничений в зависимости от суммы совершения операций?	обязательный	категория 1						
М7.13	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники?	обязательный	категория 1						
М7.14	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса при осуществлении межбанковских расчетов сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями?	обязательный	категория 1						
М7.15	Предусматривает ли комплекс защитных мер возможность блокирования приема к исполнению распоряжений клиентов?	обязательный	категория 1						
М7.16	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса доставку электронных платежных сообщений участникам обмена?	обязательный	категория 1						
М7.17	Организован ли в организации БС РФ авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип “двойного управления”)?	рекомендуемый	категория 3						
М7.18	Применяются ли для систем дистанционного банковского обслуживания процедуры, реализующие: — снижение вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами; — доведение информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов?	обязательный	категория 3						
М7.19	Обеспечены ли клиенты систем дистанционного банковского обслуживания детальными инструкциями, описывающими процедуры выполнения операций или транзакций?	обязательный	категория 3						
М7.20	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену их программных и (или) аппаратных частей?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М7.21	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации?	обязательный	категория 1						
М7.22	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры контроля отсутствия размещения на устройствах, задействованных в осуществлении банковского платежного технологического процесса, находящихся в общедоступных местах вне зоны постоянного контроля, в том числе банкоматах и платежных терминалах, специализированных средств, используемых для несанкционированного съема информации?	обязательный	категория 1						
М7.23	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации?	обязательный	категория 1						
Итоговая оценка группового показателя М7									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М8.1	Проведена ли в организации БС РФ классификация неплатежной информации?	обязательный	категория 2						
М8.2	Проводится ли классификация неплатежной информации в соответствии со степенью тяжести последствий потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности?	обязательный	категория 3						
М8.3	Определен ли документально набор требований по защите каждого из типов неплатежной информации, полученных в результате классификации?	обязательный	категория 2						
М8.4	Регламентированы (описаны) ли в организации БС РФ банковские информационные технологические процессы?	обязательный	категория 1						
М8.5	Реализованы ли банковские информационные технологические процессы в рамках созданных для этих целей АБС?	обязательный	категория 3						
М8.6	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 ИБ?	рекомендуемый	категория 3						
М8.7	Определены ли, выполняются ли и контролируются ли требования к взаимодействию АБС организаций БС РФ с информационными системами сторонних организаций (внешними информационными системами)?	обязательный	категория 1						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М9.1	Установлены ли руководством организации БС РФ цели обработки персональных данных (далее — ПДн)?	обязательный	категория 2						
М9.2	Установлена ли в организации БС РФ необходимость осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн?	обязательный	категория 2						
М9.3	Организована ли деятельность по своевременному направлению указанного уведомления в соответствии с требованиями Федерального закона “О персональных данных” в случае наличия такой необходимости?	обязательный	категория 3						
М9.4	Установлены ли в организации БС РФ критерии отнесения АБС к ИСПДн?	обязательный	категория 2						
М9.5	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета ресурсов ПДн, в том числе учета ИСПДн?	обязательный	категория 1						
М9.6	Обеспечено ли для каждого ресурса ПДн установление цели обработки ПДн?	обязательный	категория 2						
М9.7	Обеспечено ли для каждого ресурса ПДн установление и соблюдение сроков хранения персональных данных и условий прекращения их обработки?	обязательный	категория 1						
М9.8	Обеспечено ли для каждого ресурса ПДн определение перечня и категорий обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн)?	обязательный	категория 2						
М9.9	Обеспечено ли для каждого ресурса ПДн выполнение процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками организации БС РФ?	обязательный	категория 1						
М9.10	Обеспечено ли для каждого ресурса ПДн выполнение ограничения обработки ПДн достижением цели обработки ПДн?	обязательный	категория 3						
М9.11	Обеспечено ли для каждого ресурса ПДн соответствие содержания и объема обрабатываемых ПДн установленным целям обработки?	обязательный	категория 3						
М9.12	Обеспечены ли для каждого ресурса ПДн точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн?	обязательный	категория 3						
М9.13	Обеспечено ли для каждого ресурса ПДн выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”?	обязательный	категория 3						
М9.14	Обеспечено ли для каждого ресурса ПДн выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”?	обязательный	категория 3						
М9.15	Обеспечено ли для каждого ресурса ПДн прекращение обработки ПДн и уничтожение либо обезличивание ПДн по достижению целей обработки по требованию субъекта ПДн в случаях, предусмотренных Федеральным законом “О персональных данных”, в том числе при отзыве субъектом ПДн согласия на обработку его ПДн?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М9.16	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в случае достижения цели обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией БС РФ и субъектом ПДн)?	обязательный	категория 1						
М9.17	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в случае отзыва субъектом ПДн согласия на обработку его ПДн, и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией БС РФ и субъектом ПДн)?	обязательный	категория 1						
М9.18	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в случае если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки?	обязательный	категория 1						
М9.19	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в случае выявления неправомерной обработки ПДн, осуществляемой организацией БС РФ или обработчиком, действующим по ее поручению, если обеспечить правомерность обработки ПДн невозможно?	обязательный	категория 1						
М9.20	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в случае выявления неправомерной обработки ПДн без согласия субъекта ПДн?	обязательный	категория 1						
М9.21	Обеспечивает ли организация БС РФ в случае отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного Федеральным законом “О персональных данных”, их блокирование с последующим обеспечением уничтожения ПДн, которое производится не позднее шести месяцев со дня их блокирования?	обязательный	категория 1						
М9.22	Определена ли, выполняется ли и контролируется ли в организации БС РФ политика в отношении обработки ПДн, а также в случае необходимости установлены ли порядки обработки ПДн для отдельных ресурсов ПДн?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М9.23	Является ли для ресурсов ПДн, обрабатываемых в АБС организации БС РФ, в том числе ИСПДн, порядок обработки ПДн частью эксплуатационной документации на АБС и разрабатывается ли на этапе создания или модернизации АБС?	рекомендуемый	категория 2						
М9.24	Определяет ли политика в отношении обработки ПДн процедуры предоставления доступа к ПДн?	обязательный	категория 2						
М9.25	Определяет ли политика в отношении обработки ПДн процедуры внесения изменений в ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн?	обязательный	категория 2						
М9.26	Определяет ли политика в отношении обработки ПДн процедуры уничтожения, обезличивания либо блокирования ПДн в случае необходимости выполнения таких процедур?	обязательный	категория 2						
М9.27	Определяет ли политика в отношении обработки ПДн процедуры обработки обращений субъектов ПДн (их законных представителей) для случаев, предусмотренных Федеральным законом “О персональных данных”, в частности порядок подготовки информации о наличии ПДн, относящихся к конкретному субъекту ПДн, информации, необходимой для предоставления возможности ознакомления субъектом ПДн (их законных представителей) с его ПДн, а также процедуры обработки обращений об уточнении ПДн, их блокировании или уничтожении, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для установленной цели обработки?	обязательный	категория 2						
М9.28	Определяет ли политика в отношении обработки ПДн процедуры обработки запроса уполномоченного органа по защите прав субъектов ПДн?	обязательный	категория 2						
М9.29	Определяет ли политика в отношении обработки ПДн процедуры получения согласия субъекта ПДн на обработку его ПДн и на передачу обработки его ПДн третьим лицам?	обязательный	категория 2						
М9.30	Определяет ли политика в отношении обработки ПДн процедуры передачи ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками организации БС РФ, имеющими доступ к ПДн?	обязательный	категория 2						
М9.31	Определяет ли политика в отношении обработки ПДн процедуры передачи ПДн третьим лицам?	обязательный	категория 2						
М9.32	Определяет ли политика в отношении обработки ПДн процедуры работы с материальными носителями ПДн?	обязательный	категория 2						
М9.33	Определяет ли политика в отношении обработки ПДн процедуры, необходимые для осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в сроки, установленные Федеральным законом “О персональных данных”?	обязательный	категория 2						
М9.34	Определяет ли политика в отношении обработки ПДн необходимость применения типовых форм документов для осуществления обработки ПДн и процедуры работы с ними (под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая организацией БС РФ с целью сбора ПДн)?	обязательный	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М9.35	Обеспечен ли организацией БС РФ неограниченный доступ к документу, определяющему ее политику в отношении обработки ПДн, а также к сведениям о реализуемых требованиях по обеспечению безопасности персональных данных?	обязательный	категория 3						
М9.36	Установлено ли в организации БС РФ, в каких случаях необходимо получение согласия субъектов ПДн?	обязательный	категория 2						
М9.37	Регламентированы ли форма и порядок получения согласия субъектов?	обязательный	категория 2						
М9.38	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета лиц, имеющих доступ к ПДн?	обязательный	категория 1						
М9.39	Утвержден ли руководителем организации БС РФ документ, определяющий перечень лиц, имеющих доступ к ПДн?	обязательный	категория 2						
М9.40	Осуществляется ли обработка ПДн работниками организации БС РФ только с целью выполнения их должностных обязанностей?	обязательный	категория 3						
М9.41	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры ознакомления работников организации БС РФ, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами организации БС РФ, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей?	обязательный	категория 1						
М9.42	Проводит ли организация БС РФ ознакомления работников организации БС РФ, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами организации БС РФ, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей, в ходе проведения мероприятий по их обучению или повышению осведомленности?	обязательный	категория 3						
М9.43	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета помещений, в которых осуществляется обработка ПДн, а также доступа работников организации БС РФ и иных лиц в помещения, в которых ведется обработка ПДн?	обязательный	категория 1						
М9.44	Обеспечено ли при работе с материальными носителями ПДн обособление ПДн от иной информации, в частности, путем фиксации их на отдельных съемных носителях ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях)?	обязательный	категория 3						
М9.45	Обеспечен ли при работе со съемными носителями ПДн их учет?	обязательный	категория 1						
М9.46	Обеспечено ли при работе со съемными носителями ПДн установление, выполнение и контроль выполнения порядка хранения съемных, в том числе машинных, носителей ПДн и доступа к ним?	обязательный	категория 1						
М9.47	Обеспечено ли при работе со съемными носителями ПДн хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных съемных носителях?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М9.48	Обеспечено ли при работе со съемными носителями ПДн регистрация и учет мест хранения материальных носителей ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн), включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями?	обязательный	категория 3						
М9.49	Обеспечено ли при работе со съемными носителями ПДн назначение работников, ответственных за организацию их хранения?	обязательный	категория 3						
М9.50	Обеспечено ли при работе со съемными носителями ПДн установление и выполнение порядка уничтожения (стирания) информации на съемных носителях ПДн?	обязательный	категория 3						
М9.51	Осуществляется ли хранение ПДн в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн?	обязательный	категория 3						
М9.52	Создаются ли и публикуются ли организацией БС РФ общедоступные источники ПДн только для цели выполнения требований законодательства РФ?	обязательный	категория 3						
М9.53	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры публикации ПДн в общедоступных источниках ПДн?	обязательный	категория 1						
М9.54	Осуществляется ли на основании договора поручение обработки ПДн третьему лицу (далее – обработчик)?	обязательный	категория 2						
М9.55	Определен ли в указанном договоре перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки?	обязательный	категория 2						
М9.56	Установлена ли в указанном договоре обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн?	обязательный	категория 2						
М9.57	Получено ли организацией БС РФ согласие субъекта ПДн, если иное не предусмотрено федеральным законом, при поручении обработки персональных данных обработчику?	обязательный	категория 3						
М9.58	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры, выполняемые в случаях необходимости осуществления трансграничной передачи ПДн?	обязательный	категория 1						
М9.59	Назначено ли в организации БС РФ лицо, ответственное за организацию обработки ПДн?	обязательный	категория 3						
М9.60	Установлены ли руководством организации БС РФ полномочия лица, ответственного за организацию обработки ПДн, а также его права и обязанности?	обязательный	категория 2						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М10.1	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение и регистрация процедур контроля целостности и обеспечения доверенной загрузки программного обеспечения, в том числе программного обеспечения технических защитных мер, на средствах вычислительной техники, входящих в ИСПДн?	обязательный	категория 1						
М10.2	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение, регистрация и контроль процедур доступа к эксплуатационной документации и архивным файлам, содержащим параметры настройки ИСПДн, в том числе настройки применяемых технических защитных мер?	обязательный	категория 1						
М10.3	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления ПДн?	обязательный	категория 1						
М10.4	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, в том числе программного обеспечения технических защитных мер, входящего в состав ИСПДн?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М10.5	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, в части обеспечения ИБ при управлении доступом и регистрации идентификация и аутентификация устройств, используемых для осуществления доступа?	обязательный	категория 3						
М10.6	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, в части обеспечения ИБ при управлении доступом и регистрации размещение технических средств, предназначенных для администрирования ИСПДн, автоматизированных мест пользователей и серверных компонент ИСПДн в отдельных, выделенных сегментах вычислительных сетей?	обязательный	категория 3						
М10.7	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, в части обеспечения ИБ при управлении доступом и регистрации мониторинг сетевого трафика, выявление вторжений и сетевых атак и реагирования на них?	обязательный	категория 1						
М10.8	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, в части обеспечения ИБ при управлении доступом и регистрации, определение, выполнение, регистрация и контроль процедур обновления сигнатурных баз технических защитных мер, мониторинга сетевого трафика, выявления вторжений и сетевых атак?	обязательный	категория 1						
М10.9	Реализуются ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, в части обеспечения ИБ банковских информационных технологических процессов определение, выполнение, регистрация и контроль процедур использования коммуникационных портов, устройств ввода-вывода информации, съемных машинных носителей и внешних накопителей информации?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М10.10	Реализуются ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, в части обеспечения ИБ банковских информационных технологических процессов определение, выполнение, регистрация и контроль процедур доступа к архивам ПДн?	обязательный	категория 1						
М10.11	Реализованы ли в организации БС РФ защита периметров сегментов вычислительной сети, в которых расположена ИСПДн, и контроль информационного взаимодействия между сегментами вычислительных сетей?	обязательный	категория 3						
М10.12	Определены ли и контролируются ли в организации БС РФ правила информационного взаимодействия между ИСПДн с иными АБС?	обязательный	категория 1						
М10.13	Осуществляется ли использование в организации БС РФ в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных”?	обязательный	категория 3						
М10.14	Назначен ли для каждой ИСПДн работник организации БС РФ, ответственный за обеспечение безопасности персональных данных в ИСПДн?	обязательный	категория 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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М11.1	Сформирована ли руководством служба ИБ в составе не менее двух человек (назначены ли уполномоченные лица) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный	категория 3						
М11.2	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный	категория 3						
М11.3	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный	категория 3						
М11.4	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый	категория 3						
М11.5	Сформированы ли для организаций БС РФ, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	обязательный	категория 1						
М11.6	Наделена ли служба ИБ полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М11.7	Наделена ли служба ИБ полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации БС РФ?	обязательный	категория 3						
М11.8	Наделена ли служба ИБ полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М11.9	Наделена ли служба ИБ полномочиями определять требования к мерам обеспечения ИБ организации БС РФ?	обязательный	категория 3						
М11.10	Наделена ли служба ИБ полномочиями контролировать работников организации БС РФ 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	категория 3						
М11.11	Наделена ли служба ИБ полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный	категория 3						
М11.12	Наделена ли служба ИБ 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 БС РФ)?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М11.13	Наделена ли служба ИБ полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?	обязательный	категория 3						
М11.14	Наделена ли служба ИБ полномочиями осуществлять контроль обеспечения ИБ на стадиях ЖЦ АБС, в том числе при тестировании и вводе в эксплуатацию подсистем ИБ АБС организации БС РФ?	обязательный	категория 3						
М11.15	Наделена ли служба ИБ полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации БС РФ?	обязательный	категория 3						
Итоговая оценка группового показателя М11									

