СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2009

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-2008

Дата введения: 2009-06-01

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 7 мая 2009 года N Р-496.

2. ВЗАМЕН СТО БР ИББС-1.2-2007.

Введение

Стандартом Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (СТО БР ИББС-1.0-2008) с целью проверки уровня информационной безопасности (ИБ) как самого Банка России, так и организаций банковской системы (БС) Российской Федерации (РФ) определено требование проведения регулярной внешней и внутренней оценки ИБ, а также самооценки ИБ.

Настоящий стандарт устанавливает способы определения степени выполнения требований Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (СТО БР ИББС-1.0-2008), а также итогового уровня соответствия ИБ требованиям стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (СТО БР ИББС-1.0-2008) при проведении внутренней и (или) внешней оценки и самооценки ИБ.

1. Область применения

Настоящая методика распространяется на организации БС РФ, а также на организации, проводящие оценку уровня обеспечения ИБ организации БС РФ в соответствии с требованиями Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (СТО БР ИББС-1.0-2008, далее - СТО БР ИББС-1.0).

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

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

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на 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 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности" (СТО БР ИББС-1.1-2007), а также следующие термины с соответствующими определениями.

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

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

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

4. Обозначения и сокращения

АБС - автоматизированная банковская система;
БС - банковская система;
ЖЦ - жизненный цикл;
ИБ - информационная безопасность;
НСД - несанкционированный доступ;
НРД - нерегламентированные действия в рамках предоставленных полномочий;
РФ - Российская Федерация;
СКЗИ - средство криптографической защиты информации;
СМИБ - система менеджмента информационной безопасности;
СИБ - система информационной безопасности;
СОИБ - система обеспечения информационной безопасности;
ЭВМ - электронная вычислительная машина;
ЭЦП - электронная цифровая подпись;
$\alpha_{i.j}$ - коэффициент значимости частного показателя;
$EV1$ - оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "текущий уровень ИБ организации";
$EV2$ - оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "менеджмент ИБ организации";
$EV3$ - оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "уровень осознания ИБ организации";
$EV_{БИТП}$ - 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;
$EV_{Mi.j}$ - оценка степени выполнения требований СТО БР ИББС-1.0 для частного показателя;
i - номер группового показателя;

j - номер частного показателя;
Mi.j - обозначение частного показателя;

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

5. Общие положения

5.1. Целью настоящей методики является стандартизация подходов и способов оценки, используемых для определения уровня соответствия ИБ организации БС РФ (далее - организации) требованиям СТО БР ИББС-1.0 по направлениям оценки:

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

5.2. Задачами настоящей методики являются:

- определение состава показателей ИБ и способов их оценивания;
- определение способа оценивания текущего уровня ИБ организации с помощью установления степени выполнения требований, определенных в разделе 7 СТО БР ИББС-1.0;
- определение способа оценивания менеджмента ИБ организации и уровня осознания ИБ организации с помощью установления степени выполнения требований, определенных в разделе 8 СТО БР ИББС-1.0;
- определение итогового уровня соответствия ИБ организации требованиям СТО БР ИББС-1.0.

6. Показатели информационной безопасности. Способы оценивания показателей

6.1. Для оценки степени соответствия ИБ организации требованиям СТО БР ИББС-1.0 используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ. Оценки групповых показателей (EV_{Mi}) используются для получения оценки по направлениям (EV1, EV2 и EV3). Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки ($EV_{Mi.j}$), которые затем формируют оценки EV_{Mi} групповых показателей.

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

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

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

6.4. Оценка $EV_{Mi.j}$ частного показателя формируется на основании выявленной аудиторской группой степени выполнения требований посредством

экспертного оценивания.

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

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

- "нет" - оценке присваивается значение, равное нулю;
- "частично" - оценке присваивается значение 0,25; 0,5 или 0,75;
- "да" - оценке присваивается значение, равное единице.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- внутренние нормативные документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации;

- устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;

- результаты наблюдений членов аудиторской группы за деятельностью сотрудников проверяемой организации в области ИБ.

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

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

6.12. Оценка группового показателя (EV_{Mi}) вычисляется из оценок входящих в него частных показателей ($EV_{Mi.j}$) с учетом коэффициентов значимости альфа ($альфа_{i.j}$), определяющих важность частного показателя для оценивания группового показателя:

$$EV_{Mi} = SUM_{j} альфа_{i.j} \times EV_{Mi.j}.$$

При формировании коэффициентов значимости учитывалось следующее условие нормировки:

$$SUM_{j=1}^{k} альфа_{i.j} = 1,$$

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

Коэффициенты значимости альфа ($альфа_{i.j}$) для каждого частного показателя приведены в Приложении А.

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 $EV_{БИТП}$, $EV_{БПТП}$, EV2 или EV3 (см. разделы 7, 8, 9) с соответствующей корректировкой в формулах расчета количества оцениваемых групповых показателей. Оценки для таких групповых показателей не отображаются на круговой диаграмме (см. раздел 10).

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

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

- обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу;
- обеспечение ИБ на стадиях жизненного цикла АБС;
- обеспечение ИБ при управлении доступом и регистрацией;
- обеспечение ИБ средствами антивирусной защиты;
- обеспечение ИБ при использовании ресурсов сети Интернет;
- обеспечение ИБ при использовании средств криптографической защиты информации;
- обеспечение ИБ банковских платежных технологических процессов;
- обеспечение ИБ банковских информационных технологических процессов.

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

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

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M1	Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу	п. 7.2
M2	Обеспечение ИБ на стадиях жизненного цикла АБС	п. 7.3
M3	Обеспечение ИБ при управлении доступом и регистрации	п. 7.4
M4	Обеспечение ИБ средствами антивирусной защиты	п. 7.5
M5	Обеспечение ИБ при использовании ресурсов сети Интернет	п. 7.6
M6	Обеспечение ИБ при использовании средств криптографической защиты информации	п. 7.7
M7	Обеспечение ИБ банковских платежных технологических процессов	п. 7.8
M8	Обеспечение ИБ банковских информационных технологических процессов	п. 7.9

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 - M8), метрики, а также коэффициенты значимости альфа $_{i.j}$ для каждого частного показателя приведены в Приложении А.

7.4. Оценивание частных показателей в рамках групповых показателей M1

.
- М6 необходимо осуществлять по результатам анализа выполнения
.
соответствующих требований СТО БР ИББС-1.0 применительно к организации в целом, включая банковский платежный технологический процесс (М7) и банковский информационный технологический процесс (М8).

7.5. Оценки $EV_{Mi.j}$ и EV_{Mi}, полученные в результате оценивания групповых
.
показателей ИБ М1 - М8, вносятся в соответствующие графы представленных
.
в Приложении А форм.

7.6. Итоговая оценка EV1, отражающая степень выполнения требований СТО БР ИББС-1.0 по направлению "текущий уровень ИБ организации", определяется по наименьшему значению из оценок уровней ИБ банковского платежного технологического процесса и банковского информационного технологического процесса.

7.7. Оценка уровня ИБ банковского платежного технологического процесса вычисляется по формуле:

$$EV_{БПТП} = \frac{SUM\ EV_i + EV_{M7}}{7}, i = 1 - 6.$$
.

Оценка уровня ИБ банковского информационного технологического процесса вычисляется по формуле:

$$EV_{БИТП} = \frac{SUM\ EV_i + EV_{MB}}{7}, i = 1 - 6.$$
.

7.8. Оценки EV_{Mi}, полученные в результате оценивания групповых
.
показателей ИБ М1 - М8, отображаются на круговой диаграмме (см. раздел 10)
.
в секторах с 1-го по 8-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

7.9. Оценка EV1 отображается на круговой диаграмме (см. раздел 10) в секторах с 1-го по 8-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению EV1.

8. Оценка менеджмента информационной безопасности организации банковской системы Российской Федерации

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

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

- организация реализации планов обработки рисков нарушения ИБ;
- разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ;
- организация обнаружения и реагирования на инциденты безопасности;
- организация обеспечения непрерывности бизнеса и его восстановления после прерываний;
- мониторинг и контроль защитных мер;
- проведение самооценки ИБ;
- проведение внешнего аудита ИБ;
- анализ функционирования СОИБ;
- анализ СОИБ со стороны руководства организации;
- принятие решений по тактическим улучшениям СОИБ;
- принятие решений по стратегическим улучшениям СОИБ.

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

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

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
М9	Организация и функционирование службы ИБ организации	п. 8.2
М10	Определение/коррекция области действия СОИБ	п. 8.3
М11	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ	п. 8.4
М12	Разработка планов обработки рисков нарушения ИБ	п. 8.5
М13	Разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ	п. 8.6
М14	Принятие руководством организации решений о реализации и эксплуатации СОИБ	п. 8.7
М15	Организация реализации планов внедрения СОИБ	п. 8.8
М16	Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ	п. 8.9
М17	Организация обнаружения и реагирования на инциденты безопасности	п. 8.10
М18	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний	п. 8.11
М19	Мониторинг и контроль защитных мер	п. 8.12
М20	Проведение самооценки ИБ	п. 8.13
М21	Проведение аудита ИБ	п. 8.14
М22	Анализ функционирования СОИБ	п. 8.15

M23	Анализ СОИБ со стороны руководства организации	п. 8.16
M24	Принятие решений по тактическим улучшениям СОИБ	п. 8.17
M25	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 M9 - M25), метрики, а также коэффициенты значимости альфа $_{i.j}$ для каждого частного показателя приведены в Приложении А.

8.4. Оценки $EV_{Mi.j}$ и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M9 - M25, вносятся в соответствующие графы представленных в Приложении А форм.

8.5. Итоговая оценка EV2, отражающая степени выполнения требований СТО БР ИББС-1.0 по направлению "менеджмент ИБ организации", вычисляется по формуле:

$$EV2 = \frac{\sum_{i=9}^{25} EV_{Mi}}{17}.$$

8.6. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M9 - M25, отображаются на круговой диаграмме (см. раздел 10) в секторах с 9-го по 25-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

8.7. Оценка EV2 отображается на круговой диаграмме (см. раздел 10) в секторах с 9-го по 25-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению EV2.

