СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2007

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-2006

Дата введения: 2007-05-01

Москва
2007

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 28 апреля 2007 года № Р-346.

2. ВВЕДЕН ВПЕРВЫЕ.

Содержание

Введение

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

Настоящий стандарт устанавливает способы определения степени выполнения требований СТО БР ИББС-1.0, а также итогового уровня соответствия ИБ требованиям СТО БР ИББС-1.0 при проведении внутренней и(или) внешней оценки и самооценки ИБ.

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0-2006

Дата введения: 2007-05-01

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 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.

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

2. Нормативные ссылки

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

3. Термины и определения

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

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

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

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

4. Обозначения и сокращения

АБС — автоматизированная банковская система;
БС — банковская система;
ЖЦ — жизненный цикл;
ИБ — информационная безопасность;
ЛВС — локальная вычислительная сеть;
НСД — несанкционированный доступ;
РФ — Российская Федерация;

СКЗИ — средство криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
ЭВМ — электронная вычислительная машина;
$\alpha_{i.j}$ — коэффициент значимости частного показателя;
*EV*1 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению “текущий уровень ИБ организации”;
*EV*2 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению “менеджмент ИБ организации”;
$EV2_{ПЛ}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих процессы планирования СМИБ;
$EV2_{ПР}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих процессы проверки СМИБ;
$EV2_{Р}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих процессы реализации и эксплуатации СМИБ;
$EV2_{С}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих процессы совершенствования СМИБ;
*EV*3 — 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 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 БС РФ с помощью установления степени выполнения требований, определенных в разделе 8 СТО БР ИББС-1.0;
— определение способа оценивания менеджмента ИБ организации БС РФ с помощью установления степени выполнения требований, определенных в разделе 9 СТО БР ИББС-1.0;
— определение способа оценивания уровня осознания ИБ организации БС РФ с помощью установления степени выполнения принципов, определенных в разделе 6 СТО БР ИББС-1.0;
— определения итогового уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0.

6. Показатели информационной безопасности. Способы оценивания показателей

6.1. Для оценки степени соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ, менеджмента и уровня осознания ИБ. Оценки групповых показателей (EV_{Mi}) используются для получения оценки по направлениям (*EV*1, *EV*2 и *EV*3). Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки ($EV_{Mi.j}$), 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. Все частные показатели должны быть оценены. Оценка $EV_{Mi.j}$ частного показателя формируется на основании выявленной аудиторской группой степени выполнения требований посредством экспертного оценивания. Устанавливается следующая шкала степени выполнения требований:

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

Оценивание частного показателя должно сопровождаться внесением символа, например “X”, в соответствующую графу представленных в приложении А форм. Если частный показатель предназначен для оценки требований, которые не относятся к деятельности организации БС РФ, что документально зафиксировано, то данный частный показатель определяется как неоцениваемый (должна быть заполнена графа “н/о” — нет оценки) и не учитывается в формировании дальнейших результатов оценки. Определение частного показателя как неоцениваемого может быть реализовано путем исключения частного показателя ИБ из числа оцениваемых, при этом необходимо выполнить процедуру перенормировки коэффициентов значимости оставшихся частных показателей ИБ в рамках группового показателя.

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

Таблица 1. Рекомендуемые критерии выставления оценок частных показателей ИБ

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

6.4. 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 БС РФ;
— 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 БС РФ.

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 БС РФ или члена аудиторской группы соответственно.

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

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

При формировании коэффициентов значимости учитывалось следующее условие нормировки:

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

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

Коэффициенты значимости $\alpha_{i.j}$ для каждого частного показателя приведены в приложении А.

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

7.1. Текущий уровень ИБ организации БС РФ определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения требований ИБ СТО БР ИББС-1.0 для следующих областей:

- назначение и распределение ролей, обеспечение доверия к персоналу;
- стадии жизненного цикла автоматизированных банковских систем;
- управление доступом и регистрация;
- антивирусная защита;
- использование ресурсов сети Интернет;
- использование средств криптографической защиты информации;
- банковские платежные технологические процессы;
- банковские информационные технологические процессы.

7.2. Групповые показатели текущего уровня ИБ отражают совокупность требований ИБ к областям, определенным в разделе 8 СТО БР ИББС-1.0. Таблица 2 отражает соответствие между структурными элементами СТО БР ИББС-1.0, содержащими требования ИБ, и групповыми показателями ИБ, предназначенными для проверки реализации данных требований.

Таблица 2. Соответствие групповых показателей ИБ совокупности требований ИБ к областям, определенным в разделе 8 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. 8.2.2
M2	Обеспечение ИБ автоматизированных банковских систем на стадиях жизненного цикла	п. 8.2.3
M3	Обеспечение ИБ при управлении доступом и регистрации	п. 8.2.4
M4	Обеспечение ИБ средствами антивирусной защиты	п. 8.2.5
M5	Обеспечение ИБ при использовании ресурсов сети Интернет	п. 8.2.6
M6	Обеспечение ИБ при использовании средств криптографической защиты информации	п. 8.2.7
M7	Выполнение правил обеспечения ИБ банковских платежных технологических процессов	п. 8.2.8
M8	Выполнение правил обеспечения ИБ банковских информационных технологических процессов	п. 8.2.9

7.3. Частные показатели текущего уровня ИБ отражают отдельные требования ИБ СТО БР ИББС-1.0, предъявляемые по каждой из областей. Частные показатели текущего уровня ИБ (показатели М1 ÷ М8) и метрики приведены в приложении А.

7.4. Оценка частного показателя ИБ ($EV_{Mi.j}$) определяется посредством экспертного оценивания. Для принятия решения следует проводить анализ нормативных, распорядительных, программных и других документов организации БС РФ, имеющих отношение к проверяемым областям ИБ, и уточнять полученную информацию с помощью опросов сотрудников организации БС РФ и наблюдения за деятельностью.