Групповой показатель М12 “Определение/коррекция области действия СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М12.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета структурированных по классам (типам) защищаемых информационных активов?	обязательный	категория 1						
М12.2	Проводится ли классификация информационных активов на основании оценок ценности информационных активов для интересов (целей) организации БС РФ, например в соответствии с тяжестью последствий потери свойств ИБ информационных активов?	рекомендуемый	категория 3						
М12.3	Установлены ли в организации БС РФ критерии отнесения конкретных информационных активов к одному или нескольким типам информационных активов?	обязательный	категория 2						
М12.4	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 1						
М12.5	Определены ли в организации БС РФ роли по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
М12.6	Назначены ли в организации БС РФ ответственные за выполнение ролей по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М13.1	Принята ли в организации БС РФ и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный	категория 1						
М13.2	Определены ли в организации БС РФ критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный	категория 2						
М13.3	Определяет ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ организации БС РФ 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 БС РФ (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	категория 2						
М13.4	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный	категория 2						
М13.5	Проводится ли оценка рисков нарушения ИБ для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ?	обязательный	категория 3						
М13.6	Соотносятся ли величины рисков, полученные в результате оценивания рисков нарушения ИБ, с уровнем допустимого риска, принятого в организации БС РФ?	обязательный	категория 3						
М13.7	Зафиксирован ли в организации БС РФ 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 БС РФ?	обязательный	категория 2						
М13.8	Определены ли в организации БС РФ роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М13.9	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М13.10	Определены ли в организации БС РФ роли по оценке рисков нарушения ИБ?	обязательный	категория 3						
М13.11	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный	категория 3						
Итоговая оценка группового показателя М13									