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

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

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

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

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

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M26	Оценка деятельности руководства организации по поддержке функционирования службы ИБ организации	п. 8.2
M27	Оценка деятельности руководства организации по принятию решений о реализации и эксплуатации СОИБ	п. 8.7
M28	Оценка деятельности руководства организации по поддержке планирования СОИБ	п. 8.3, 8.4, 8.5, 8.6, 8.8
M29	Оценка деятельности руководства организации по поддержке реализации СОИБ	п. 8.9, 8.10, 8.11
M30	Оценка деятельности руководства организации по поддержке проверки СОИБ	п. 8.12, 8.13, 8.14, 8.15
M31	Оценка деятельности руководства организации по анализу СОИБ	п. 8.16
M32	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 M25 - M32), метрики, а также коэффициенты значимости альфа для каждого частного показателя приведены в Приложении А.

9.4. Оценки $EV_{Mi.j}$ и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M25 - M32, вносятся в соответствующие графы представленных в Приложении А форм.

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

$$EV3 = \frac{\sum_{i=26}^{32} EV_{Mi}}{7}.$$

9.6. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M26 - M32, отображаются на круговой диаграмме (см. раздел 10) в секторах с 26-го по 32-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

9.7. Оценка EV3 отображается на круговой диаграмме (см. раздел 10) в секторах с 26-го по 32-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению EV3.

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

10.1. Если оценка EV1, EV2 или EV3 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 EV1, EV2 или EV3 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 EV1, EV2 или EV3 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 EV1, EV2 или EV3 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 EV1, EV2 или EV3 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 EV1, EV2 или EV3 лежит в интервале от 0,95 до 1 включительно, то данному направлению оценки присваивается пятый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

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

- оценки уровня осознания ИБ организации (EV3);
- оценки менеджмента ИБ организации (EV2);
- оценки текущего уровня ИБ организации (EV1).

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

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

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

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

Секторы с 1-го по 8-й используются для отображения оценки текущего уровня ИБ организации.

Секторы с 9-го по 25-й используются для отображения оценки процессов менеджмента ИБ организации.

Секторы с 26-го по 32-й используются для отображения оценки уровня осознания ИБ организации.

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

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

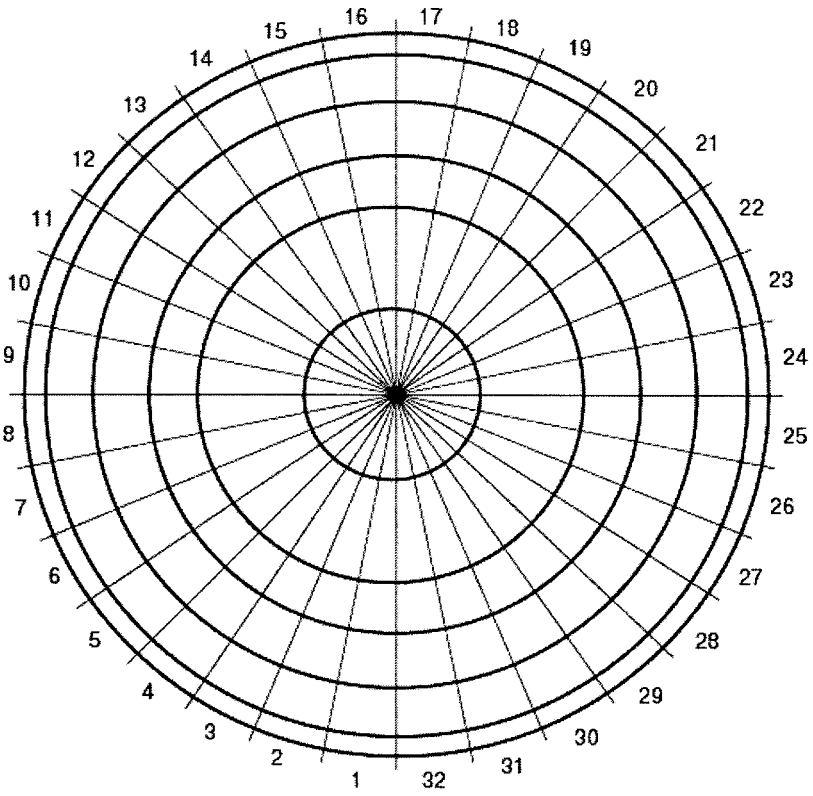
Третьему уровню соответствуют окружность радиусом 0,7 и кольцо до окружности радиусом 0,85.

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

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

Нулевому уровню соответствует круг до окружности радиусом 0,25.

Рисунок 1 - Круговая диаграмма для отображения результатов оценивания



Приложение А

(обязательное)

ПОКАЗАТЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М1.1	Определены ли в документах организации роли ее работников?	обязательный							0,0581	
М1.2	Формируются ли роли, связанные с выполнением деятельности по обеспечению ИБ, на основании требований разделов 7 и 8 стандарта СТО БР ИББС-1.0?	обязательный							0,0291	
М1.3	Персонифицированы ли роли в организации с установлением ответственности за их выполнение?	обязательный							0,0502	
М1.4	Зафиксирована ли документально в должностных инструкциях ответственность за выполнение ролей?	обязательный							0,0461	

М1.5	Отсутствуют ли в организации роли, совмещающие функции разработки и сопровождения системы/ПО?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0522	
М1.6	Отсутствуют ли в организации роли, совмещающие функции разработки и эксплуатации системы/ПО?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0610	
М1.7	Отсутствуют ли в организации роли, совмещающие функции сопровождения и эксплуатации?	рекомендуемый	//// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0522	
М1.8	Отсутствуют ли в организации роли, совмещающие функции администратора системы и администратора информационной безопасности?	рекомендуемый	//// //// //// //// ////	///// ///// ///// ///// /////	///// ///// ///// ///// /////	///// ///// ///// ///// /////			0,0661	
М1.9	Отсутствуют ли в организации роли, совмещающие функции по выполнению операций в системе и контроля их выполнения?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0661	
М1.10	Определены ли документально в организации и выполняются ли процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации?	обязательный							0,1001	

М1.11	Определены ли в документах организации процедуры приема на работу, влияющую на обеспечение ИБ, включающие: - проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических навыков; - проверку в части профессиональных навыков и оценку профессиональной пригодности?	обязательный							0,0513	
М1.12	Предусматривают ли указанные в частном показателе М1.11 процедуры документальную фиксацию результатов проводимых проверок?	обязательный							0,0371	
М1.13	Определены ли в документах организации процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников?	рекомендуемый	//// //// //// //// ////	///// ///// ///// ///// /////	///// ///// ///// ///// /////	///// ///// ///// ///// /////			0,0302	
М1.14	Предусматривают ли указанные в частном показателе М1.13 процедуры документальную фиксацию результатов проводимых проверок?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0302	Р
М1.15	Определены ли в документах организации процедуры внеплановой проверки работников при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0433	

М1.16	Предусматривают ли указанные в частном показателе М1.15 процедуры документальную фиксацию результатов проводимых проверок?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0391	
М1.17	Обязаны ли все работники организации давать письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов?	обязательный							0,0383	
М1.18	Регламентируются ли положениями, включенными в договоры (соглашения) с внешними организациями и клиентами, требования по ИБ?	обязательный							0,0449	
М1.19	Определены ли в трудовых контрактах (соглашениях, договорах) и (или) должностных инструкциях обязанности персонала по выполнению требований ИБ?	обязательный							0,0582	
М1.20	Приравнивается ли невыполнение работниками организации требований ИБ к невыполнению должностных обязанностей и приводит ли как минимум к дисциплинарной ответственности?	обязательный							0,0462	
Итоговая оценка группового показателя М1										

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М2.1	Рассматриваются ли при формировании требований ИБ следующие стадии модели ЖЦ АБС: - разработка технических заданий; - проектирование; - создание и тестирование; - приемка и ввод в действие; - эксплуатация; - сопровождение и модернизации; - снятие с эксплуатации?	рекомендуемый	//// ////	///// /////	///// /////	///// /////			0,0504	
М2.2	Осуществляются ли разработка технических заданий и приемка АБС по согласованию и при участии подразделения (лиц) в организации, ответственных за обеспечение ИБ?	обязательный							0,0616	
М2.3	Осуществляются ли ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС под контролем подразделений (лиц) в организации, ответственных за обеспечение ИБ?	обязательный							0,0591	

М2.4	Имеют ли соответствующие лицензии организации, которые привлекаются на договорной основе для разработки и (или) производства средств и систем защиты АБС?	обязательный							0,0563	
М2.5	Снабжены ли разрабатываемые АБС и (или) их компоненты документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации?	обязательный							0,0646	
М2.6	Снабжены ли приобретаемые организацией АБС и (или) их компоненты документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации?	рекомендуемый	//// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// /////			0,0604	
М2.7	Содержит ли документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки?	обязательный							0,0450	

М2.8	Реализуется ли при взаимодействии организации с разработчиком АБС и их компонентов одна из трех альтернатив: 1) в договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов включаются положения по сопровождению поставляемых изделий на весь срок их службы; 2) организация приобретает полный комплект рабочей конструкторской документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика; 3) руководство организации оценивает и документально оформляет допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов?	обязательный							0,0604	

М2.9	Учитывается ли при разработке технических заданий на системы дистанционного банковского обслуживания, что защита данных должна обеспечиваться в условиях: - попыток доступа к банковской информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования; - возможности ошибок авторизованных пользователей систем; - возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями?	обязательный							0,0596	
М2.10	Обеспечиваются ли на стадии тестирования анонимность данных и проверка адекватности разграничения доступа?	обязательный							0,0474	
М2.11	Определены ли в документах организации и выполняются ли на стадии эксплуатации АБС процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер?	обязательный							0,0700	
М2.12	Предусматривают ли указанные в частном показателе М2.11 процедуры документальную фиксацию результатов контроля?	обязательный							0,0626	