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о невыполнении соответствующих требований ИБ, то оценке $EV_{Mi.j}$ присваивается значение, равное нулю.

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о частичном выполнении соответствующих требований ИБ, то оценка $EV_{Mi.j}$ по решению аудиторской группы может быть установлена равной 0,25; 0,5 или 0,75 (в зависимости от степени выполнения требований ИБ).

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о полном выполнении соответствующих требований ИБ, то оценке $EV_{Mi.j}$ присваивается значение, равное единице.

7.5. Оценка группового показателя (EV_{Mi}) вычисляется из оценок входящих в него частных показателей ($EV_{Mi.j}$) с учетом коэффициентов значимости $\alpha_{i.j}$:

$$EV_{Mi} = \sum_{j} \alpha_{i.j} \cdot EV_{Mi.j},$$

где $j = 1 \div N_i$;

N_i — количество частных показателей ИБ, входящих в групповой показатель M_i;

$i = 1 \div 8$.

Коэффициенты значимости $\alpha_{i.j}$ для каждого частного показателя приведены в приложении А.

7.6. Оценивание частных показателей в рамках групповых показателей М1÷М6 необходимо осуществлять по результатам анализа выполнения соответствующих требований СТО БР ИББС-1.0 применительно к организации БС РФ в целом, включая банковский платежный технологический процесс и банковский информационный технологический процесс.

7.7. 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.

7.8. Итоговая оценка EV1, отражающая текущий уровень ИБ организации БС РФ, определяется по наименьшему значению из оценок уровней ИБ банковского платежного технологического процесса и банковского информационного технологического процесса.

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

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

Оценка уровня ИБ банковского информационного технологического процесса вычисляется по формуле:

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

7.10. 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.

7.11. Оценка *EV*1 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 *EV*2.

8. Оценка процессов системы менеджмента информационной безопасности организации банковской системы Российской Федерации

8.1. Групповые показатели по направлению оценки “менеджмент ИБ организации” оцениваются по стадиям циклической модели менеджмента ИБ. Групповые показатели М9÷М13 предназначены для оценки процессов планирования системы менеджмента ИБ (СМИБ). Групповые показатели М14÷М18 предназначены для оценки процессов реализации СМИБ. Групповые показатели М19÷М23 предназначены для оценки процессов проверки СМИБ. Групповые показатели М24÷М27 предназначены для оценки процессов совершенствования СМИБ.

8.2. Таблица 3 отражает соответствие между структурными элементами СТО БР ИББС-1.0 и групповыми показателями ИБ, предназначенными для оценивания процессов менеджмента ИБ. Наименования групповых показателей соответствуют наименованиям процессов СМИБ организации БС РФ, установленных в СТО БР ИББС-1.0.

Таблица 3. Соответствие групповых показателей ИБ процессам СМИБ, представленным в СТО БР ИББС-1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
Планирование СМИБ		
М9	Определение/уточнение области действия СМИБ и выбор подхода к оценке рисков ИБ	элемент перечисления а) раздела 9.1
М10	Анализ и оценка рисков ИБ, варианты обработки рисков ИБ	элемент перечисления б) раздела 9.1
М11	Определение/уточнение политики ИБ организации БС РФ	элемент перечисления в) раздела 9.1
М12	Выбор/уточнение целей ИБ и защитных мер	элемент перечисления г) раздела 9.1
М13	Принятие руководством организации БС РФ остаточных рисков и решения о реализации и эксплуатации/совершенствовании СМИБ	элемент перечисления д) раздела 9.1, раздел 9.7
Реализация и эксплуатация СМИБ		
М14	Разработка плана обработки рисков ИБ	элемент перечисления а) раздела 9.2
М15	Реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СМИБ	элемент перечисления б) раздела 9.2
М16	Реализация программ по обучению и осведомлению ИБ	элемент перечисления в) раздела 9.2
М17	Обнаружение и реагирование на инциденты безопасности	элемент перечисления г) раздела 9.2
М18	Обеспечение непрерывности бизнеса и восстановления после прерываний	элемент перечисления д) раздела 9.2, раздел 9.6
Проверка (мониторинг и анализ) СМИБ		
М19	Мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ	элемент перечисления а) раздела 9.3, раздел. 10.9
М20	Анализ эффективности СМИБ, включая анализ уровней остаточного и приемлемого рисков ИБ	элемент перечисления б) раздела 9.3
М21	Внутренний аудит СМИБ	элемент перечисления в) раздела 9.3, раздел 10
М22	Анализ СМИБ со стороны высшего руководства	элемент перечисления г) раздела 9.3
М23	Внешний аудит СМИБ	элемент перечисления д) раздела 9.3, раздел 10
Совершенствование СМИБ		
М24	Реализация тактических улучшений в СМИБ	элемент перечисления а) раздела 9.4
М25	Реализация стратегических улучшений СМИБ. Использование опыта	элемент перечисления б) раздела 9.4
М26	Информирование об изменениях и их согласование с заинтересованными сторонами	элемент перечисления в) раздела 9.4
М27	Оценка достижения поставленных целей	элемент перечисления г) раздела 9.4

8.3. Частные показатели по направлению оценки “менеджмент ИБ организации” (показатели М9÷М27) и метрики приведены в приложении А.

8.4. Оценка частного показателя ИБ ($EV_{Mi.j}$) определяется посредством экспертного оценивания. Для принятия решения следует производить анализ нормативных, распорядительных, программных и других документов организации БС РФ, имеющих отношение к проверяемым областям ИБ, и уточнять полученную информацию с помощью опросов сотрудников организации БС РФ и наблюдения за деятельностью.

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о невыполнении соответствующих требований ИБ (отсутствии процессов менеджмента), то оценке $EV_{Mi.j}$ присваивается значение, равное нулю.

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о частичном выполнении соответствующих требований ИБ (частичной реализации процессов менеджмента), то оценка $EV_{Mi.j}$ по решению аудиторской группы может быть установлена равной 0,25; 0,5 или 0,75 (в зависимости от степени выполнения требований ИБ или реализации процессов менеджмента).