Групповой показатель М14 “Разработка планов обработки рисков нарушения ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М14.1	Определен ли в организации БС РФ по каждому из недопустимых рисков нарушения ИБ план, устанавливающий 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	категория 2						
М14.2	Согласованы ли планы обработки рисков нарушения ИБ с руководителем службы ИБ либо лицом, отвечающим в организации БС РФ за обеспечение ИБ?	обязательный	категория 2						
М14.3	Утверждены ли руководством организации БС РФ планы обработки рисков нарушения ИБ?	обязательный	категория 2						
М14.4	Содержат ли планы реализации требований ИБ последовательность и сроки реализации и внедрения организационных, технических и иных мер защиты?	обязательный	категория 3						
М14.5	Определены ли в организации БС РФ роли по разработке планов обработки рисков нарушения ИБ?	обязательный	категория 3						
М14.6	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М15.1	Проводится ли разработка и коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ в организации БС РФ, 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	категория 3						
М15.2	Разработана ли политика ИБ организации БС РФ?	обязательный	категория 2						
М15.3	Утверждена ли политика ИБ организации БС РФ руководством?	обязательный	категория 2						
М15.4	Корректируется ли политика ИБ организации БС РФ?	обязательный	категория 3						
М15.5	Разработаны ли частные политики ИБ организации БС РФ?	обязательный	категория 2						
М15.6	Корректируются ли частные политики ИБ организации БС РФ?	обязательный	категория 3						
М15.7	Разработаны ли в организации БС РФ документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ?	обязательный	категория 2						
М15.8	Корректируются ли в организации БС РФ документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ?	обязательный	категория 3						
М15.9	Определен ли в организации БС РФ перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ?	обязательный	категория 2						
М15.10	Определены ли в политике ИБ (частных политиках ИБ) организации БС РФ: — 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	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М15.11	Корректируются ли в политике ИБ (частных политиках ИБ) организации БС РФ: — 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	категория 3						
М15.12	Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства РФ; — комплекса БР ИББС, в частности требования разделов 7 и 8 стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации БС РФ со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов или типов информационных активов?	обязательный	категория 3						
М15.13	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства РФ; — комплекса БР ИББС, в частности требования разделов 7 и 8 стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации БС РФ со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов или типов информационных активов?	обязательный	категория 3						
М15.14	Содержит ли совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, требования по обеспечению ИБ всех выявленных информационных активов или типов информационных активов, находящихся в области действия СОИБ организации БС РФ?	обязательный	категория 3						
М15.15	Не противоречат ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положениям политики ИБ и частных политик ИБ?	обязательный	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М15.16	Детализируют ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положения политики ИБ и частных политик ИБ?	обязательный	категория 3						
М15.17	Утвержден ли руководством организации БС РФ порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации БС РФ (в случае наличия в структурных подразделениях организации БС РФ работников, ответственных за обеспечение ИБ)?	обязательный	категория 2						
М15.18	Определены ли в составе документов, регламентирующих деятельность в области обеспечения ИБ, перечень свидетельств выполнения указанной деятельности и ответственность работников организации БС РФ за выполнение этой деятельности?	обязательный	категория 2						
М15.19	Определены ли в организации БС РФ процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный	категория 2						
М15.20	Определен ли в организации БС РФ порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 2						
М15.21	Определены ли в организации БС РФ роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М15.22	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М16.1	Зафиксированы ли 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 разделах 7 и 8 СТО БР ИББС-1.0; — о распределении ролей в области обеспечения ИБ организации БС РФ; — о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований разделов 7 и 8 СТО БР ИББС-1.0 и снижение рисков ИБ; — о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ?	обязательный	категория 2						
М16.2	Утверждены ли руководством все планы внедрения СОИБ, в частности планы реализаций требований разделов 7 и 8 СТО БР ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых определены: — последовательность выполнения мероприятий в рамках указанных планов; — сроки начала и окончания запланированных мероприятий; — должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия?	обязательный	категория 2						
М16.3	Определен ли в организации БС РФ порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации БС РФ?	обязательный	категория 2						
М16.4	Зафиксированы ли решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 2						
Итоговая оценка группового показателя М16									