М2.13	Определены ли в документах организации и выполняются ли на стадии сопровождения (модернизации) АБС процедуры контроля, обеспечивающие защиту от: - умышленного несанкционированного раскрытия, модификации или уничтожения информации; - неумышленной модификации, раскрытия или уничтожения информации; - отказа в обслуживании или ухудшения обслуживания?	обязательный							0,0596	
М2.14	Предусматривают ли указанные в частном показателе М2.13 процедуры документальную фиксацию результатов контроля?	обязательный							0,0533	
М2.15	Проводятся ли на стадии сопровождения (модернизации) при любом внесении изменений в АБС процедуры проверки функциональности, результаты которых документируются?	обязательный							0,0646	

М2.16	Определены ли документально и выполняются ли на стадии снятия с эксплуатации процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и с внешних носителей (за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами)?	обязательный							0,0675	
М2.17	Предусматривают ли указанные в частном показателе М2.16 процедуры документальную фиксацию результатов их выполнения?	обязательный							0,0576	
Итоговая оценка группового показателя М2										

Групповой показатель М3 "Обеспечение информационной безопасности при управлении доступом и регистрации"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М3.1	Определен ли в документах организации перечень информационных активов (их типов)?	обязательный							0,0356	
М3.2	Зафиксированы ли документально права доступа работников и клиентов к информационным активам организации?	обязательный							0,0360	
М3.3	Применяются ли в составе АБС встроенные защитные меры?	обязательный							0,0345	
М3.4	Применяются ли в составе АБС сертифицированные или разрешенные к применению руководством организации средства защиты информации от НСД и НРД и средства криптографической защиты информации?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0334	
М3.5	Определены ли в документах организации, утверждены ли руководством организации, выполняются ли и контролируются ли процедуры идентификации, аутентификации и авторизации?	обязательный							0,0366	
М3.6	Документируются ли результаты контроля процедур, указанных в частном показателе М3.5?	обязательный							0,0345	
М3.7	Определены ли в документах организации, выполняются ли и контролируются ли процедуры управления доступом?	обязательный							0,0360	
М3.8	Документируются ли результаты контроля процедур, указанных в частном показателе М3.7?	обязательный							0,0334	

М3.9	Определены ли в документах организации, выполняются ли и контролируются ли процедуры контроля целостности?	обязательный							0,0340	
М3.10	Документируются ли результаты контроля процедур, указанных в частном показателе М3.9?	обязательный							0,0319	
М3.11	Определены ли в документах организации, выполняются ли и контролируются ли процедуры регистрации событий и действий?	обязательный							0,0319	
М3.12	Документируются ли результаты контроля процедур, указанных в частном показателе М3.11?	обязательный							0,0286	
М3.13	Исключают ли процедуры управления доступом возможность "самосанкционирования"?	обязательный							0,0308	
М3.14	Определены ли в документах организации процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявить неправомерные или подозрительные операции и транзакции?	обязательный							0,0331	
М3.15	Используются ли специализированные программные и (или) технические средства для проведения процедур мониторинга и анализа данных регистрации, действия и операций?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0255	

М3.16	Используют ли процедуры мониторинга и анализа документально определенные критерии выявления неправомерных или подозрительных действий и операций?	обязательный							0,0266	
М3.17	Применяются ли процедуры мониторинга и анализа на регулярной основе (например, ежедневно) ко всем выполненным операциям и транзакциям?	обязательный							0,0286	
М3.18	Регламентирован ли во внутренних документах организации порядок доступа работников организации в помещения, в которых размещаются объекты среды информационных активов?	обязательный							0,0292	
М3.19	Контролируется ли выполнение порядка доступа работников организации в помещения, в которых размещаются объекты среды информационных активов?	обязательный							0,0297	
М3.20	Оформляются ли документально результаты выполнения контроля порядка доступа работников организации в помещения, в которых размещаются объекты среды информационных активов?	обязательный							0,0263	

М3.21	Обеспечивают ли используемые в организации АБС, в том числе системы дистанционного банковского обслуживания, возможность регистрации: - операций с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов; - проводимых транзакций, имеющих финансовые последствия; - операций, связанных с назначением и распределением прав пользователей?	обязательный							0,0328	
М3.22	Реализованы ли в системах дистанционного банковского обслуживания, используемых в организации, защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций (например, ЭЦП)?	обязательный							0,0344	
М3.23	Придано ли протоколам операций, выполняемых посредством дистанционного банковского обслуживания, свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание?	рекомендуемый	////	/////	/////	/////			0,0312	

М3.24	Производится ли при заключении договоров со сторонними организациями юридическое оформление договоренностей, определяющих необходимый уровень взаимодействия в случае выхода инцидента ИБ за рамки отдельной организации?	рекомендуемый	//// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// /////			0,0274	
М3.25	Определены ли в документах организации процедуры, определяющие действия работников и клиентов организации в случае компрометации информации, необходимой для их идентификации, аутентификации и (или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев?	обязательный							0,0294	
М3.26	Доведены ли до сведения работников и клиентов организации процедуры, указанные в частном показателе М3.25?	обязательный							0,0283	
М3.27	Предусматривают ли указанные в частном показателе М3.26 процедуры документирование работниками и клиентами своих действий и их результатов?	обязательный							0,0254	

М3.28	Реализованы ли в системах дистанционного банковского обслуживания механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имени?	обязательный							0,0239	
М3.29	Применяются ли в организации защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и(или) авторизации клиентов и работников организации?	обязательный							0,0319	
М3.30	Регистрируются ли все попытки НСД и НРД к информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и сотрудников организации?	обязательный							0,0326	
М3.31	Определена ли в документах организации и выполняется ли процедура пересмотра прав доступа при увольнении или изменении должностных обязанностей работников организации, имевших доступ к информации, необходимой для идентификации, аутентификации и(или) авторизации клиентов и сотрудников организации?	обязательный							0,0316	

М3.32	Осуществляется ли работа всех пользователей АБС под уникальными учетными записями?	обязательный							0,0349	
Итоговая оценка группового показателя М3										

Групповой показатель М4 "Обеспечение информационной безопасности средствами антивирусной защиты"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М4.1	Применяются ли на всех автоматизированных рабочих местах и серверах АБС организации, если иное не предусмотрено технологическим процессом, средства антивирусной защиты?	обязательный							0,0744	
М4.2	Определены ли в документах организации процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС?	обязательный							0,0721	
М4.3	Осуществляются ли установка и регулярное обновление средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС администраторами АБС или иными официально уполномоченными лицами?	обязательный							0,0653	

М4.4	Организован ли автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0559	
М4.5	Контролируются ли установка и обновление антивирусных средств представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ?	обязательный							0,0688	
М4.6	Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме?	рекомендуемый	//// //// ////	///// ///// /////	///// ///// /////	///// ///// /////			0,0583	
М4.7	Разработаны и введены ли в действие инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов?	обязательный							0,0619	
М4.8	Проводится ли антивирусная фильтрация всего трафика электронного почтового обмена?	обязательный							0,0706	
М4.9	Построена ли в организации эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах?	рекомендуемый	//// //// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// /////			0,0501	

М4.10	Определены ли в документах организации и выполняются ли процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов?	обязательный							0,0605	
М4.11	Проводится ли антивирусная проверка после установки и изменения программного обеспечения?	обязательный							0,0616	
М4.12	Документируются ли результаты установки, изменения программного обеспечения и антивирусной проверки?	обязательный							0,0619	
М4.13	Определены ли в документах организации процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых зафиксированы: - необходимые меры по отражению и устранению последствий вирусной атаки; - порядок официального информирования руководства; - порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки)?	обязательный							0,0651	

М4.14	Определены ли в документах организации и выполняются ли процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АБС?	обязательный							0,0557	
М4.15	Предусматривают ли указанные в частном показателе М4.14 процедуры документальную фиксацию результатов контроля?	обязательный							0,0513	
М4.16	Возложена ли обязанность по выполнению предписанных мер антивирусной защиты на каждого работника организации, имеющего доступ к ЭВМ и(или) АБС, а ответственность за выполнение требований инструкции по антивирусной защите - на руководителей функциональных подразделений организации?	обязательный							0,0665	
Итоговая оценка группового показателя М4										

Групповой показатель М5 "Обеспечение информационной безопасности при использовании ресурсов сети Интернет"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М5.1	Принято ли документально руководством организации решение об использовании сети Интернет для производственной и(или) собственной хозяйственной деятельности, в котором явно перечислены цели использования сети Интернет?	обязательный							0,0586	
М5.2	Запрещается ли использование ресурсов сети Интернет в неустановленных целях?	обязательный							0,0512	
М5.3	Проведено ли в организации выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0398	
М5.4	Проводится ли наделение работников организации правами пользователя конкретного пакета в соответствии с его должностными обязанностями, в частности, в соответствии с назначенными ему ролями?	рекомендуемый	//// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// /////			0,0355	
М5.5	Оформляется ли документально наделение работников организации правами пользователя конкретного пакета?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,0398	

M5.6	Определен ли документально в организации порядок подключения и использования ресурсов сети Интернет, включающий в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственных за обеспечение ИБ?	обязательный							0,0583	
M5.7	Применяются ли при осуществлении дистанционного банковского обслуживания с использованием сети Интернет средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации), которые обеспечивают прием и передачу информации только в установленном формате и только по конкретной технологии?	обязательный							0,0518	
M5.8	Выполнено ли выделение и организована ли физическая изоляция от внутренних сетей тех ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0292	
M5.9	Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный							0,0479	