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о полном выполнении соответствующих требований ИБ (реализации процессов менеджмента), то оценке $EV_{Mi.j}$ присваивается значение, равное единице.

8.5. Оценка группового показателя (EV_{Mi}) вычисляется из оценок входящих в него частных показателей ($EV_{Mi.j}$) с учетом коэффициентов значимости $\alpha_{i.j}$:

$$EV_{Mi} = \sum_{j} \alpha_{i.j} \cdot EV_{Mi.j},$$

где $j = 1 \div Ni$;

Ni — количество частных показателей ИБ, представляющих групповой показатель Mi;

$i = 9 \div 27$.

Коэффициенты значимости $\alpha_{i.j}$ для каждого частного показателя приведены в приложении А.

8.6. Оценки $EV_{Mi.j}$ и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ М9÷М27, вносятся в соответствующие графы представленных в приложении А форм.

8.7. Оценка $EV2_{ПЛ}$, определяющая уровень процессов планирования СМИБ организации БС РФ, вычисляется по формуле:

$$EV2_{ПЛ} = \frac{\sum_{i=9}^{13} EV_{Mi}}{5}.$$

8.8. Оценка $EV2_{Р}$, определяющая уровень процессов реализации и эксплуатации СМИБ организации БС РФ, вычисляется по формуле:

$$EV2_{Р} = \frac{\sum_{i=14}^{18} EV_{Mi}}{5}.$$

8.9. Оценка $EV2_{ПР}$, определяющая уровень процессов проверки СМИБ организации БС РФ, вычисляется по формуле:

$$EV2_{ПР} = \frac{\sum_{i=19}^{23} EV_{Mi}}{5}.$$

8.10. Оценка $EV2_{С}$, определяющая уровень процессов совершенствования СМИБ организации БС РФ, вычисляется по формуле:

$$EV2_{С} = \frac{\sum_{i=24}^{27} EV_{Mi}}{4}.$$

8.11. Итоговая оценка *EV*2, отражающая уровень процессов СМИБ организации БС РФ, определяется по наименьшему значению из оценок $EV2_{ПЛ}$, $EV2_{Р}$, $EV2_{ПР}$ и $EV2_{С}$.

8.12. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M9÷M27, отображаются на круговой диаграмме (см. раздел 10) в секторах с 9-го по 27-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

8.13. Оценка *EV*2 отображается на круговой диаграмме (см. раздел 10) в секторах с 9-го по 27-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению *EV*2.

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

9.1. Уровень осознания ИБ организации БС РФ определяется с помощью групповых и частных показателей ИБ, позволяющих оценить степень выполнения (соблюдения) общих и специальных принципов обеспечения ИБ организации БС РФ, определенных в разделе 6 СТО БР ИББС-1.0:

- своевременность обнаружения проблем;
- прогнозируемость развития проблем;
- оценка влияния проблем на бизнес-цели;
- адекватность защитных мер;
- эффективность защитных мер;
- использование опыта при принятии и реализации решений;
- непрерывность принципов безопасного функционирования;
- контролируемость защитных мер;
- определенность целей;
- знание своих клиентов и служащих;
- персонификация и адекватное разделение ролей и ответственности;
- адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки;
- доступность услуг и сервисов;
- наблюдаемость и оцениваемость обеспечения ИБ.

9.2. Групповые показатели M28÷M32 предназначены для оценки уровня осознания ИБ. Они отражают общие принципы безопасного функционирования и специальные принципы обеспечения ИБ организации БС РФ, определенные в разделе 6 СТО БР ИББС-1.0. Таблица 4 отражает соответствие между структурными элементами СТО БР ИББС-1.0, содержащими принципы ИБ, и групповыми показателями ИБ, предназначенными для оценивания уровня осознания ИБ.

Таблица 4. Соответствие групповых показателей ИБ общим и специальным принципам БР ИББС-1.0

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M28	Своевременность обнаружения проблем, прогноз развития проблем ИБ и оценка их влияния на бизнес-цели организации БС РФ	пункты 6.1.1, 6.1.2, 6.1.3
M29	Определенность целей, адекватность выбора защитных мер, их эффективность и контролируемость	пункты 6.1.4, 6.1.5, 6.1.8, 6.2.1
M30	Непрерывность обеспечения ИБ и использование опыта при принятии и реализации решений	пункты 6.1.6, 6.1.7
M31	Знание своих клиентов и служащих, персонификация и адекватное разделение ролей и ответственности, адекватность ролей функциям и процедурам	пункты 6.2.2, 6.2.3, 6.2.4
M32	Доступность услуг и сервисов, наблюдаемость и оцениваемость обеспечения ИБ	пункты 6.2.5, 6.2.6

9.3. Частные показатели ИБ по направлению оценки “уровень осознания ИБ организации” дают возможность определить степень реализации общих принципов безопасного функционирования организации БС РФ и специальных принципов обеспечения ИБ организации БС РФ. Частные показатели по направлению оценки “уровень осознания ИБ организации” (показатели M28÷M32) и метрики приведены в приложении А.

9.4. Оценка частных показателей ИБ ($EV_{Mi.j}$) определяется посредством экспертного оценивания. Для принятия решения следует производить анализ нормативно-распорядительных и

других документов организации БС РФ, имеющих отношение к общим принципам безопасного функционирования и специальным принципам обеспечения ИБ, определенным в разделе 6 СТО БР ИББС-1.0, и уточнять полученную информацию с помощью опросов сотрудников организации БС РФ и наблюдения за деятельностью организации БС РФ по выполнению общих принципов безопасного функционирования и специальных принципов обеспечения ИБ организации БС РФ.

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о невыполнении соответствующих принципов, то оценке $EV_{Mi.j}$ присваивается значение, равное нулю.