Групповой показатель М17 “Организация реализации планов внедрения СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М17.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры проектирования/приобретения/развертывания, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер (СИБ), предусмотренных планами реализации требований ИБ?	обязательный	категория 1						
М17.2	Реализуются ли при построении элементов СИБ (применительно к конкретной области или сфере деятельности организации БС РФ) защитные меры, применяемые к объектам среды в соответствии с существующими в организации БС РФ требованиями обеспечения ИБ, сформулированными в политике ИБ и других внутренних документах организации БС РФ?	обязательный	категория 1						
М17.3	Определены ли в организации БС РФ роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный	категория 3						
М17.4	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М18.1	Организована ли санкционированная руководством организации БС РФ работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ?	обязательный	категория 3						
М18.2	Разработаны ли планы, программы обучения и повышения осведомленности в области ИБ, по результатам выполнения которых должна осуществляться проверка полученных знаний?	обязательный	категория 1						
М18.3	Установлены ли в планах обучения и повышения осведомленности требования к периодичности обучения и повышения осведомленности?	обязательный	категория 2						
М18.4	Разрабатываются ли программы обучения и повышения осведомленности для различных групп сотрудников с учетом их должностных обязанностей и выполняемых ролей? Включена ли в них информация: — по существующим политикам ИБ; — по применяемым в организации защитным мерам; — по правильному использованию защитных мер в соответствии с внутренними документами организации БС РФ; — о значимости и важности деятельности работников для обеспечения ИБ организации БС РФ?	обязательный	категория 2						
М18.5	Определен ли в организации БС РФ перечень свидетельств выполнения программ обучения и повышения осведомленности в области ИБ? В частности, такими свидетельствами могут являться: — документы (журналы), подтверждающие прохождение руководителями и работниками организации БС РФ обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых; — документы, содержащие результаты проверок обучения работников организации БС РФ; — документы, содержащие результаты проверок осведомленности в области ИБ в организации БС РФ	обязательный	категория 2						
М18.6	Организуется ли для работника, получившего новую роль, обучение или инструктаж в области ИБ в соответствии с полученной ролью?	обязательный	категория 3						
М18.7	Определены ли в организации БС РФ роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
М18.8	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
Итоговая оценка группового показателя М18									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М19.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры обработки инцидентов, включающие: — процедуры обнаружения инцидентов ИБ; — процедуры информирования об инцидентах, в том числе информирования службы ИБ; — 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	категория 1						
М19.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры хранения и распространения информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ?	обязательный	категория 1						
М19.3	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры действий работников организации БС РФ при обнаружении нетипичных событий, связанных с ИБ, и порядок информирования о данных событиях?	обязательный	категория 1						
М19.4	Осведомлены ли работники организации БС РФ о порядке действий при обнаружении нетипичных событий, связанных с ИБ, и порядке информирования о данных событиях?	обязательный	категория 3						
М19.5	Учитывают ли процедуры расследования инцидентов действующее законодательство РФ, положения нормативных актов Банка России, а также внутренних документов организации БС РФ в области ИБ?	обязательный	категория 3						
М19.6	Принимаются ли, фиксируются ли и выполняются ли в организации БС РФ решения по всем выявленным инцидентам ИБ?	обязательный	категория 1						
М19.7	Определены ли в организации БС РФ роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
М19.8	Назначены ли в организации БС РФ ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М20.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета информационных активов или типов информационных активов, существенных для обеспечения непрерывности бизнеса организации БС РФ?	обязательный	категория 1						
М20.2	Установлены ли в организации БС РФ требования обеспечения ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания, в том числе требования к мероприятиям по восстановлению необходимой информации, программного обеспечения, технических средств, а также каналов связи?	обязательный	категория 2						
М20.3	Определен ли в организации БС РФ план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации БС РФ, в состав которого включены: — условия активации 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 БС РФ; — обязанности работников организации БС РФ с указанием ответственных за выполнение каждого из положений плана?	обязательный	категория 2						
М20.4	Основывается ли разработка планов обеспечения непрерывности бизнеса и его восстановления после прерываний на результатах оценки рисков нарушения ИБ организации БС РФ применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М20.5	Применяются ли защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М20.6	Основывается ли применение защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания на соответствующих требованиях по обеспечению ИБ?	обязательный	категория 3						
М20.7	Согласован ли план обеспечения непрерывности бизнеса и его восстановления после прерываний с существующими в организации БС РФ процедурами обработки инцидентов ИБ?	обязательный	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М20.8	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры периодического тестирования плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 1						
М20.9	Составлен ли сценарий тестирования плана обеспечения непрерывности бизнеса и его восстановления после прерывания с учетом существующей в организации БС РФ модели угроз и нарушителей, а также результатов оценки рисков?	обязательный	категория 3						
М20.10	Проводится ли при необходимости корректировка плана обеспечения непрерывности бизнеса и его восстановления после прерывания по результатам тестирования?	обязательный	категория 3						
М20.11	Реализована ли в организации БС РФ программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний?	обязательный	категория 3						
М20.12	Определены ли в организации БС РФ роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М20.13	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке плана, обеспечение непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
Итоговая оценка группового показателя М20									

Групповой показатель М21 “Мониторинг ИБ и контроль защитных мер”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М21.1	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры мониторинга ИБ 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 организовываются службой ИБ?	обязательный	категория 1						
М21.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры сбора и хранения информации о действиях работников организации БС РФ, событиях и параметрах, имеющих отношение к функционированию защитных мер?	обязательный	категория 1						
М21.3	Учтена ли в рамках выполнения процедур хранения информации об инцидентах ИБ информация обо всех инцидентах ИБ, выявленных в процессе мониторинга ИБ и контроля защитных мер?	обязательный	категория 3						
М21.4	Подвергаются ли процедуры мониторинга ИБ и контроля защитных мер регулярным и регистрируемым 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	категория 3						
М21.5	Определены ли в организации БС РФ роли, связанные с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
М21.6	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
Итоговая оценка группового показателя М21									

Групповой показатель М22 “Проведение самооценки ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М22.1	Проводится ли самооценка ИБ собственными силами и по инициативе руководства организации БС РФ?	обязательный	категория 3						
М22.2	Проводится ли самооценка ИБ в соответствии с настоящим стандартом?	обязательный	категория 3						
М22.3	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	категория 3						
М22.4	Установлена ли в организации БС РФ 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	категория 1						
М22.5	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры: — формирования, сбора и хранения свидетельств самооценки ИБ; — соблюдения периодичности проведения самооценки ИБ; — хранения и распространения результатов самооценки ИБ?	обязательный	категория 1						
М22.6	Установлен ли в организации БС РФ для каждой проводимой в организации БС РФ 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 БС РФ, связанных с проведением самооценки ИБ?	обязательный	категория 2						
М22.7	Подготавливаются ли по результатам самооценок ИБ отчеты?	обязательный	категория 3						
М22.8	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М22.9	Определены ли в организации БС РФ роли, связанные с выполнением программы самооценок ИБ?	обязательный	категория 3						
М22.10	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный	категория 3						
М22.11	Проводится ли в организации БС РФ оценка соответствия ИБ в виде самооценки ИБ или аудита ИБ не реже одного раза в два года?	обязательный	категория 1						
Итоговая оценка группового показателя М22									

Групповой показатель М23 “Проведение аудита ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М23.1	Проводится ли аудит ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности” и СТО БР ИББС-1.0?	обязательный	категория 3						
М23.2	Установлена ли в организации БС РФ 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	категория 1						
М23.3	Установлен ли в организации БС РФ для каждого проводимого в организации БС РФ 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	категория 2						
М23.4	Оформлены ли договоры с аудиторскими организациями с установленными в них процедурами: — хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ; — взаимодействия с аудиторской организацией в процессе проведения аудита ИБ; — взаимодействия аудиторской группы и руководства, позволяющими представителям аудиторской группы при необходимости непосредственно обращаться к руководству; — организации опроса работников; — организации наблюдения за деятельностью работников организации БС РФ со стороны представителей аудиторской организации?	обязательный	категория 2						
М23.5	Подготавливаются ли по результатам аудитов ИБ отчеты?	обязательный	категория 2						
М23.6	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М23.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности отчетов аудитов?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М23.8	Определены ли в организации БС РФ роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный	категория 3						
М23.9	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный	категория 3						
М23.10	Проводится ли в организации БС РФ оценка соответствия ИБ в виде аудита ИБ или самооценки ИБ не реже одного раза в два года?	обязательный	категория 1						
Итоговая оценка группового показателя М23									

Групповой показатель М24 “Анализ функционирования СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М24.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры анализа функционирования СОИБ, использующие в том числе: — результаты мониторинга ИБ 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 БС РФ, например данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации БС РФ; — данные об изменениях вне организации БС РФ, например данные об изменениях в законодательстве РФ, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах организации БС РФ?	обязательный	категория 1						
М24.2	Проводится ли анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации БС РФ, требованиям законодательства РФ, требованиям стандартов Банка России, контрактным требованиям организации?	обязательный	категория 3						
М24.3	Проводится ли анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в организации БС РФ, требованиям политик ИБ организации БС РФ?	обязательный	категория 3						
М24.4	Проводится ли оценка рисков в области ИБ организации БС РФ, включая оценку уровня остаточного и допустимого рисков, а также оценка адекватности модели угроз организации БС РФ существующим угрозам ИБ?	обязательный	категория 3						
М24.5	Проводится ли оценка адекватности используемых мер защиты требованиям внутренних документов организации БС РФ и результатам оценки рисков?	обязательный	категория 3						
М24.6	Проводится ли анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании мер защиты?	обязательный	категория 3						
М24.7	Определены ли в организации БС РФ роли, связанные с процедурами анализа функционирования СОИБ?	обязательный	категория 3						
М24.8	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М25.1	Установлен ли в организации БС РФ перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный	категория 2						
М25.2	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: — мониторинга ИБ и контроля защитных мер; — анализа функционирования СОИБ; — аудитов ИБ; — самооценок ИБ?	обязательный	категория 3						
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 РФ и (или) в положениях стандартов Банка России; — о выявленных инцидентах ИБ?	обязательный	категория 3						
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	категория 3						
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	категория 3						
М25.6	Установлен ли в организации БС РФ план выполнения деятельности по контролю и анализу СОИБ?	обязательный	категория 2						
М25.7	Содержит ли план выполнения деятельности по контролю и анализу СОИБ положения по проведению совещаний на уровне руководства, на которых в том числе производится поиск и анализ проблем ИБ, влияющих на бизнес организации БС РФ?	обязательный	категория 3						
М25.8	Определены ли в организации БС РФ роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный	категория 3						
М25.9	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный	категория 3						
Итоговая оценка группового показателя М25									