M5.10	Регистрируются ли регламентированным образом попытки подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный							0,0440	
M5.11	Все ли операции клиентов в течение сеанса работы с системами дистанционного банковского обслуживания выполняются только после проведения процедур идентификации, аутентификации и авторизации?	обязательный							0,0581	
M5.12	Обеспечивается ли повторное выполнение процедур идентификации, аутентификации и авторизации в случаях нарушения или разрыва соединения при работе с системами дистанционного банковского обслуживания?	обязательный							0,0415	
M5.13	Используется ли специализированное клиентское программное обеспечение для доступа пользователей к системам дистанционного банковского обслуживания?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0331	
M5.14	Применяются ли защитные меры для осуществления почтового обмена через сеть Интернет?	обязательный							0,0450	
M5.15	Определены ли в документах организации перечень защитных мер и порядок их использования для осуществления почтового обмена через сеть Интернет?	обязательный							0,0491	

M5.16	Организован ли почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски)?	рекомендуемый							0,0331	
M5.17	Осуществляется ли архивирование электронной почты?	обязательный							0,0368	
M5.18	Доступен ли архив электронной почты подразделению (лицу), ответственному за обеспечение ИБ?	обязательный							0,0368	
M5.19	Не допускаются ли изменения в архиве электронной почты?	обязательный							0,0390	
M5.20	Определен ли документально порядок доступа к информации архива электронной почты?	обязательный							0,0433	
M5.21	Не применяется ли в организации практика хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которой осуществляется взаимодействие с сетью Интернет в режиме on-line?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0436	

М5.22	Всегда ли наличие банковской информации на ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, определяется бизнес-целями организации и документально санкционируется ее руководством?	обязательный							0,0430	
М5.23	Определены ли документально и используются ли защитные меры, позволяющие обеспечить противодействие атакам хакеров и распространению спама?	обязательный							0,0415	
Итоговая оценка группового показателя М5										

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М6.1	Проводится ли применение СКЗИ в АБС в соответствии с моделью нарушителя, принятой в организации, с целью защиты информации при ее обработке, хранении и передаче по каналам связи?	обязательный							0,0776	

М6.2	Утверждена ли политика (концепция) применения СКЗИ в организации?	рекомендуемый	//// //// ////	///// ///// /////	///// ///// /////	///// ///// /////			0,0694	
М6.3	Допускают ли СКЗИ возможность встраивания в технологическую схему обработки электронных сообщений?	обязательный							0,0691	
М6.4	Обеспечивают ли СКЗИ взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов?	обязательный							0,0691	
М6.5	Поставляются ли СКЗИ разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения?	обязательный							0,0919	

М6.6	Выполняется ли как минимум одна из трех альтернатив: - сертифицированы ли СКЗИ уполномоченным государственным органом; - реализованы ли СКЗИ на основе рекомендованных уполномоченным государственным органом алгоритмов либо алгоритмов, определенных условиями договора с контрагентом (клиентом) организации; - соответствуют ли СКЗИ стандартам организации, взаимодействующей с проверяемой организацией?	обязательный							0,0936	
М6.7	Поддерживается ли непрерывность процессов протоколирования работы СКЗИ при применении СКЗИ в АБС?	обязательный							0,0755	
М6.8	Поддерживается ли непрерывность процессов обеспечения целостности программного обеспечения для всех звеньев АБС, взаимодействующих со СКЗИ?	обязательный							0,0755	
М6.9	Обеспечивается ли ИБ процессов изготовления ключевых документов СКЗИ комплексом технологических, организационных, технических и программных мер и средств защиты?	обязательный							0,0847	

М6.10	Реализованы ли процедуры мониторинга, предусматривающие регистрацию всех значимых событий, состоявшихся в процессе обмена электронными сообщениями, и всех инцидентов ИБ?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0755	
М6.11	Определен ли руководством порядок применения СКЗИ в АБС, включающий: - порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС; - порядок эксплуатации; - порядок восстановления работоспособности в аварийных случаях; - порядок внесения изменений; - порядок снятия с эксплуатации; - порядок управления ключевой системой; - порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей?	обязательный							0,0745	
М6.12	Самостоятельно ли изготавливаются в организации и(или) физическим лицом ключи ЭЦП и(или) иных СКЗИ?	обязательный							0,0663	
М6.13	Отражены ли в соответствующих договорах правовые и организационные последствия изготовления ключей СКЗИ для одной организации в другой организации?	обязательный							0,0773	

Итоговая оценка группового показателя М6	

Групповой показатель М7 "Обеспечение информационной безопасности банковских платежных технологических процессов"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М7.1	Определен ли в документах организации банковский платежный технологический процесс?	обязательный							0,0405	
М7.2	Определены ли документально перечни программного обеспечения, устанавливаемого и(или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских платежных технологических процессов?	обязательный							0,0365	
М7.3	Соответствует ли состав установленного и используемого в ЭВМ и АБС программного обеспечения определенному перечню?	обязательный							0,0389	
М7.4	Контролируется ли выполнение требований, оцениваемых в частных показателях М7.2, М7.3 с документированием результатов контроля?	обязательный							0,0319	

М7.5	Зафиксирован ли порядок обмена платежной информацией в договорах между участниками данного обмена?	обязательный							0,0451	
М7.6	Отсутствуют ли в организации работники, обладающие полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения несанкционированных операций по изменению состояния банковских счетов?	обязательный							0,0448	
М7.7	Контролируются (проверяются) ли и удостоверяются ли результаты технологических операций по обработке платежной информации лицами/автоматизированными процессами?	обязательный							0,0458	
М7.8	Осуществляются ли обработка платежной информации и контроль (проверка) результатов обработки разными работниками / автоматизированными процессами?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0442	
М7.9	Возложены ли обязанности по администрированию средств защиты платежной информации приказами или распоряжениями по организации на администраторов ИБ с отражением этих обязанностей в должностных инструкциях?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0365	

М7.10	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений?	обязательный							0,0436	
М7.11	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса доступ работника организации только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации?	обязательный							0,0384	
М7.12	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации?	обязательный							0,0389	

М7.13	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса аутентификацию входящих электронных платежных сообщений?	обязательный							0,0412	
М7.14	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями?	обязательный							0,0412	
М7.15	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса возможность ввода платежной информации в АБС только для авторизованных пользователей?	обязательный							0,0436	
М7.16	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершения операций и т.д.)?	обязательный							0,0436	

М7.17	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники?	обязательный							0,0392	
М7.18	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса при осуществлении межбанковских расчетов сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями?	обязательный							0,0436	
М7.19	Предусматривает ли комплекс мер по обеспечению ИБ банковского платежного технологического процесса доставку электронных платежных сообщений участникам обмена?	обязательный							0,0408	
М7.20	Организован ли в организации авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип "двойного управления")?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0364	

М7.21	Определены ли в документах организации и выполняются ли при проектировании, разработке, эксплуатации систем дистанционного банковского обслуживания процедуры, реализующие механизмы: - снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами; - доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов?	обязательный							0,0337	
М7.22	Обеспечены ли клиенты систем дистанционного банковского обслуживания детальными инструкциями, описывающими процедуры выполнения операций или транзакций?	обязательный							0,0364	
М7.23	Определены ли в документах организации и выполняются ли процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену их программных и(или) аппаратных частей?	обязательный							0,0368	

М7.24	Определена ли в документах организации, согласована ли со службой либо лицом, отвечающим в организации за обеспечение ИБ, и выполняется ли процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации?	обязательный							0,0392	
М7.25	Определена ли в документах организации, согласована ли со службой либо лицом, отвечающим в организации за обеспечение ИБ, и выполняется ли процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации?	обязательный							0,0392	
Итоговая оценка группового показателя М7										

Групповой показатель М8 "Обеспечение информационной безопасности банковских информационных технологических процессов"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М8.1	Проведена ли в организации классификация неплатежной информации?	рекомендуемый	//// //// ////	///// ///// /////	///// ///// /////	///// ///// /////			0,0852	

М8.2	Проводится ли классификация неплатежной информации в соответствии со степенью тяжести последствий потери ее свойств ИБ, в частности свойств доступности, целостности и конфиденциальности?	рекомендуемый	//// //// //// //// //// ////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// /////			0,0779	
М8.3	Определен ли документально набор требований по защите каждого из типов неплатежных информационных активов (типов неплатежной информации), полученных в результате классификации?	обязательный							0,0970	
М8.4	Возложены ли обязанности по администрированию средств защиты неплатежной информации приказами или распоряжениями по организации на администраторов ИБ с отражением этих обязанностей в должностных инструкциях?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0814	
М8.5	Определен ли документально порядок контроля функционирования со стороны лиц, отвечающих за ИБ, для каждой АБС организации?	обязательный							0,0777	
М8.6	Определены ли в документах организации банковские информационные технологические процессы, согласованы ли эти документы со службой ИБ организации?	обязательный							0,0740	
М8.7	Реализованы ли банковские информационные технологические процессы в рамках созданных для этих целей АБС?	обязательный							0,0639	

М8.8	Изолированы ли серверы, офисные ЭВМ и другое оборудование, не входящее в состав АБС, реализующих банковские информационные технологические процессы, от указанных АБС на уровне локальных вычислительных сетей способом, согласованным со службой либо лицом, отвечающим в организации за ИБ?	рекомендуемый	//// //// //// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// /////			0,0758	
М8.9	Определены ли документально перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских информационных технологических процессов?	обязательный							0,0646	
М8.10	Соответствует ли состав установленного и используемого в ЭВМ и АБС программного обеспечения определенному перечню?	обязательный							0,0646	
М8.11	Контролируется ли выполнение требований частных показателей М8.9, М8.10 с документированием результатов контроля?	обязательный							0,0676	