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о частичном выполнении соответствующих принципов, то оценка $EV_{Mi.j}$ по решению аудиторской группы может быть установлена равной 0,25; 0,5 или 0,75 (в зависимости от степени выполнения принципов соответствующих принципов ИБ).

Если в результате оценивания частного показателя *Mi.j* аудиторской группой сделан вывод о полном выполнении соответствующих принципов, то оценке $EV_{Mi.j}$ присваивается значение, равное единице.

9.5. Оценка группового показателя (EV_{Mi}) вычисляется из оценок входящих в него частных показателей ($EV_{Mi.j}$) с учетом коэффициентов значимости $\alpha_{i.j}$:

$$EV_{Mi} = \sum_{j} \alpha_{i.j} \cdot EV_{Mi.j},$$

где $j = 1 \div N_i$;

N_i — количество частных показателей ИБ, представляющих групповой показатель Mi;

$i = 28 \div 32$.

Коэффициенты значимости $\alpha_{i.j}$ для каждого частного показателя приведены в приложении А.

9.6. Оценки $EV_{Mi.j}$ и EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M28÷M32, вносятся в соответствующие графы представленных в приложении А форм.

9.7. Итоговая оценка *EV*3, отражающая уровень осознания ИБ для деятельности организации БС РФ, вычисляется по формуле:

$$\frac{\sum_{i=28}^{32} EV_{Mi}}{5}.$$

9.8. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M28÷M32, отображаются на круговой диаграмме (см. раздел 10) в секторах с 28-го по 32-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

9.9. Оценка *EV*3 отображается на круговой диаграмме (см. раздел 10) в секторах с 28-го по 32-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению *EV*3.

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

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

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

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

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

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

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

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

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

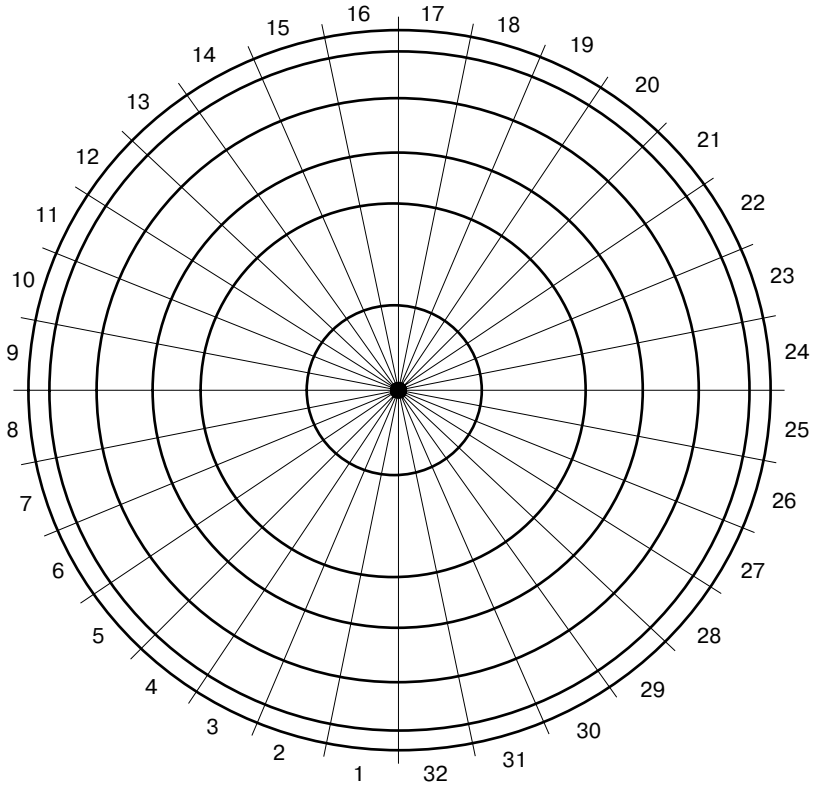
10.3. Полученное в результате оценки соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 значение *R* является основой для формирования аудиторского заключения по результатам аудита ИБ.

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 из себя круговую диаграмму для отображения результатов оценивания.

Рисунок 1. Круговая диаграмма для отображения результатов оценивания



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

Секторы с 9-го по 27-й используются для отображения оценки процессов менеджмента ИБ организации БС РФ.

Секторы с 28-го по 32-й используются для отображения оценки уровня осознания ИБ организации БС РФ.

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 соответствуют круг до окружности радиусом 0,25.