Групповой показатель М26 “Принятие решений по тактическим улучшениям СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М26.1	Рассматриваются ли при принятии решений, связанных с тактическими улучшениями СОИБ, результаты: — аудитов ИБ; — самооценок ИБ; — мониторинга ИБ 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	категория 3						
М26.2	Зафиксированы ли решения по тактическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо направления тактических улучшений СОИБ?	обязательный	категория 2						
М26.3	Регистрируется ли деятельность по реализации тактических улучшений СОИБ?	обязательный	категория 2						
М26.4	Установлены ли в организации БС РФ планы реализации тактических улучшений СОИБ?	обязательный	категория 2						
М26.5	Существуют ли в организации БС РФ документы, в которых фиксируются результаты выполнения планов реализации тактических улучшений СОИБ?	обязательный	категория 3						
М26.6	Санкционирует и контролирует ли руководство службы ИБ организации БС РФ деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный	категория 3						
М26.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ 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?	обязательный	категория 1						
М26.8	Установлены ли роли и назначены ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный	категория 3						
Итоговая оценка группового показателя М26									

Групповой показатель М27 “Принятие решений по стратегическим улучшениям СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М27.1	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, результаты: — аудитов ИБ; — самооценок ИБ; — мониторинга ИБ и контроля защитных мер; — анализа функционирования СОИБ; — обработки инцидентов ИБ; — выявления новых информационных активов организации БС РФ 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	категория 3						
М27.2	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, изменения интересов, целей и задач бизнеса организации БС РФ, контрактных обязательств организации БС РФ, а также изменения в законодательстве РФ и нормативных актах Банка России?	обязательный	категория 2						
М27.3	Фиксируются ли в организации БС РФ решения по стратегическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо направления стратегических улучшений СОИБ?	обязательный	категория 2						
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 БС РФ; — изменения в области действия СОИБ; — пересмотр моделей угроз и нарушителей; — изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ?	обязательный	категория 1						
М27.5	Регистрируется ли деятельность по реализации стратегических улучшений СОИБ?	обязательный	категория 3						
М27.6	Установлены ли в организации БС РФ планы реализации стратегических улучшений СОИБ?	обязательный	категория 2						
М27.7	Существуют ли в организации БС РФ документы, в которых фиксируются результаты выполнения планов реализации стратегических улучшений СОИБ?	обязательный	категория 2						
М27.8	Согласуется ли со службой ИБ, санкционируется ли и контролируется ли руководством организации БС РФ деятельность, связанная с реализацией стратегических улучшений СОИБ?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М27.9	В случае стратегических улучшений СОИБ выполняется ли деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых мер защиты 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	категория 3						
М27.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ 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?	обязательный	категория 1						
М27.11	Установлены ли роли и назначены ли ответственные за реализацию решений по стратегическим улучшениям СОИБ в случае их принятия?	обязательный	категория 2						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М28.1 (аналог М11.1)	Сформирована ли руководством служба ИБ в составе не менее двух человек (назначены ли уполномоченные лица) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный	категория 3						
М28.2 (аналог М11.2)	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный	категория 3						
М28.3 (аналог М11.3)	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный	категория 3						
М28.4 (аналог М11.4)	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый	категория 3						
М28.5 (аналог М11.5)	Сформированы ли для организаций БС РФ, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	обязательный	категория 1						
М28.6 (аналог М11.6)	Наделена ли служба ИБ полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М28.7 (аналог М11.7)	Наделена ли служба ИБ полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации БС РФ?	обязательный	категория 3						
М28.8 (аналог М11.8)	Наделена ли служба ИБ полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М28.9 (аналог М11.9)	Наделена ли служба ИБ полномочиями определять требования к мерам обеспечения ИБ организации БС РФ?	обязательный	категория 3						
М28.10 (аналог М11.10)	Наделена ли служба ИБ полномочиями контролировать работников организации БС РФ 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	категория 3						
М28.11 (аналог М11.11)	Наделена ли служба ИБ полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М28.12 (аналог М11.12)	**Наделена ли служба ИБ 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 БС РФ)?**	**обязательный**	**категория 3**						
М28.13 (аналог М11.13)	**Наделена ли служба ИБ полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?**	**обязательный**	**категория 3**						
М28.14 (аналог М11.15)	**Наделена ли служба ИБ полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации БС РФ?**	**обязательный**	**категория 3**						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М29.1 (аналог М16.1)	Зафиксированы ли 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 разделах 7 и 8 СТО БР ИББС-1.0; — о распределении ролей в области обеспечения ИБ организации БС РФ; — о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований разделов 7 и 8 СТО БР ИББС-1.0 и снижение рисков ИБ; — о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ?	обязательный	категория 2						
М29.2 (аналог М16.2)	Утверждены ли руководством все планы внедрения СОИБ, в частности планы реализаций требований разделов 7 и 8 СТО БР ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых определены: — последовательность выполнения мероприятий в рамках указанных планов; — сроки начала и окончания запланированных мероприятий; — должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия?	обязательный	категория 2						
М29.3 (аналог М16.3)	Определен ли в организации БС РФ порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации БС РФ?	обязательный	категория 2						
М29.4 (аналог М16.4)	Зафиксированы ли решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 2						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М30.1 (аналог М12.1)	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета структурированных по классам (типам) защищаемых информационных активов?	обязательный	категория 1						
М30.2 (аналог М12.5)	Определены ли в организации БС РФ роли по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
М30.3 (аналог М12.6)	Назначены ли в организации БС РФ ответственные за выполнение ролей по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
М30.4 (аналог М13.1)	Принята ли в организации БС РФ и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный	категория 1						
М30.5 (аналог М13.2)	Определены ли в организации БС РФ критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный	категория 2						
М30.6 (аналог М13.4)	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный	категория 2						
М30.7 (аналог М13.8)	Определены ли в организации БС РФ роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М30.8 (аналог М13.9)	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М30.9 (аналог М13.10)	Определены ли в организации БС РФ роли по оценке рисков нарушения ИБ?	обязательный	категория 3						
М30.10 (аналог М13.11)	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный	категория 3						
М30.11 (аналог М14.3)	Утверждены ли руководством организации БС РФ планы обработки рисков нарушения ИБ?	обязательный	категория 2						
М30.12 (аналог М14.5)	Определены ли в организации БС РФ роли по разработке планов обработки рисков нарушения ИБ?	обязательный	категория 3						
М30.13 (аналог М14.6)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный	категория 3						
М30.14 (аналог М15.2)	Разработана ли политика ИБ организации БС РФ?	обязательный	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М30.15 (аналог М15.3)	Утверждена ли политика ИБ организации БС РФ руководством?	обязательный	категория 2						
М30.16 (аналог М15.4)	Корректируется ли политика ИБ организации БС РФ?	обязательный	категория 3						
М30.17 (аналог М15.5)	Разработаны ли частные политики ИБ организации БС РФ?	обязательный	категория 2						
М30.18 (аналог М15.6)	Корректируются ли частные политики ИБ организации БС РФ?	обязательный	категория 3						
М30.19 (аналог М15.10)	Определены ли в политике ИБ (частных политиках ИБ) организации БС РФ: — 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	категория 2						
М30.20 (аналог М15.11)	Корректируются ли в политике ИБ (частных политиках ИБ) организации БС РФ: — 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	категория 3						
М30.21 (аналог М15.12)	Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства РФ; — комплекса БР ИББС, в частности требования разделов 7 и 8 стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации БС РФ со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов или типов информационных активов?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М30.22 (аналог М15.13)	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства РФ; — комплекса БР ИББС, в частности требования разделов 7 и 8 стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации БС РФ со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов или типов информационных активов?	обязательный	категория 3						
М30.23 (аналог М15.17)	Утвержден ли руководством организации БС РФ порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации БС РФ (в случае наличия в структурных подразделениях организации БС РФ работников, ответственных за обеспечение ИБ)?	обязательный	категория 2						
М30.24 (аналог М15.19)	Определены ли в документах организации БС РФ процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный	категория 2						
М30.25 (аналог М15.21)	Определены ли в организации БС РФ роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М30.26 (аналог М15.22)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М30.27 (аналог М17.3)	Определены ли в организации БС РФ роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный	категория 3						
М30.28 (аналог М17.4)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М31.1 (аналог М18.1)	Организована ли санкционированная руководством организации БС РФ работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ?	обязательный	категория 3						
М31.2 (аналог М18.2)	Разработаны ли планы, программы обучения и повышения осведомленности в области ИБ, по результатам выполнения которых должна осуществляться проверка полученных знаний?	обязательный	категория 1						
М31.3 (аналог М18.7)	Определены ли в организации БС РФ роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
М31.4 (аналог М18.8)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
М31.5 (аналог М19.7)	Определены ли в организации БС РФ роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
М31.6 (аналог М19.8)	Назначены ли в организации БС РФ ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
М31.7 (аналог М20.3)	Определен ли в организации БС РФ план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации БС РФ, в состав которого включены: — условия активации плана; — порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персоналу); — процедуры восстановления; — процедуры тестирования и проверки плана; — план обучения и повышения осведомленности работников организации БС РФ; — обязанности работников организации БС РФ с указанием ответственных за выполнение каждого из положений плана?	обязательный	категория 2						
М31.8 (аналог М20.12)	Определены ли в организации БС РФ роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М31.9 (аналог М20.13)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке плана, обеспечение непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М32.1 (аналог М21.5)	Определены ли в организации БС РФ роли, связанные с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
М32.2 (аналог М21.6)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
М32.3 (аналог М22.4)	Установлена ли в организации БС РФ 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	категория 1						
М32.4 (аналог М22.8)	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М32.5 (аналог М22.9)	Определены ли в организации БС РФ роли, связанные с выполнением программы самооценок ИБ?	обязательный	категория 3						
М32.6 (аналог М22.10)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный	категория 3						
М32.7 (аналог М22.11, М23.10)	Проводится ли в организации БС РФ оценка соответствия ИБ в виде или самооценки ИБ аудита ИБ не реже одного раза в два года?	обязательный	категория 1						
М32.8 (аналог М23.2)	Установлена ли в организации БС РФ 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	категория 1						
М32.9 (аналог М23.6)	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М32.10 (аналог М23.8)	Определены ли в организации БС РФ роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный	категория 3						
М32.11 (аналог М23.9)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный	категория 3						
М32.12 (аналог М24.7)	Определены ли в организации БС РФ роли, связанные с процедурами анализа функционирования СОИБ?	обязательный	категория 3						
М32.13 (аналог М24.8)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный	категория 3						
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	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М33.1 (аналог М25.1)	Установлен ли в организации БС РФ перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный	категория 2						
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 ИБ и контроля защитных мер; — анализа функционирования СОИБ; — аудитов ИБ; — самооценок ИБ?	обязательный	категория 3						
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 РФ и (или) в положениях стандартов Банка России; — о выявленных инцидентах ИБ?	обязательный	категория 3						
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 выполнения планов обработки рисков?	обязательный	категория 3						
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	категория 3						
М33.6 (аналог М25.6)	Установлен ли в организации БС РФ план выполнения деятельности по контролю и анализу СОИБ?	обязательный	категория 2						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М33.7 (аналог М25.7)	Содержит ли план выполнения деятельности по контролю и анализу СОИБ положения по проведению совещаний на уровне руководства, на которых в том числе производится поиск и анализ проблем ИБ, влияющих на бизнес организации БС РФ?	обязательный	категория 3						
М33.8 (аналог М25.8)	Определены ли в организации БС РФ роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный	категория 3						
М33.9 (аналог М25.9)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный	категория 3						
Итоговая оценка группового показателя М33									