М8.12	Регламентирована ли в документах организации, согласована ли со службой ИБ либо лицом, отвечающим за обеспечение ИБ, и выполняется ли процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ неплатежной информации?	обязательный							0,0889	
М8.13	Регламентирована ли в документах организации, согласована ли со службой ИБ либо лицом, отвечающим за обеспечение ИБ, и выполняется ли процедура восстановления всех реализованных программно-техническими средствами и организационными мерами функций по обеспечению ИБ неплатежной информации?	обязательный							0,0814	
Итоговая оценка группового показателя М8										

Групповой показатель М9 "Организация и функционирование службы ИБ организации БС РФ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М9.1	Сформирована ли руководством служба ИБ (назначено ли уполномоченное лицо) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный							0,0816	
М9.2	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный							0,0753	
М9.3	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный							0,0750	
М9.4	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый	//// ////	///// /////	///// /////	///// /////			0,0530	
М9.5	Сформированы ли для организаций, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0615	
М9.6	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации?	обязательный							0,0694	

М9.7	Наделена ли служба ИБ (уполномоченное лицо) полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации?	обязательный							0,0725	
М9.8	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0725	
М9.9	Наделена ли служба ИБ (уполномоченное лицо) полномочиями определять требования к мерам обеспечения ИБ организации?	обязательный							0,0781	
М9.10	Наделена ли служба ИБ (уполномоченное лицо) полномочиями контролировать работников организации в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам?	обязательный							0,0725	

М9.11	Наделена ли служба ИБ (уполномоченное лицо) полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный							0,0725	
М9.12	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации)?	обязательный							0,0787	
М9.13	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?	обязательный							0,0587	
М9.14	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации?	обязательный							0,0787	
Итоговая оценка группового показателя М9										

Групповой показатель М10 "Определение/коррекция области действия СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М10.1	Определена ли в документах организации и корректируется ли опись структурированных по классам защищаемых информационных активов (типов информационных активов - типов информации)?	обязательный							0,1956	
М10.2	Проводится ли классификация информационных активов по типам на основании оценок ценности информационных активов для интересов (целей) организации, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов?	рекомендуемый	//// //// //// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// /////			0,1614	
М10.3	Содержит ли опись информационных активов информацию о принадлежности конкретного информационного актива к выделенным типам информационных активов (в случае наличия в организации классификации информационных активов)?	обязательный							0,1352	

М10.4	Содержит ли опись информационных активов (типов информационных активов) перечень их объектов среды, покрывающий все уровни информационной инфраструктуры организации, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный							0,1098	
М10.5	Определены ли в документах организации процедуры анализа и пересмотра области действия СОИБ (в частности, процедуры пересмотра при изменении перечня информационных активов организации или типов информационных активов)?	обязательный							0,1276	
М10.6	Определены ли в документах организации роли по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,1352	
М10.7	Назначены ли в организации ответственные за выполнение ролей по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,1352	
Итоговая оценка группового показателя М10										

Групповой показатель М11 "Выбор/коррекция подхода
к оценке рисков нарушения ИБ и проведению оценки рисков
нарушения ИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М11.1	Принята ли в организации и корректируется ли методика оценки рисков нарушения ИБ/подход к оценке рисков нарушения ИБ?	обязательный							0,1154	
М11.2	Определены ли в организации критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный							0,1070	

М11.3	Определяет ли методика оценки рисков нарушения ИБ/подход к оценке рисков нарушения ИБ организации способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания: - степени возможности реализации угроз ИБ выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированных в моделях угроз и нарушителей, в результате их воздействия на объекты среды информационных активов организации (типов информационных активов); - степени тяжести последствий от потери свойств ИБ, в частности свойств доступности, целостности и конфиденциальности для рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0854	
М11.4	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный							0,0854	
М11.5	Проводится ли оценка рисков нарушения ИБ для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ?	обязательный							0,0676	

M11.6	Создан ли и поддерживается ли в актуальном состоянии единый информационный ресурс (база данных), содержащий информацию об инцидентах ИБ?	рекомендуемый	//// //// //// //// ////	///// ///// ///// ///// /////	///// ///// ///// ///// /////	///// ///// ///// ///// /////			0,0688	
M11.7	Соотносятся ли величины рисков, полученные в результате оценивания рисков нарушения ИБ, с уровнем допустимого риска, принятого в организации?	обязательный							0,0766	
M11.8	Определен ли в документах организации перечень недопустимых рисков нарушения ИБ, сформированный на основе сравнения полученных в результате оценивания рисков нарушения ИБ величин рисков с уровнем допустимого риска, принятого в организации?	обязательный							0,0766	
M11.9	Определены ли в документах организации роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ/ подхода к оценке риска нарушения ИБ?	обязательный							0,0782	
M11.10	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ/ подхода к оценке риска нарушения ИБ?	обязательный							0,0782	

М11.11	Определены ли в документах организации роли по оценке рисков нарушения ИБ?	обязательный							0,0782	
М11.12	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный							0,0826	
Итоговая оценка группового показателя М11										

Групповой показатель М12 "Разработка планов обработки рисков нарушения ИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М12.1	Определен ли в документах организации по каждому из недопустимых рисков нарушения ИБ план, определяющий один из возможных способов обработки риска: - перенос риска на сторонние организации (например, путем страхования указанного риска); - уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска); - осознанное принятие риска; - формирование требований ИБ, снижающих риск до допустимого уровня, и формирование планов по их реализации?	обязательный							0,1814	
М12.2	Согласованы ли планы обработки рисков нарушения ИБ с руководителем службы ИБ либо лицом, отвечающим в организации за обеспечение ИБ?	обязательный							0,1814	
М12.3	Утверждены ли руководством организации планы обработки рисков нарушения ИБ?	обязательный							0,1814	
М12.4	Содержат ли планы реализации требований ИБ последовательность и сроки реализации и внедрения организационных, технических и иных защитных мер?	обязательный							0,1702	

М12.5	Определены ли в документах организации роли по разработке планов обработки рисков нарушения ИБ?	обязательный							0,1428	
М12.6	Назначены ли ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный							0,1428	
Итоговая оценка группового показателя М12										

Групповой показатель М13 "Определение/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М13.1	Проводится ли разработка и коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ в организации, с учетом рекомендаций по стандартизации Банка России РС БР ИББС-2.0 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0"?	рекомендуемый	//// //// //// //// //// //// //// //// //// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// /////			0,0406	
М13.2	Разработана ли политика ИБ организации? Утверждена ли политика ИБ руководством?	обязательный							0,0628	
М13.3	Корректируется ли политика ИБ организации?	обязательный							0,0557	
М13.4	Разработаны ли частные политики ИБ организации?	обязательный							0,0580	
М13.5	Корректируются ли частные политики ИБ организации?	обязательный							0,0557	
М13.6	Разработаны ли в организации документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ?	обязательный							0,0510	

M13.7	Корректируются ли в организации документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ?	обязательный							0,0489	
M13.8	Определены ли в организации перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ?	обязательный							0,0407	

M13.9	Определены ли в политике ИБ (частных политиках ИБ) организации: - цели и задачи обеспечения ИБ; - основные области обеспечения ИБ; - типы основных защищаемых информационных активов; - модели угроз и нарушителей; - совокупность правил, требований и руководящих принципов в области ИБ; - основные требования к обеспечению ИБ; - принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; - основные принципы повышения уровня осознания и осведомленности в области ИБ; - принципы реализации и контроля выполнения требований политики ИБ?	обязательный							0,0510	

M13.10	Корректируются ли в политике ИБ (частных политиках ИБ) организации: - цели и задачи обеспечения ИБ; - основные области обеспечения ИБ; - типы основных защищаемых информационных активов; - модели угроз и нарушителей; - совокупность правил, требований и руководящих принципов в области ИБ; - основные требования к обеспечению ИБ; - принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; - основные принципы повышения уровня осознания и осведомленности в области ИБ; - принципы реализации и контроля выполнения требований политики ИБ?	обязательный							0,0486	

M13.11	Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: - законодательства Российской Федерации; - комплекса БР ИББС, в частности требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; - нормативных актов и предписаний регулирующих и надзорных органов; - договорных требований организации со сторонними организациями; - результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0519	

М13.12	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: - законодательства Российской Федерации; - комплекса БР ИББС, в частности требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; - нормативных актов и предписаний регулирующих и надзорных органов; - договорных требований организации со сторонними организациями; - результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0510	
М13.13	Содержит ли совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, требования по обеспечению ИБ всех выявленных информационных активов (типов информационных активов), находящихся в области действия СОИБ организации?	обязательный							0,0501	

М13.14	Не противоречат ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положениям политики ИБ и частных политик ИБ?	обязательный							0,0510	
М13.15	Детализируют ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положения политики ИБ и частных политик ИБ?	обязательный							0,0426	
М13.16	Утвержден ли руководством организации порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации (в случае наличия в структурных подразделениях организации работников, ответственных за обеспечение ИБ)?	обязательный							0,0354	
М13.17	Определены ли в составе документов, регламентирующих деятельность в области обеспечения ИБ, перечень свидетельств выполнения указанной деятельности и ответственность работников организации за выполнение этой деятельности?	обязательный							0,0426	

M13.18	Определены ли в документах организации процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный							0,0443	
M13.19	Определен ли в документах организации порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0406	
M13.20	Определены ли в документах организации роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0382	
M13.21	Назначены ли ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0393	
Итоговая оценка группового показателя M13										

Групповой показатель M14 "Принятие руководством организации БС РФ решений о реализации и эксплуатации СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М14.1	Оформлены ли документально и утверждены ли руководством решения о реализации и эксплуатации СОИБ, в частности решения: - об анализе и принятии остаточных рисков нарушения ИБ; - о планировании этапов внедрения СОИБ, в частности требований ИБ, изложенных в 7-м и 8-м разделах СТО БР ИББС-1.0; - о распределении ролей в области обеспечения ИБ организации; - о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований 7-го и 8-го разделов СТО БР ИББС-1.0 и снижение рисков ИБ; - о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ?	обязательный							0,2752	