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	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М1.1	Определены ли роли персонала организации БС РФ (далее — организации)?							0,09	
М1.2	Персонифицированы ли роли в организации?							0,09	
М1.3	Установлена ли ответственность за исполнение ролей, зафиксированная в должностных инструкциях персонала?							0,09	
М1.4	Отсутствуют ли в организации роли, концентрирующие в себе все или большинство наиболее важных функций, необходимых для реализации одной из целей организации?							0,09	
М1.5	Отсутствует ли совмещение в одном лице ролей исполнителя и администратора, администратора и контролера, исполнителя и контролера и подобное?							0,09	
М1.6	Все ли роли в организации обеспечены ресурсами, необходимыми и достаточными для их выполнения?							0,09	
М1.7	Возложена ли на руководство (уполномоченного менеджера, высшего менеджера и т.п.) обязанность по координации своевременности и качества выполнения сотрудниками своих ролей?							0,09	
М1.8	Существуют ли в организации выделенные роли для контроля за качеством выполнения требований ИБ?							0,09	
М1.9	Выполняются ли при приеме на работу проверки идентичности личности, точности и полноты биографических фактов и заявляемой квалификации?							0,0724	
М1.10	Проводятся ли проверки профессиональных навыков и оценка профессиональной пригодности кандидатов при приеме на работу, связанную с защищаемыми активами и операциями?							0,0724	
М1.11	Имеются ли письменные обязательства сотрудников о соблюдении конфиденциальности всей защищаемой информации, доверенной или ставшей им известной в процессе выполнения служебных обязанностей, а также о приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов?							0,045	
М1.12	Обеспечивается ли компетентность персонала в области ИБ с помощью процессов обучения, осведомленности персонала, а также периодической проверки его компетентности в области ИБ?							0,045	
М1.13	Определены ли в трудовых контрактах всех сотрудников обязанности по выполнению требований ИБ?							0,0452	
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	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М2.1	Всегда ли выдвижение технических требований, разработка технических заданий, проектирование, создание, тестирование и приемка средств обеспечения ИБ АБС осуществляются по согласованию с подразделениями (лицами) в организации, ответственными за обеспечение ИБ?							0,1087	
М2.2	Всегда ли ввод в действие, эксплуатация, снятие с эксплуатации АБС осуществляются при участии подразделений (лиц) в организации, ответственных за обеспечение ИБ?							0,1087	
М2.3	Применяются (применялись) ли на стадии разработки АБС разработчиками меры для защиты от угроз ИБ: — принятия неверных проектных решений; — внесения дефектов на уровне архитектурных решений; — внесения недокументированных возможностей в АБС; — неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к АБС; — угрозы разработки некачественной документации; — сборки АБС разработчиком/производителем с нарушением требований; — неверного конфигурирования АБС; — приемки АБС, не отвечающей требованиям заказчика; — внесения недокументированных возможностей в АБС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ?							0,098	
М2.4	Имеют ли соответствующие лицензии организации, которые привлекаются на договорной основе для разработки и/или производства средств обеспечения ИБ АБС?							0,086	
М2.5	Получает ли организация документацию по всем приобретаемым АБС и их компонентам, содержащую описание защитных мер, предпринятых разработчиком АБС и их компонентов относительно безопасности разработки, безопасности поставки и эксплуатации, поддержки жизненного цикла, и оценку уязвимостей?							0,1086	
М2.6	Обеспечивают ли на стадии эксплуатации применяемые меры и средства обеспечения ИБ защиту от угроз несанкционированного раскрытия, модификации или уничтожения информации, недоставки или ошибочной доставки информации, отказа в обслуживании или ухудшения обслуживания, отказа от авторства сообщений?							0,098	
М2.7	Обеспечивается ли возможность сопровождения всех АБС организации и их компонентов (наличием договоров сопровождения или полным комплектом рабочей конструкторской документации)?							0,098	
М2.8	Применяются ли на стадии сопровождения меры для защиты от угрозы внесения изменений в АБС, приводящих к нарушению функциональности АБС либо к появлению недокументированных возможностей, а также для защиты от угрозы невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и состояния АБС?							0,098	
М2.9	Применяются ли на стадии снятия с эксплуатации меры для защиты от угроз ненадежного удаления информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС или с внешних носителей?							0,098	
М2.10	Включаются ли требования ИБ во все договоры и контракты на проведение работ или оказание услуг на всех стадиях жизненного цикла АБС?							0,098	
Итоговая оценка группового показателя М2									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М3.1	Соблюдаются ли при распределении прав доступа к активам организации принципы: – “знать своего клиента”; – “знать своего служащего”; – “необходимо знать”; – “двойное управление”?							0,069	
М3.2	Применяются ли в составе АБС встроенные механизмы защиты информации и/или сертифицированные (или разрешенные к применению) средства защиты информации от НСД?							0,133	
М3.3	Применяется ли парольная защита или другие средства аутентификации для всех ЭВМ и ЛВС, задействованных в технологических процессах?							0,133	
М3.4	Проводится ли назначение/лишение полномочий по доступу сотрудников к ресурсам ЭВМ и/или ЛВС только с санкции руководителя функционального подразделения организации?							0,133	
М3.5	Выполняется ли контроль доступа пользователей к ресурсам всех ЭВМ и/или ЛВС, задействованных в технологических процессах?							0,133	
М3.6	Формируются ли уникальные идентификаторы для всех пользователей, задействованных в технологических процессах?							0,133	
М3.7	Регистрируются ли действия сотрудников и пользователей, влияющие на ИБ, в специальном электронном журнале либо регистрация обеспечивается организационными и/или административными мерами?							0,133	
М3.8	Предоставлен ли доступ к электронному журналу регистрации действий пользователей и сотрудников только администратору ИБ и отсутствует ли возможность редактирования записей данного электронного журнала?							0,133	
Итоговая оценка группового показателя М3									