Групповой показатель М34 “Оценка деятельности руководства по поддержке совершенствования СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного 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 БС РФ деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный	категория 3						
М34.2 (аналог М26.8)	Установлены ли роли и назначены ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный	категория 3						
М34.3 (аналог М27.8)	Согласуется ли со службой ИБ, санкционируется ли и контролируется ли руководством организации БС РФ деятельность, связанная с реализацией стратегических улучшений СОИБ?	обязательный	категория 2						
М34.4 (аналог М27.11)	Установлены ли роли и назначены ли ответственные за реализацию решений по стратегическим улучшениям СОИБ в случае их принятия?	обязательный	категория 2						
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)

Таблица соответствия частных показателей и требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в приложении 2 к Положению Банка России от 9 июня 2012 года № 382-П и учитываемых при оценивании частных показателей

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М1.3	П. 32	2.6.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации
М1.4	П. 1	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по осуществлению доступа к защищаемой информации
	П. 2	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по управлению криптографическими ключами
	П. 3	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа
	П. 4	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений
М1.7	П. 5	2.4.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры
М1.8	П. 6	2.4.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени ролей, связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и эксплуатацией объекта информационной инфраструктуры в части его технического обслуживания и ремонта
М1.11	П. 1	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по осуществлению доступа к защищаемой информации
	П. 2	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по управлению криптографическими ключами
	П. 3	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию лиц, обладающих правами по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 4	2.4.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений
	П. 7	2.4.3	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль и регистрацию действий лиц, которым назначены роли, определенные в подпункте 2.4.1 пункта 2.4 Положения Банка России от 9 июня 2012 года № 382-П (далее — Положение)
М2.2	П. 9	2.5.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры
	П. 10	2.5.3	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий
М2.4	П. 8	2.5.1	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств
М2.5	П. 14	2.5.5	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры
М2.6	П. 11	2.5.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают наличие эксплуатационной документации на используемые технические средства защиты информации
М2.10	П. 12	2.5.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации
	П. 15	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают реализацию запрета несанкционированного копирования защищаемой информации
	П. 16	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают защиту резервных копий защищаемой информации
	П. 17	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, правилами платежной системы и (или) договорами, заключенными оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором платежной системы, оператором услуг платежной инфраструктуры

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 54	2.8.1	При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения
М2.11	П. 13	2.5.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе
	П. 71	2.10.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают учет и контроль состава установленного и (или) используемого на средствах вычислительной техники программного обеспечения
М2.15	П. 38	2.6.8	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение хищений носителей защищаемой информации
М2.16	П. 16	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают защиту резервных копий защищаемой информации
	П. 17	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, правилами платежной системы и (или) договорами, заключенными оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором платежной системы, оператором услуг платежной инфраструктуры
М2.18	П. 15	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают реализацию запрета несанкционированного копирования защищаемой информации
М2.19	П. 15	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают реализацию запрета несанкционированного копирования защищаемой информации
	П. 16	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают защиту резервных копий защищаемой информации
	П. 17	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, правилами платежной системы и (или) договорами, заключенными оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором платежной системы, оператором услуг платежной инфраструктуры