М14.2	Утверждены ли руководством все планы внедрения СОИБ, в частности планы реализаций требований 7-го и 8-го разделов СТО БР ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых документально зафиксированы: - последовательность выполнения мероприятий в рамках указанных планов; - сроки начала и окончания запланированных мероприятий; - должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия?	обязательный							0,2812	
М14.3	Определен ли документально порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации?	обязательный							0,2096	
М14.4	Оформлены ли документально решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,2340	
Итоговая оценка группового показателя М14										

Групповой показатель М15 "Организация реализации планов

внедрения СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
M15.1	Определены ли в документах организации и выполняются ли проектирование/приобретение/ развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер (СИБ), предусмотренных планами реализации требований ИБ?	обязательный							0,2540	
M15.2	Реализуются ли при построении элементов СИБ (применительно к конкретной области или сфере деятельности организации) защитные меры, применяемые к объектам среды, в соответствии с существующими в организации требованиями обеспечения ИБ, сформулированными в политике ИБ и других внутренних документах организации?	обязательный							0,2688	
M15.3	Определены ли в документах организации роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный							0,2412	

M15.4	Назначены ли ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный							0,2360	
Итоговая оценка группового показателя M15										

Групповой показатель M16 "Разработка
и организация реализации программ по обучению и повышению
осведомленности в области ИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
M16.1	Организована ли документально оформленная работа с персоналом организации в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов? Утверждена ли руководством указанная работа?	обязательный							0,1898	
M16.2	Установлены ли в планах обучения и повышения осведомленности требования к периодичности обучения и повышения осведомленности?	обязательный							0,1378	

M16.3	Включена ли в программы обучения и повышения осведомленности информация: - по существующим политикам ИБ; - по применяемым в организации защитным мерам; - по правильному использованию защитных мер в соответствии с внутренними документами организации; - о значимости и важности деятельности работников для обеспечения ИБ организации?	обязательный							0,1536	
M16.4	Определен ли в организации перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ, в частности: - документы (журналы), подтверждающие прохождение руководителями и работниками организации обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых; - документы, содержащие результаты проверок обучения работников организации; - документы, содержащие результаты проверок осведомленности в области ИБ в организации?	обязательный							0,1164	

М16.5	Организуется ли для работника, получившего новую роль, обучение или инструктаж в области ИБ, соответствующий полученной роли?	обязательный							0,1396	
М16.6	Определены ли в документах организации роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1290	
М16.7	Назначены ли ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1338	
Итоговая оценка группового показателя М16										

Групповой показатель М17 "Организация обнаружения и реагирования на инциденты безопасности"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М17.1	Существуют ли в организации документы, регламентирующие процедуры обработки инцидентов, включающие: - процедуры обнаружения инцидентов ИБ; - процедуры информирования об инцидентах; - процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ; - процедуры реагирования на инцидент; - процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости - с участием внешних экспертов в области ИБ)?	обязательный							0,1372	
М17.2	Сформирована и поддерживается ли в актуальном состоянии централизованная база инцидентов ИБ?	рекомендуемый	//// //// //// ////	///// ///// ///// /////	///// ///// ///// /////	///// ///// ///// /////			0,1152	
М17.3	Определены ли в документах организации процедуры по хранению информации: - об инцидентах ИБ; - о практиках анализа инцидентов ИБ; - о результатах реагирования на инциденты ИБ?	обязательный							0,1152	

М17.4	Определены ли в документах организации порядок действий работников организации при обнаружении нетипичных событий, связанных с ИБ, и порядок информирования о данных событиях?	обязательный							0,1124	
М17.5	Осведомлены ли работники организации о порядке действий при обнаружении нетипичных событий, связанных с ИБ, и порядке информирования о данных событиях?	обязательный							0,1124	
М17.6	Учитывают ли процедуры расследования инцидентов действующее законодательство Российской Федерации, положения нормативных актов Банка России, а также внутренних документов организации в области ИБ?	обязательный							0,0948	
М17.7	Принимаются и выполняются ли в организации документально оформленные решения по всем выявленным инцидентам ИБ?	обязательный							0,1076	
М17.8	Определены ли в документах организации роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1026	
М17.9	Назначены ли ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1026	

Итоговая оценка группового показателя М17	

Групповой показатель М18 "Организация
обеспечения непрерывности бизнеса и его восстановления
после прерываний"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М18.1	Выделены ли в описи защищаемых информационных активов организации активы, существенные для обеспечения непрерывности бизнеса организации?	обязательный							0,0876	
М18.2	Определены ли документально в организации требования обеспечения ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0888	

M18.3	Определен ли в документах организации план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации, в состав которого включены: - условия активизации плана; - порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персонала); - процедуры восстановления; - процедуры тестирования и проверки плана; - план обучения и повышения осведомленности работников организации; - обязанности работников организации с указанием ответственных за выполнение каждого из положений плана?	обязательный							0,0907	

M18.4	Основывается ли разработка планов обеспечения непрерывности бизнеса и его восстановления после прерываний на документально оформленных результатах оценки рисков нарушения ИБ организации применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0673	
M18.5	Определены ли документально, реализованы и эксплуатируются ли защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0801	
M18.6	Основываются ли реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания на соответствующих требованиях обеспечения ИБ?	обязательный							0,0758	
M18.7	Согласован ли план обеспечения непрерывности бизнеса и его восстановления после прерываний с существующими в организации процедурами обработки инцидентов ИБ?	обязательный							0,0593	

M18.8	Определено ли в документах организации и выполняется ли периодическое тестирование плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0550	
M18.9	Составлен ли сценарий тестирования плана обеспечения непрерывности бизнеса и его восстановления после прерывания с учетом существующей в организации модели угроз и нарушителей, а также результатов оценки рисков?	обязательный							0,0587	
M18.10	Проводится ли при необходимости корректировка плана обеспечения непрерывности бизнеса и его восстановления после прерывания по результатам тестирования?	обязательный							0,0699	
M18.11	Реализована ли в организации программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний?	обязательный							0,0593	

M18.12	Определены ли в документах организации и выполняются ли процедуры регулярного пересмотра и обновления плана обеспечения непрерывности бизнеса и его восстановления после прерывания (для обеспечения уверенности в их эффективности), учитывающие изменения в приоритетах, целях и интересах бизнеса организации; пересмотр моделей угроз; оценку рисков нарушения ИБ?	обязательный							0,0717	
M18.13	Определены ли в документах организации роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0679	
M18.14	Назначены ли ответственные за выполнение ролей по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,0679	
Итоговая оценка группового показателя M18										

Групповой показатель M19 "Мониторинг и контроль защитных мер"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

M19.1	Определены ли в документах организации процедуры мониторинга СОИБ и контроля защитных мер, которые охватывают все реализованные и эксплуатируемые защитные меры, входящие в СИБ, проводятся персоналом организации, ответственным за обеспечение ИБ?	обязательный							0,1482	
M19.2	Фиксируются ли документально результаты выполнения процедур мониторинга СОИБ и контроля защитных мер?	обязательный							0,1352	
M19.3	Определены ли в документах организации и выполняются ли процедуры сбора и хранения информации о действиях работников организации, событиях и параметрах, имеющих отношение к функционированию защитных мер?	обязательный							0,1068	
M19.4	Включается ли в базу данных инцидентов информация обо всех инцидентах ИБ, выявленных в процессе мониторинга СОИБ и контроля защитных мер?	обязательный							0,1352	

M19.5	Подвергаются ли процедуры мониторинга СОИБ и контроля защитных мер регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ?	обязательный							0,1312	
M19.6	Определен ли в документах организации порядок пересмотра процедур мониторинга СОИБ и контроля защитных мер?	обязательный							0,1066	
M19.7	Определены ли в документах организации роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,1184	
M19.8	Назначены ли ответственные за выполнение ролей, связанных с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,1184	
Итоговая оценка группового показателя M19										

Групповой показатель M20 "Проведение самооценки ИБ"

Обозначение	Частный показатель ИБ	Обязательность	Оценка частного показателя ИБ	Коэффициент	Выч

частного показателя ИБ		выполнения	0	0,25	0,5	0,75	1	н/о	значимости частного показателя ИБ	знач пок ИБ
M20.1	Проводится ли самооценка ИБ в соответствии с настоящим стандартом?	обязательный							0,1340	
M20.2	Организован ли порядок проведения самооценки ИБ в соответствии с рекомендациями по стандартизации Банка России РС БР ИББС-2.1 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0"?	рекомендуемый	//// //// //// //// //// //// //// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// ///// /////			0,1118	
M20.3	Определена ли в документах организации и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный							0,1026	

М20.4	Определены ли в документах организации: - порядок формирования, сбора и хранения свидетельств самооценки ИБ; - периодичность проведения самооценки ИБ; - порядок хранения и использования результатов самооценки ИБ?	обязательный							0,1098	
М20.5	Оформлен ли в документах организации для каждой проводимой в организации самооценки ИБ план ее проведения, определяющий: - цель самооценки ИБ; - объекты и деятельность, подвергающиеся самооценке ИБ; - порядок и сроки выполнения мероприятий самооценки ИБ; - распределение ролей среди работников организации, связанных с проведением самооценки ИБ?	обязательный							0,0978	
М20.6	Подготавливаются ли по результатам самооценок ИБ отчеты?	обязательный							0,1150	
М20.7	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации?	обязательный							0,1262	
М20.8	Определены ли в документах организации роли, связанные с выполнением программы самооценок ИБ?	обязательный							0,1014	

М20.9	Назначены ли ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный							0,1014	
Итоговая оценка группового показателя М20										

Групповой показатель М21 "Проведение аудита ИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М21.1	Проводится ли аудит ИБ организации в соответствии с требованиями стандарта Банка России СТО БР ИББС-1.1 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности" и настоящего стандарта?	обязательный							0,1192	