Групповой показатель М4 “Обеспечение информационной безопасности средствами антивирусной защиты”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М4.1	Применяются ли в организации только официально приобретенные средства антивирусной защиты?							0,1064	
М4.2	Осуществляется ли установка средств антивирусной защиты на автоматизированных рабочих местах и серверах АБС администраторами АБС?							0,1064	
М4.3	Осуществляется ли регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах АБС автоматически или администраторами АБС?							0,1064	
М4.4	Разработаны ли и введены ли в действие инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов?							0,0845	
М4.5	Всегда ли проводится антивирусная фильтрация трафика электронного почтового обмена?							0,1064	
М4.6	Применяются ли защитные меры, не допускающие присутствия и использования в ЭВМ и АБС программного обеспечения и данных, не связанных с выполнением конкретных функций в банковских технологических процессах организации?							0,0964	
М4.7	Всегда ли проводится антивирусная проверка до и после установки или изменения программного обеспечения?							0,1064	
М4.8	Указаны ли в инструкциях по антивирусной защите действия сотрудников при обнаружении компьютерного вируса?							0,1064	
М4.9	Контролируются ли установка и обновление антивирусных средств представителями подразделений или лицами, ответственными за ИБ?							0,0964	
М4.10	Возложена ли обязанность по выполнению мер антивирусной защиты на каждого сотрудника организации, имеющего доступ к ЭВМ и/или АБС, а ответственность за выполнение сотрудниками инструкций по антивирусной защите — на руководителей функциональных подразделений?							0,0843	
Итоговая оценка группового показателя М4									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М5.1	Используются ли ресурсы сети Интернет не более чем для ведения дистанционного банковского обслуживания, получения и распространения информации, связанной с банковской деятельностью, информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями исключительно с внешними организациями, а также ведения собственной хозяйственной деятельности?							0,131	
М5.2	Применяются ли при осуществлении дистанционного банковского обслуживания через сеть Интернет средства защиты информации, которые обеспечивают прием и передачу информации только в установленном формате и только по конкретной технологии?							0,131	
М5.3	Применяются ли защитные меры для осуществления безопасного электронного почтового обмена через сеть Интернет?							0,131	
М5.4	Осуществляется ли архивирование сообщений электронной почты?							0,131	
М5.5	Применяются ли защитные меры, запрещающие изменение архива сообщений электронной почты и разрешающие доступ к нему только подразделению (лицу), ответственному за обеспечение ИБ?							0,131	
М5.6	Используются ли при взаимодействии с сетью Интернет средства, позволяющие обеспечивать противодействие атакам и распространению спама?							0,12	
М5.7	Контролируется ли подразделениями (лицами) в организации, ответственными за обеспечение ИБ, подключение и использование ресурсов сети Интернет?							0,105	
М5.8	Санкционируется ли руководством функционального подразделения организации любое подключение и использование сети Интернет?							0,12	
Итоговая оценка группового показателя М5									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М6.1	Поставлены ли СКЗИ разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения?							0,1111	
М6.2	Реализованы ли СКЗИ на основе алгоритмов, соответствующих стандартам РФ, условиям договора с контрагентом и/или стандартам организации?							0,1111	
М6.3	Существует ли регламент использования ключей, предполагающий контроль со стороны администратора ИБ за действиями пользователя при получении ключевого носителя, вводе ключей, использовании ключей и сдаче ключевого носителя?							0,1111	
М6.4	Обеспечивают ли СКЗИ реализацию процедур сброса ключей при отсутствии штатной активности пользователей в соответствии с регламентом использования ключей или при переходе АБС в нештатный режим работы?							0,1111	
М6.5	Поддерживается ли непрерывность процессов протоколирования работы СКЗИ при применении СКЗИ в АБС?							0,1111	
М6.6	Поддерживается ли непрерывность процессов обеспечения целостности программного обеспечения СКЗИ для всех звеньев АБС?							0,1111	
М6.7	Обеспечивается ли ИБ процессов изготовления ключевых документов СКЗИ комплексом технологических, организационных, технических и программных мер и средств защиты?							0,1111	
М6.8	Содержит ли внутренний порядок применения СКЗИ в АБС описание процессов ввода в действие, эксплуатации, восстановления работоспособности в аварийных случаях, внесения изменений, снятия с эксплуатации, управления ключевой системой, обращения с носителями ключевой информации?							0,1111	
М6.9	Самостоятельно ли в организации изготавливаются ключи кодов аутентификации и/или электронной цифровой подписи (если нет, зафиксировано ли в договоре согласие организации считать данные ключи своими)?							0,1112	
Итоговая оценка группового показателя М6									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М7.1	Определен (отражен) ли однозначно в нормативно-методических документах организации банковский платежный технологический процесс?							0,13	
М7.2	Зафиксирован ли порядок обмена платежной информацией в договорах между участниками данного обмена?							0,13	
М7.3	Отсутствуют ли сотрудники, обладающие всеми полномочиями на бесконтрольное создание, авторизацию, уничтожение и изменение платежной информации, а также проведение операций по изменению состояния банковских счетов?							0,13	
М7.4	Контролируются ли и удостоверяются ли результаты технологических операций по обработке платежной информации обязательными процедурами контроля, независимыми от процесса обработки?							0,13	
М7.5	Назначены ли на каждом технологическом участке ответственные за администрирование средств защиты платежной информации (администраторы ИБ)?							0,13	
М7.6	Существует ли нормативный документ (документы), которым руководствуются администраторы ИБ в своей деятельности?							0,118	
М7.7	Предусматривает ли комплекс мер по обеспечению ИБ: — защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платежных документов; — минимально необходимый, гарантированный доступ сотрудника только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации?							0,102	
М7.8	Включает ли комплекс мер по обеспечению ИБ: — контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации; — аутентификацию платежной информации; — двустороннюю аутентификацию участников обмена платежной информацией и двустороннюю аутентификацию автоматизированных рабочих мест; — восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники; — авторизованный ввод платежной информации в АБС двумя сотрудниками с последующей программной сверкой результатов ввода на совпадение; — сверку выходных платежных сообщений с соответствующими поступившими сообщениями; — гарантированную доставку платежных сообщений участникам обмена?							0,13	
Итоговая оценка группового показателя М7									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М8.1	Определено ли руководством, какая информация, не являющаяся платежной, подлежит защите, и классифицирована ли данная информация?							0,0848	
М8.2	Изолированы ли АБС, обрабатывающие информацию, относящуюся к сведениям, составляющим государственную тайну, и сведениям ограниченного распространения, полученным из федеральных органов исполнительной власти (если такие АБС имеются), от прочих АБС организации?							0,0848	
М8.3	Назначен ли в АБС администратор ИБ, если в АБС обрабатывается информация, требующая по решению руководства защиты?							0,0848	
М8.4	Отсутствует ли совмещение в одном лице функций администратора АБС и администратора ИБ?							0,0848	
М8.5	Отсутствуют ли в роли администратора ИБ правила, пересекающиеся с правилами роли администратора АБС?							0,0848	
М8.6	Осуществляет ли администратор ИБ контроль над действиями администраторов АБС и пользователей?							0,0848	
М8.7	Назначаются ли права доступа к информации подразделением, ответственным за эту информацию (владельцем информационного актива)?							0,0848	
М8.8	Определен ли порядок контроля функционирования каждой АБС лицами, отвечающими за ИБ?							0,0848	
М8.9	Регламентированы ли и согласованы ли со службой ИБ процессы подготовки, ввода, обработки и хранения информации, а также порядок установки, настройки, эксплуатации и восстановления технических и программных средств?							0,0848	
М8.10	Регламентировано ли и согласовано ли со службой ИБ тестирование всех функций по обеспечению ИБ, реализованных программно-техническими средствами?							0,076	
М8.11	Проводится ли периодическое тестирование всех реализованных программно-техническими средствами функций по обеспечению ИБ?							0,076	
М8.12	Регламентирована ли в организации процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ?							0,0848	
Итоговая оценка группового показателя М8									