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М3.1	П. 18	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления
М3.3	П. 19	2.6.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов
	П. 20	2.6.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия
М3.7	П. 21	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации
	П. 22	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают идентификацию, аутентификацию, авторизацию участников платежной системы при осуществлении переводов денежных средств
	П. 26	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают выполнение процедур идентификации, аутентификации, авторизации лиц, осуществляющих доступ к программному обеспечению банкоматов и платежных терминалов
	П. 29.3	2.6.3	Оператор по переводу денежных средств определяет во внутренних документах: порядок формирования уникального идентификатора клиента в автоматизированной системе, программном обеспечении; перечень кодов действий клиентов, выполняемых при осуществлении переводов денежных средств с использованием автоматизированной системы, программного обеспечения; подлежащий регистрации идентификатор устройства; порядок регистрации и хранения информации, указанной в абзацах тринадцатом—шестнадцатом подпункта 2.6.3 пункта 2.6 Положения
М3.9	П. 25	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации
	П. 29	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения. Банковским платежным агентом (субагентом) обеспечивается регистрация действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, при наличии технической возможности с учетом выполняемого перечня операций и используемых автоматизированных систем, программного обеспечения, эксплуатация которых обеспечивается банковским платежным агентом (субагентом)

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М3.10	П. 29.4	2.6.3	Оператор по переводу денежных средств определяет требования к порядку, форме и срокам передачи ему информации о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, регистрируемой банковскими платежными агентами (субагентами)
М3.11	П. 23	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают определение порядка использования информации, необходимой для выполнения аутентификации
М3.21	П. 31	2.6.4	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реализацию запрета несанкционированного расширения прав доступа к защищаемой информации
М3.22	П. 24	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий при осуществлении доступа своих работников к защищаемой информации
	П. 28	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 настоящего Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении
	П. 29.1	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию следующей информации о действиях клиентов, выполняемых с использованием автоматизированной системы, программного обеспечения: дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента; идентификатор клиента; код, соответствующий выполняемому действию; идентификатор устройства
	П. 30	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов
М3.24	П. 29.2	2.6.3	Оператор по переводу денежных средств обеспечивает хранение информации, указанной в абзацах тринадцатом—шестнадцатом подпункта 2.6.3 пункта 2.6 Положения, не менее пяти лет начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения
	П. 29.3	2.6.3	Оператор по переводу денежных средств определяет во внутренних документах: порядок формирования уникального идентификатора клиента в автоматизированной системе, программном обеспечении; перечень кодов действий клиентов, выполняемых при осуществлении переводов денежных средств с использованием автоматизированной системы, программного обеспечения; подлежащий регистрации идентификатор устройства; порядок регистрации и хранения информации, указанной в абзацах тринадцатом—шестнадцатом подпункта 2.6.3 пункта 2.6 настоящего Положения

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М3.27	П. 29.1	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию следующей информации о действиях клиентов, выполняемых с использованием автоматизированной системы, программного обеспечения: дата (день, месяц, год) и время (часы, минуты, секунды) осуществления действия клиента; идентификатор клиента; код, соответствующий выполняемому действию; идентификатор устройства
М3.30	П. 29.2	2.6.3	Оператор по переводу денежных средств обеспечивает хранение информации, указанной в абзацах тринадцатом—шестнадцатом подпункта 2.6.3 пункта 2.6 Положения, не менее пяти лет начиная с даты осуществления клиентом действия, выполняемого с использованием автоматизированной системы, программного обеспечения
М3.38	П. 27	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают выполнение процедур идентификации и контроль деятельности лиц, осуществляющих техническое обслуживание банкоматов и платежных терминалов
	П. 33	2.6.5	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для контроля физического доступа к объектам информационной инфраструктуры (за исключением банкоматов, платежных терминалов и электронных средств платежа), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются
	П. 34	2.6.5	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для предотвращения физического воздействия на средства вычислительной техники и телекоммуникационное оборудование, сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов, платежных терминалов и электронных средств платежа
	П. 35	2.6.5	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для регистрации доступа к банкоматам, в том числе с использованием систем видеонаблюдения
	П. 36	2.6.6	В случае принятия оператором по переводу денежных средств, банковским платежным агентом (субагентом), оператором услуг платежной инфраструктуры решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, указанных в подпункте 2.6.5 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение указанных организационных мер защиты информации и (или) использование указанных технических средств защиты информации

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М3.39	П. 25	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации
	П. 29	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения. Банковским платежным агентом (субагентом) обеспечивается регистрация действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, при наличии технической возможности с учетом выполняемого перечня операций и используемых автоматизированных систем, программного обеспечения, эксплуатация которых обеспечивается банковским платежным агентом (субагентом)
	П. 30	2.6.3	При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных в подпункте 2.6.1 пункта 2.6 Положения, оператор по переводу денежных средств обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов
М3.53	П. 52	2.8.1	При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по сети Интернет
М4.1	П. 40	2.7.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают использование технических средств защиты информации от воздействия вредоносного кода на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности
М4.2	П. 41	2.7.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания
М4.3	П. 42	2.7.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме при наличии технической возможности
М4.5	П. 43	2.7.2	Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода
М4.7	П. 44	2.7.3	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении переводов денежных средств, при наличии технической возможности

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М4.8	П. 45	2.7.4	При наличии технической возможности оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы
М4.9	П. 46	2.7.4	При наличии технической возможности оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения
М4.10	П. 47	2.7.5	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода
	П. 48	2.7.5	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают принятие мер, направленных на устранение последствий воздействия вредоносного кода
	П. 49	2.7.5	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор платежной системы, оператор услуг платежной инфраструктуры приостанавливают при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом
	П. 50	2.7.5	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают информирование оператора платежной системы
	П. 51	2.7.5	В случае обнаружения вредоносного кода или факта воздействия вредоносного кода оператор платежной системы обеспечивает информирование операторов услуг платежной инфраструктуры и участников платежной системы
М5.7	П. 52	2.8.1	При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по сети Интернет
М5.8	П. 53	2.8.1	При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети Интернет
	П. 56	2.8.1	При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет
М5.9	П. 57	2.8.2	Оператор по переводу денежных средств обеспечивает формирование для клиентов рекомендаций по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М5.24	П. 55	2.8.1	При использовании сети Интернет для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств
М6.1	П. 70	2.9.5	Оператор платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации
М6.3	П. 58	2.9.1	Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ “Об электронной подписи”, Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 и технической документацией на СКЗИ
М6.6	П. 60	2.9.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые допускают встраивание СКЗИ в технологические процессы осуществления переводов денежных средств, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов
М6.7	П. 61	2.9.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения
М6.8	П. 59	2.9.1	В случае если оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа
М6.10	П. 62	2.9.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые поддерживают непрерывность процессов протоколирования работы СКЗИ и 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
М6.11	П. 62	2.9.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры применяют СКЗИ, которые поддерживают непрерывность процессов протоколирования работы СКЗИ и 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

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М6.14	П. 63	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств
	П. 64	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок эксплуатации СКЗИ
	П. 65	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе
	П. 66	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ
	П. 67	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок снятия с эксплуатации СКЗИ
	П. 68	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок управления ключевой системой
	П. 69	2.9.3	В случае применения СКЗИ оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей
М7.3	П. 72	2.10.2	Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств
	П. 73	2.10.2	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 Положения
М7.6	П. 72	2.10.2	Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств
	П. 73	2.10.2	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 Положения