M21.2	Определена ли в документах организации и реализуется ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки?	обязательный							0,0974	
M21.3	Оформлен ли в документах организации для каждого проводимого в организации аудита ИБ план аудита, определяющий: - цель аудита ИБ; - критерии аудита ИБ; - область аудита ИБ; - дату и продолжительность проведения аудита ИБ; - состав аудиторской группы; - описание деятельности и мероприятий по проведению аудита ИБ; - распределение ресурсов при проведении аудита ИБ?	обязательный							0,1112	

М21.4	Оформлены ли договоры с аудиторскими организациями и определены ли в соответствующих документах: - порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ; - порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ; - порядок взаимодействия аудиторской группы и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству; - порядок организации опроса работников; - порядок организации наблюдения за деятельностью работников организации со стороны представителей аудиторской организации?	обязательный							0,1246	
М21.5	Подготавливаются ли по результатам аудитов ИБ отчеты?	обязательный							0,1186	
М21.6	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации?	обязательный							0,1312	

М21.7	Определен ли в документах организации порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности отчетов аудитов?	обязательный							0,0886	
М21.8	Определены ли в документах организации роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный							0,1046	
М21.9	Назначены ли ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный							0,1046	
Итоговая оценка группового показателя М21										

Групповой показатель М22 "Анализ функционирования СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

М22.1	Проводится ли в организации анализ функционирования СОИБ, использующий в том числе: - результаты мониторинга СОИБ и контроля защитных мер; - сведения об инцидентах ИБ; - результаты проведения аудитов ИБ, самооценок ИБ; - данные об угрозах, возможных нарушителях и уязвимостях ИБ; - данные об изменениях внутри организации, например данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации; - данные об изменениях вне организации, например данные об изменениях в законодательстве Российской Федерации, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах организации?	обязательный							0,1274	
М22.2	Проводится ли анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации, требованиям законодательства РФ, требованиям стандартов Банка России, контрактным требованиям организации?	обязательный							0,1058	

M22.3	Проводится ли анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в организации, требованиям политик ИБ организации?	обязательный							0,1002	
M22.4	Проводится ли оценка рисков в области ИБ организации, включая оценку уровня остаточного и допустимого рисков?	обязательный							0,0946	
M22.5	Проводится ли проверка адекватности модели угроз организации существующим угрозам ИБ?	обязательный							0,0946	
M22.6	Проводится ли оценка адекватности используемых защитных мер требованиям внутренних документов организации и результатам оценки рисков?	обязательный							0,0930	
M22.7	Проводится ли анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер?	обязательный							0,0822	
M22.8	Документируются ли результаты анализа функционирования СОИБ?	обязательный							0,1026	
M22.9	Определены ли в документах организации роли, связанные с процедурами анализа функционирования СОИБ?	обязательный							0,0998	

М22.10	Назначены ли ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный							0,0998	
Итоговая оценка группового показателя М22										

Групповой показатель М23 "Анализ СОИБ со стороны руководства организации БС РФ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М23.1	Утвержден ли в организации перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный							0,1376	
М23.2	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: - мониторинга СОИБ и контроля защитных мер; - анализа функционирования СОИБ; - аудитов ИБ; - самооценок ИБ?	обязательный							0,1464	

M23.3	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию: - о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; - о новых выявленных уязвимостях и угрозах ИБ; - о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством; - об изменениях, которые могли бы повлиять на организацию СОИБ, например изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России; - о выявленных инцидентах ИБ?	обязательный							0,1318	
M23.4	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например выполнение планов обработки рисков?	обязательный							0,1154	

M23.5	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1228	
M23.6	Определен ли в организации и утвержден ли руководством план выполнения деятельности по контролю и анализу СОИБ, содержащий, в частности, положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации?	обязательный							0,1104	
M23.7	Определены ли в документах организации роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
M23.8	Назначены ли ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
Итоговая оценка группового показателя M23										

Групповой показатель M24 "Принятие решений по тактическим улучшениям СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М24.1	Рассматриваются ли при принятии решений, связанных с тактическими улучшениями СОИБ, документально оформленные результаты: - аудитов ИБ; - самооценок ИБ; - мониторинга СОИБ и контроля защитных мер; - анализа функционирования СОИБ; - обработки инцидентов ИБ; - выявления новых угроз и уязвимостей ИБ; - оценки рисков; - анализа перечня защитных мер, возможных для применения; - стратегических улучшений СОИБ; - анализа СОИБ со стороны руководства; - анализа успешных практик в области ИБ (собственных или других организаций)?	обязательный							0,1354	

M24.2	Оформляются ли документально решения по тактическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо направления тактических улучшений СОИБ?	обязательный							0,1354	
M24.3	Формируются ли направления тактических улучшений СОИБ в виде корректирующих и превентивных действий?	обязательный							0,1216	
M24.4	Определены ли в документах организации планы реализации тактических улучшений СОИБ?	обязательный							0,1354	
M24.5	Существуют ли в организации документы, в которых фиксируются результаты выполнения планов реализации тактических улучшений СОИБ?	обязательный							0,1272	
M24.6	Санкционирует и контролирует ли руководство службы ИБ организации деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный							0,1300	

M24.7	Определены ли в документах организации и выполняются ли процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ? Фиксируются ли результаты выполнения указанных процедур?	обязательный							0,0934	
M24.8	Назначаются ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный							0,1216	
Итоговая оценка группового показателя M24										

Групповой показатель M25 "Принятие решений
по стратегическим улучшениям СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		

M25.1	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, документально оформленные результаты: - аудитов ИБ; - самооценок ИБ; - мониторинга СОИБ и контроля защитных мер; - анализа функционирования СОИБ; - обработки инцидентов ИБ; - выявления новых информационных активов организации или их типов; - выявления новых угроз и уязвимостей ИБ; - оценки рисков; - пересмотра основных рисков ИБ; - анализа СОИБ со стороны руководства; - анализа успешных практик в области ИБ (собственных или других организаций)?	обязательный							0,1130	
M25.2	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, изменения интересов, целей и задач бизнеса организации, контрактных обязательств организации, а также изменения в законодательстве РФ и нормативных актах Банка России?	обязательный							0,1058	

M25.3	Оформляются ли документально решения по стратегическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо направления стратегических улучшений СОИБ?	обязательный							0,0984	
M25.4	Формируются ли направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например: - уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ (частных политик ИБ) организации; - изменения в области действия СОИБ; - уточнение описи типов информационных активов; - пересмотр моделей угроз и нарушителей; - изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ?	обязательный							0,0984	
M25.5	Определены ли в документах организации планы реализации стратегических улучшений СОИБ?	обязательный							0,1016	
M25.6	Существуют ли в организации документы, в которых фиксируются результаты выполнения планов реализации стратегических улучшений СОИБ?	обязательный							0,0962	

M25.7	Санкционирует и контролирует ли руководство организации деятельность, связанную с реализацией стратегических улучшений СОИБ?	обязательный							0,1108	
M25.8	В случае стратегических улучшений СОИБ выполняется ли деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых защитных мер и соответствующих внутренних документов, в частности, выполняются ли: - выработка планов тактических улучшений СОИБ; - уточнение планов обработки рисков; - уточнение программы внедрения защитных мер; - уточнение процедур использования защитных мер?	обязательный							0,1058	

М25.9	Определены ли в документах организации и выполняются ли процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ? Фиксируются ли документально результаты выполнения указанных процедур?	обязательный							0,0822	
М25.10	Назначаются ли ответственные за реализацию решений по стратегическим улучшениям СОИБ?	обязательный							0,0878	
Итоговая оценка группового показателя М25										

Групповой показатель М26 "Оценка деятельности руководства организации БС РФ по поддержке функционирования службы ИБ организации БС РФ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М26.1 (аналог М9.1)	Сформирована ли руководством служба ИБ (назначено ли уполномоченное лицо) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный							0,0816	

M26.2 (аналог M9.2)	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный							0,0753	
M26.3 (аналог M9.3)	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный							0,0750	
M26.4 (аналог M9.4)	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый	//// ////	///// /////	///// /////	///// /////			0,0530	
M26.5 (аналог M9.5)	Сформированы ли для организаций, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	рекомендуемый	//// //// //// //// //// //// ////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////	///// ///// ///// ///// ///// ///// /////			0,0615	
M26.6 (аналог M9.6)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации?	обязательный							0,0694	
M26.7 (аналог M9.7)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации?	обязательный							0,0725	

M26.8 (аналог M9.8)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0725	
M26.9 (аналог M9.9)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями определять требования к мерам обеспечения ИБ организации?	обязательный							0,0781	
M26.10 (аналог M9.10)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями контролировать работников организации в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам?	обязательный							0,0725	
M26.11 (аналог M9.11)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный							0,0725	

М26.12 (аналог М9.12)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации)?	обязательный							0,0787	
М26.13 (аналог М9.13)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?	обязательный							0,0587	
М26.14 (аналог М9.14)	Наделена ли служба ИБ (уполномоченное лицо) полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации?	обязательный							0,0787	
Итоговая оценка группового показателя М26										

Групповой показатель М27 "Оценка деятельности руководства организации БС РФ по принятию решений о реализации и эксплуатации СОИБ"

Обозначение	Частный показатель ИБ	Обязательность	Оценка частного показателя ИБ	Коэффициент	Выч

частного показателя ИБ		выполнения	0	0,25	0,5	0,75	1	н/о	значимости частного показателя ИБ	знач пок ИБ
M27.1 (аналог M14.1)	Оформлены ли документально и утверждены ли руководством решения о реализации и эксплуатации СОИБ, в частности решения: - об анализе и принятии остаточных рисков нарушения ИБ; - о планировании этапов внедрения СОИБ, в частности требований ИБ, изложенных в 7-м и 8-м разделах СТО БР ИББС-1.0; - о распределении ролей в области обеспечения ИБ организации; - о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований 7-го и 8-го разделов СТО БР ИББС-1.0 и снижение рисков ИБ; - о выделении ресурсов, необходимых для реализации и эксплуатации функционирования СОИБ?	обязательный							0,2752	