Групповой показатель М9 “Определение/уточнение области действия СМИБ и выбор подхода к оценке рисков ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М9.1	Существуют ли документы, в которых определена область действия СМИБ?							0,1321	
М9.2	Обосновано ли в документах, определяющих область действия СМИБ, ограничение области действия, если таковое имеется?							0,1471	
М9.3	Учитывается ли в документах, определяющих область действия СМИБ, значимость информационных активов организации?							0,1471	
М9.4	Пересматривается ли область действия СМИБ при изменении перечня информационных активов или их значимости для целей бизнеса организации?							0,1321	
М9.5	Учитывается ли в документах организации, определяющих область действия СМИБ, обязательность непрерывности бизнеса организации?							0,1471	
М9.6	Установлен ли в документах организации, определяющих область действия СМИБ, подход к оценке рисков ИБ, включающий: — оценку последствий неисполнения требований СТО БР ИББС-1.0 и нормативных актов Банка России по обеспечению ИБ; — оценку угроз нарушения процессов управления ИБ или вследствие реализации иных угроз?							0,1471	
М9.7	Реализуются ли в организации основные процессы СМИБ, связанные с планированием процессов выполнения требований ИБ, с реализацией и эксплуатацией защитных мер, с проверкой процессов выполнения требований ИБ и с совершенствованием процессов выполнения требований ИБ?							0,1474	
Итоговая оценка группового показателя М9									

Групповой показатель М10 “Анализ и оценка рисков ИБ, варианты обработки рисков ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М10.1	Осуществляется ли в организации оценка рисков ИБ, в том числе связанных с неисполнением требований нормативных актов Банка России, имеющих отношение к ИБ, а также связанных с угрозами нарушения процессов управления ИБ?							0,0794	
М10.2	Существует ли документ (документы), в котором (которых) отражены результаты анализа и оценки рисков ИБ?							0,0714	
М10.3	Определены ли роли в части деятельности по оценке и обработке рисков ИБ и определена ли ответственность исполнителей, выполняющих данные роли?							0,0794	
М10.4	Назначены ли в организации лица, ответственные за управление рисками ИБ?							0,0794	
М10.5	Выполнена ли идентификация информационных активов и их уязвимостей?							0,0794	
М10.6	Выполнена ли оценка потенциального ущерба бизнесу организации в случае реализации угроз ИБ?							0,0794	
М10.7	Анализируется ли и учитывается ли при оценке рисков ИБ степень актуальности угроз?							0,0714	
М10.8	Пересматриваются ли перечень актуальных угроз информационным активам организации и степень их актуальности?							0,0714	
М10.9	Анализируется ли и учитывается ли при оценке рисков ИБ степень актуальности уязвимостей информационных активов?							0,0714	
М10.10	Пересматривается ли перечень уязвимостей информационных активов организации и степень их актуальности?							0,0714	
М10.11	Оценивается ли возможность переноса информационных рисков на другие стороны (например, страховщиков, поставщиков, органы сертификации и т.п.)?							0,0644	
М10.12	Учитываются ли данные об инцидентах ИБ при оценке рисков ИБ?							0,0644	
М10.13	Проводятся ли в организации обсуждения деятельности по оценке и обработке рисков ИБ с участием высшего руководства и руководителя службы ИБ?							0,0714	
М10.14	Определены ли в организации критерии для принятия рисков ИБ и уровни приемлемых рисков ИБ?							0,0458	
Итоговая оценка группового показателя М10									

Групповой показатель М11 “Определение/уточнение политики ИБ организации”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М11.1	Существует ли утвержденный руководством организации документ, определяющий политику ИБ организации (цели ИБ, общие задачи управления ИБ, основные области обеспечения ИБ, объекты защиты ИБ, принципы реализации и контроля политики ИБ и т.д.)?							0,12	
М11.2	Существуют ли утвержденные руководством организации документы, определяющие частные политики ИБ?							0,12	
М11.3	Определен ли порядок пересмотра документов, определяющих политику ИБ организации и частные политики?							0,11	
М11.4	Определены ли требования по регулярной отчетности должностному лицу в организации, утвердившему политику ИБ организации, о реализации положений данной политики?							0,095	
М11.5	Существует ли нормативно-методический документ (документы) по обеспечению ИБ, определяющий (определяющие) требования по реализации положений политик ИБ организации?							0,095	
М11.6	Учитываются ли в положениях политики ИБ организации результаты оценки рисков ИБ?							0,12	
М11.7	Есть ли в организации лицо (орган), ответственное за реализацию и контроль политики ИБ организации?							0,12	
М11.8	Зафиксированы ли его обязанности и ответственность за реализацию и контроль политики ИБ организации документально?							0,11	
М11.9	Имеются ли в организации отчетные документы о реализации положений политики ИБ организации?							0,11	
Итоговая оценка группового показателя М11									

Групповой показатель М12 “Выбор/уточнение целей ИБ и защитных мер”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М12.1	Существуют ли документы, в которых определен порядок внедрения защитных мер, выбранных в соответствии с требованиями раздела 8 СТО БР ИББС-1.0 и другими действующими нормативными актами организации?							0,215	
М12.2	Существуют ли документы, в которых определен план выбора защитных мер, описанных в СТО БР ИББС-1.0 и других действующих нормативных актах организации?							0,19	
М12.3	Проводятся ли в организации обсуждения по выбору защитных мер по обеспечению ИБ с участием экспертов в областях ИБ, в области финансов и в области управления персоналом?							0,19	
М12.4	Проводятся ли обсуждения по выбору новых (модернизации существующих) защитных мер по обеспечению ИБ при выявлении новых угроз и уязвимостей информационных активов организации?							0,19	
М12.5	Согласован ли выбор поставляемых (разрабатываемых) защитных мер со службой ИБ организации?							0,215	
Итоговая оценка группового показателя М12									