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 74	2.10.3	Распоряжение клиента, распоряжение участника платежной системы и распоряжение платежного клирингового центра в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом
	П. 75	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации
М7.8	П. 76	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры
М7.9	П. 72	2.10.2	Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств
	П. 73	2.10.2	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 Положения
	П. 77	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают аутентификацию входных электронных сообщений
М7.10	П. 78	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями
М7.12	П. 81	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации
М7.13	П. 79	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают восстановление информации об остатках денежных средств на банковских счетах, информации об остатках электронных денежных средств и данных держателей платежных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М7.14	П. 72	2.10.2	Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств
	П. 73	2.10.2	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 Положения порядка
	П. 80	2.10.4	При эксплуатации объектов информационной инфраструктуры оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в платежной системе
М7.15	П. 39	2.6.9	Оператор по переводу денежных средств обеспечивает возможность приостановления (блокирования) клиентом приема к исполнению распоряжений об осуществлении переводов денежных средств от имени указанного клиента
М7.16	П. 72	2.10.2	Оператор платежной системы определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств
	П. 73	2.10.2	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанного в подпункте 2.10.2 пункта 2.10 Положения порядка
М7.22	П. 37	2.6.7	Оператор по переводу денежных средств, банковский платежный агент (субагент) обеспечивают контроль отсутствия размещения на платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств
М11.1	П. 82	2.11.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают формирование службы информационной безопасности, а также определяют во внутренних документах цели и задачи деятельности этой службы
М11.2	П. 83	2.11.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющейся юридическим лицом, оператор услуг платежной инфраструктуры предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач
М11.3	П. 84	2.11.1	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры назначают куратора службы информационной безопасности из состава своего органа управления и определяют его полномочия
	П. 85	2.11.1	Служба информационной безопасности и служба информатизации (автоматизации) не должны иметь общего куратора
М11.5	П. 86	2.11.2	Оператор по переводу денежных средств, имеющий филиалы, обеспечивает формирование служб информационной безопасности в указанных филиалах, определяет для них необходимые полномочия и выделяет необходимые ресурсы
	П. 87	2.11.2	Оператор по переводу денежных средств, имеющий филиалы, обеспечивает взаимодействие и координацию работ служб информационной безопасности
М11.6	П. 88	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М11.9	П. 89	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями определять требования к техническим средствам защиты информации и организационным мерам защиты информации
М11.10	П. 90	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств
М11.12	П. 91	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации
М11.13	П. 92	2.11.3	Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется полномочиями участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платежной системы после сбоев и отказов в работе объектов информационной инфраструктуры
М12.1 (М30.1)	П. 18	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления
М12.4	П. 18	2.5.6	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления
М17.1	П. 107	2.14.2	Оператор платежной системы устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств путем: самостоятельного определения оператором платежной системы порядка обеспечения защиты информации при осуществлении переводов денежных средств; распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы; передачи функций по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств оператором платежной системы, не являющимся кредитной организацией, расчетному центру
	П. 108	2.14.2	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают определение порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках распределения обязанностей, установленных оператором платежной системы
	П. 109	2.14.3	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 110	2.14.4	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 111	2.14.5	Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) применения организационных мер защиты информации
	П. 112	2.14.5	Служба информационной безопасности оператора по переводу денежных средств, оператора услуг платежной инфраструктуры осуществляет контроль (мониторинг) использования технических средств защиты информации
М18.1	П. 93	2.12.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации
	П. 94	2.12.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации по порядку использования технических средств защиты информации
	П. 96	2.12.3	Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению
М18.4	П. 93	2.12.1	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации
М18.6	П. 95	2.12.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), являющийся юридическим лицом, оператор услуг платежной инфраструктуры обеспечивают повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации
М19.1	П. 97	2.13.1	Оператор платежной системы определяет требования к порядку, форме и срокам информирования оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 98	2.13.1	Информирование оператора платежной системы о выявленных операторами по переводу денежных средств, являющимися участниками платежной системы, и операторами услуг платежной инфраструктуры, привлекаемыми для оказания услуг платежной инфраструктуры в платежной системе, инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, осуществляется ежемесячно
	П. 99	2.13.1	Оператор платежной системы определяет требования к взаимодействию оператора платежной системы, операторов по переводу денежных средств и операторов услуг платежной инфраструктуры в случае выявления в платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 100	2.13.1	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в подпункте 2.13.1 пункта 2.13 Положения требований
	П. 101	2.13.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 102	2.13.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают информирование службы информационной безопасности, в случае ее наличия, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 103	2.13.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 104	2.13.2	Оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты
	П. 106.1	2.13.4	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры обеспечивают регистрацию самостоятельно выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств. Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных клиентами данного оператора по переводу денежных средств. Оператор по переводу денежных средств обеспечивает регистрацию ставших ему известными инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, выявленных банковскими платежными агентами (субагентами)
М19.2	П. 105	2.13.3	Оператор платежной системы обеспечивает учет и доступность для операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в платежной системе, информации о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 106	2.13.3	Оператор платежной системы обеспечивает учет и доступность для операторов по переводу денежных средств, являющихся участниками платежной системы, и операторов услуг платежной инфраструктуры, привлекаемых для оказания услуг платежной инфраструктуры в платежной системе, информации о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 106.2	2.13.4	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры определяют во внутренних документах порядок регистрации и хранения сведений об инцидентах, указанных в абзацах первом—третьем подпункта 2.13.4 пункта 2.13 Положения
М22.4 (М32.3)	П. 113	2.15.2	Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России
	П. 113.1	2.15.2	Организация, ставшая оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры, должна провести первую оценку соответствия в течение шести месяцев после получения соответствующего статуса

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М22.5	П. 114	2.16.1	Оператор платежной системы устанавливает требования к содержанию, форме и периодичности представления информации, направляемой операторами по переводу денежных средств и операторами услуг платежной инфраструктуры оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств
	П. 115	2.16.1	Оператор по переводу денежных средств и оператор услуг платежной инфраструктуры обеспечивают выполнение указанных в подпункте 2.16.1 пункта 2.16 Положения требований
	П. 116	2.16.2	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств
М22.7	П. 113	2.15.2	Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры по результатам оценки соответствия в целях ее документального подтверждения формируют отчет, который утверждается исполнительными органами управления и хранится в порядке, установленном соответствующим оператором
М24.1	П. 117	2.16.2	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 118	2.16.2	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 119	2.16.2	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о результатах проведенных оценок соответствия
	П. 120	2.16.2	Информация, направляемая операторами по переводу денежных средств и операторами услуг платежной инфраструктуры, за исключением операционных центров, находящихся за пределами Российской Федерации, оператору платежной системы для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, включает информацию о выявленных угрозах и уязвимостях в обеспечении защиты информации

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
М26.1	П. 121	2.17.1	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями требований к защите информации, определенных правилами платежной системы
	П. 122	2.17.1	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе
	П. 123	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения требований к защите информации, определенных правилами платежной системы
	П. 124	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе
	П. 125	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 126	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств
	П. 127	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 128	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия
М26.4	П. 121	2.17.1	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями требований к защите информации, определенных правилами платежной системы
	П. 122	2.17.1	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 123	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения требований к защите информации, определенных правилами платежной системы
	П. 124	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе
	П. 125	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 126	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств
	П. 127	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 128	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия
М26.6	П. 129	2.17.3	Принятие решений оператора по переводу денежных средств, оператора услуг платежной инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности
М27.1	П. 122	2.17.1	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе
	П. 123	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения требований к защите информации, определенных правилами платежной системы
	П. 124	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 125	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 126	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств
	П. 127	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 128	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия
М27.6	П. 122	2.17.1	Оператор платежной системы, оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных оператором платежной системы, в связи с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе
	П. 123	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения требований к защите информации, определенных правилами платежной системы
	П. 124	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующих отношения в национальной платежной системе
	П. 125	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 126	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 127	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 128	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия
М27.7	П. 129	2.17.3	Принятие решений оператора по переводу денежных средств, оператора услуг платежной инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности

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.