М27.2 (аналог М14.2)	Утверждены ли руководством все планы внедрения СОИБ, в частности планы реализаций требований 7-го и 8-го разделов СТО БР ИББС-1.0, планы обработки рисков нарушения ИБ и внедрения защитных мер, в которых документально зафиксированы: - последовательность выполнения мероприятий в рамках указанных планов; - сроки начала и окончания запланированных мероприятий; - должностные лица (подразделения), ответственные за выполнение каждого указанного мероприятия?	обязательный							0,2812	
М27.3 (аналог М14.3)	Определен ли документально порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации?	обязательный							0,2096	
М27.4 аналог М14.4)	Оформлены ли документально решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,2340	
Итоговая оценка группового показателя М27										

Групповой показатель М28 "Оценка деятельности руководства

организации БС РФ по поддержке планирования СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М28.1 (аналог М10.1)	Определена ли в документах организации и корректируется ли опись структурированных по классам защищаемых информационных активов (типов информационных активов - типов информации)?	обязательный							0,0386	
М28.2 (аналог М10.6)	Определены ли в документах организации роли по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,0364	
М28.3 (аналог М10.7)	Назначены ли в организации ответственные за выполнение ролей по определению/коррекции области действия СОИБ и по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ?	обязательный							0,0364	
М28.4 (аналог М11.1)	Принята ли в организации и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный							0,0386	

M28.5 (аналог M11.2)	Определены ли в организации критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный							0,0386	
M28.6 (аналог M11.4)	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный							0,0345	
M28.7 (аналог M11.9)	Определены ли в документах организации роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный							0,0364	
M28.8 (аналог M11.10)	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный							0,0364	
M28.9 (аналог M11.11)	Определены ли в документах организации роли по оценке рисков нарушения ИБ?	обязательный							0,0345	
M28.10 (аналог M11.12)	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный							0,0345	
M28.11 (аналог M12.3)	Утверждены ли руководством организации планы обработки рисков нарушения ИБ?	обязательный							0,0364	

M28.12 (аналог M12.5)	Определены ли в документах организации роли по разработке планов обработки рисков нарушения ИБ?	обязательный							0,0345	
M28.13 (аналог M12.6)	Назначены ли ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный							0,0364	
M28.14 (аналог M13.2)	Разработана ли политика ИБ организации? Утверждена ли политика ИБ руководством?	обязательный							0,0408	
M28.15 (аналог M13.3)	Корректируется ли политика ИБ организации?	обязательный							0,0386	
M28.16 (аналог M13.4)	Разработаны ли частные политики ИБ организации?	обязательный							0,0408	
M28.17 (аналог M13.5)	Корректируются ли частные политики ИБ организации?	обязательный							0,0364	

М28.18 (аналог М13.9)	Определены ли в политике ИБ (частных политиках ИБ) организации: - цели и задачи обеспечения ИБ; - основные области обеспечения ИБ; - типы основных защищаемых информационных активов; - модели угроз и нарушителей; - совокупность правил, требований и руководящих принципов в области ИБ; - основные требования к обеспечению ИБ; - принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; - основные принципы повышения уровня осознания и осведомленности в области ИБ; - принципы реализации и контроля выполнения требований политики ИБ?	обязательный							0,0386	

М28.19 (аналог М13.10)	Корректируются ли в политике ИБ (частных политиках ИБ) организации: - цели и задачи обеспечения ИБ; - основные области обеспечения ИБ; - типы основных защищаемых информационных активов; - модели угроз и нарушителей; - совокупность правил, требований и руководящих принципов в области ИБ; - основные требования к обеспечению ИБ; - принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов; - основные принципы повышения уровня осознания и осведомленности в области ИБ; - принципы реализации и контроля выполнения требований политики ИБ?	обязательный							0,0364	

М28.20 (аналог М13.11)	Разрабатываются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: - законодательства Российской Федерации; - комплекса БР ИББС, в частности требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; - нормативных актов и предписаний регулирующих и надзорных органов; - договорных требований организации со сторонними организациями; - результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0408	

М28.21 (аналог М13.12)	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: - законодательства Российской Федерации; - комплекса БР ИББС, в частности требования 7-го и 8-го разделов стандарта СТО БР ИББС-1.0; - нормативных актов и предписаний регулирующих и надзорных органов; - договорных требований организации со сторонними организациями; - результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов)?	обязательный							0,0386	
М28.22 (аналог М13.16)	Утвержден ли руководством организации порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации (в случае наличия в структурных подразделениях организации работников, ответственных за обеспечение ИБ)?	обязательный							0,0345	

M28.23 (аналог M13.18)	Определены ли в документах организации процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный							0,0345	
M28.24 (аналог M13.20)	Определены ли в документах организации роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0386	
M28.25 (аналог M13.21)	Назначены ли ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации?	обязательный							0,0364	
M28.26 (аналог M15.3)	Определены ли в документах организации роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный							0,0364	
M28.27 (аналог M15.4)	Назначены ли ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный							0,0364	
Итоговая оценка группового показателя M28										

Групповой показатель M29 "Оценка деятельности руководства организации БС РФ по поддержке реализации СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М29.1 (аналог М16.1)	Организована ли документально оформленная работа с персоналом организации в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов? Утверждена ли руководством указанная работа?	обязательный							0,1442	
М29.2 (аналог М16.6)	Определены ли в документах организации роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1024	
М29.3 (аналог М16.7)	Назначены ли ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный							0,1024	
М29.4 (аналог М17.8)	Определены ли в документах организации роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1404	

М29.5 (аналог М17.9)	Назначены ли ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный							0,1268	
М29.6 (аналог М18.3)	Определен ли в документах организации план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации, в состав которого включены: - условия активизации плана; - порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персонала); - процедуры восстановления; - процедуры тестирования и проверки плана; - план обучения и повышения осведомленности работников организации; - обязанности работников организации с указанием ответственных за выполнение каждого из положений плана?	обязательный							0,1442	
М29.7 (аналог М18.13)	Определены ли в документах организации роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1198	

М29.8 (аналог М18.14)	Назначены ли ответственные за выполнение ролей по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1198	
Итоговая оценка группового показателя М29										

Групповой показатель М30 "Оценка деятельности руководства организации БС РФ по поддержке проверки СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М30.1 (аналог М19.7)	Определены ли в документах организации роли, связанные с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,0921	
М30.2 (аналог М19.8)	Назначены ли ответственные за выполнение ролей, связанных с выполнением процедур мониторинга СОИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный							0,0921	

М30.3 (аналог М20.3)	Определена ли в документах организации и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный							0,0848	
М30.4 (аналог М20.7)	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации?	обязательный							0,0943	
М30.5 (аналог М20.8)	Определены ли в документах организации роли, связанные с выполнением программы самооценок ИБ?	обязательный							0,0734	
М30.6 (аналог М20.9)	Назначены ли ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный							0,0734	

М30.7 (аналог М21.2)	Определена ли в документах организации и реализована ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки?	обязательный							0,0808	
М30.8 (аналог М21.6)	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации?	обязательный							0,0969	
М30.9 (аналог М21.8)	Определены ли в документах организации роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный							0,0805	
М30.10 (аналог М21.9)	Назначены ли ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный							0,0805	
М30.11 (аналог М22.9)	Определены ли в документах организации роли, связанные с процедурами анализа функционирования СОИБ?	обязательный							0,0756	
М30.12 (аналог М22.10)	Назначены ли ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный							0,0756	

Итоговая оценка группового показателя М30	

Групповой показатель М31 "Оценка деятельности руководства организации БС РФ по анализу СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М31.1 (аналог М23.1)	Утвержден ли в организации перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный							0,1376	
М31.2 (аналог М23.2)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: - мониторинга СОИБ и контроля защитных мер; - анализа функционирования СОИБ; - аудитов ИБ; - самооценок ИБ?	обязательный							0,1464	

М31.3 (аналог М23.3)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию: - о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; - о новых выявленных уязвимостях и угрозах ИБ; - о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством; - об изменениях, которые могли бы повлиять на организацию СОИБ, например изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России; - о выявленных инцидентах ИБ?	обязательный							0,1318	
М31.4 (аналог М23.4)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например выполнение планов обработки рисков?	обязательный							0,1154	

М31.5 (аналог М23.5)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания?	обязательный							0,1228	
М31.6 (аналог М23.6)	Определен ли в организации и утвержден ли руководством план выполнения деятельности по контролю и анализу СОИБ, содержащий, в частности, положения по проведению совещаний на уровне руководства, на которых в том числе производятся поиск и анализ проблем ИБ, влияющих на бизнес организации?	обязательный							0,1104	
М31.7 (аналог М23.7)	Определены ли в документах организации роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
М31.8 (аналог М23.8)	Назначены ли ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный							0,1178	
Итоговая оценка группового показателя М31										

Групповой показатель М32 "Оценка деятельности руководства по поддержке совершенствования СОИБ"

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Выч знач пок ИБ
			0	0,25	0,5	0,75	1	н/о		
М32.1 (аналог М24.6)	Санкционирует и контролирует ли руководство службы ИБ организации деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный							0,2560	
М32.2 (аналог М24.8)	Назначаются ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный							0,2248	
М32.3 (аналог М25.7)	Санкционирует и контролирует ли руководство организации деятельность, связанную с реализацией стратегических улучшений СОИБ?	обязательный							0,2816	
М32.4 (аналог М25.10)	Назначаются ли ответственные за реализацию решений по стратегическим улучшениям СОИБ?	обязательный							0,2376	
Итоговая оценка группового показателя М32										

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)

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.