Групповой показатель М13 “Принятие менеджментом организации остаточных рисков и решения о реализации и эксплуатации/совершенствовании СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М13.1	Существует ли документ, в котором отражено принятие руководством организации остаточных рисков?							0,105	
М13.2	Имеется ли административное и кадровое обеспечение комплекса средств управления ИБ организации?							0,105	
М13.3	Существует ли в организации служба ИБ (ответственный за ИБ)?							0,116	
М13.4	Определены ли роли по обеспечению ИБ во всех структурных подразделениях организации?							0,105	
М13.5	Существуют ли документы, утвержденные руководством организации, определяющие перечень целей и задач службы ИБ, включающий: — управление всеми планами по обеспечению ИБ организации; — разработку и внесение предложений по изменению политики ИБ организации; — изменение существующих и принятие новых нормативно-методических документов по обеспечению ИБ организации; — выбор средств управления и обеспечения ИБ организации; — контроль пользователей, в первую очередь пользователей, имеющих максимальные полномочия; — контроль активности, связанной с доступом и использованием средств антивирусной защиты, а также с применением других средств обеспечения ИБ организации; — осуществление мониторинга событий, связанных с ИБ организации; — расследование событий, связанных с нарушениями ИБ, и в случае необходимости выхода с предложениями по применению санкций в отношении лиц, осуществивших противоправные действия, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ организации; — участие в действиях по восстановлению работоспособности АБС после сбоев и аварий; — создание, поддержку и совершенствование системы управления ИБ организации?							0,116	
М13.6	Выделен ли собственный бюджет службы ИБ организации в рамках бюджета организации?							0,116	
М13.7	Имеет ли служба ИБ организации собственного куратора на уровне первых лиц в руководстве организации?							0,105	
М13.8	Взаимодействует ли служба ИБ организации с сотрудниками, ответственными за ИБ в структурных подразделениях?							0,116	
М13.9	Обеспечена ли служба ИБ организации необходимыми и достаточными полномочиями для выполнения установленных целей и задач?							0,116	
Итоговая оценка группового показателя М13									

Групповой показатель М14 “Разработка плана обработки рисков ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М14.1	Имеются ли в организации планы по внедрению и развитию СМИБ (план обработки или минимизации рисков ИБ), определяющие совокупность мероприятий, методов и средств, создаваемых и поддерживаемых для обеспечения требуемого уровня безопасности информационных активов?							0,172	
М14.2	Утвержден ли план минимизации рисков ИБ руководством организации?							0,172	
М14.3	Есть ли в организации лицо (орган), ответственное за реализацию плана минимизации рисков ИБ?							0,172	
М14.4	Зафиксированы ли документально обязанности ответственного за реализацию плана минимизации рисков ИБ?							0,156	
М14.5	Согласован ли план минимизации рисков ИБ с планами инвестирования в обеспечение ИБ организации?							0,156	
М14.6	Корректируется ли план минимизации рисков ИБ при изменении рисков ИБ и выявлении новых рисков ИБ?							0,172	
Итоговая оценка группового показателя М14									

Групповой показатель М15 “Реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М15.1	Существуют ли свидетельства реализации плана обработки (минимизации) рисков?							0,18	
М15.2	Существуют ли план поставки/установки/сопровождения оборудования, АБС и их компонентов и/или план проведения НИОКР, соответствующие плану внедрения и развития СМИБ организации?							0,16	
М15.3	Контролирует ли руководство организации выполнение плана поставки/установки/сопровождения оборудования, АБС и их компонентов и/или плана проведения НИОКР?							0,14	
М15.4	Имеются ли в договорах на поставку/установку/сопровождение оборудования, АБС и их компонентов, включая средства ИБ, требования по обеспечению ИБ?							0,18	
М15.5	Отвечают ли процессы СМИБ по выбору, реализации и эксплуатации защитных мер требованиям, определенным разделом 8 СТО БР ИББС-1.0?							0,18	
М15.6	Предоставляются ли руководству организации отчетные документы о реализации плана внедрения и развития СМИБ?							0,16	
Итоговая оценка группового показателя М15									

Групповой показатель М16 “Реализация программ по обучению и осведомлению ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М16.1	Существует ли программа по обучению ИБ?							0,1234	
М16.2	Существуют ли свидетельства реализации программы по обучению ИБ?							0,1234	
М16.3	Проводится ли обучение ИБ персонала организации по установленному графику?							0,1	
М16.4	Проводится ли обучение ИБ сотрудника, получившего новую роль?							0,11	
М16.5	Соответствует ли программа обучения ИБ существующим политикам ИБ, применяемым защитным мерам и средствам управления ИБ?							0,1232	
М16.6	Проводится ли проверка результатов обучения ИБ сотрудников организации?							0,11	
М16.7	Имеют ли руководители и сотрудники организации документы, подтверждающие прохождение обучения ИБ?							0,11	
М16.8	Поддерживается ли осведомленность сотрудников организации о политиках и требованиях ИБ, в том числе о значимости и важности их деятельности по обеспечению ИБ?							0,1	
М16.9	Проводится ли проверка осведомленности об ИБ в организации?							0,1	
Итоговая оценка группового показателя М16									

Групповой показатель М17 “Обнаружение и реагирование на инциденты безопасности”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М17.1	Существуют ли документы, в которых определены процедуры обнаружения и регистрации инцидентов ИБ?							0,17	
М17.2	Существуют ли документы, в которых определены процедуры анализа и реагирования на инциденты ИБ?							0,17	
М17.3	Осведомлены ли сотрудники о порядке действий при обнаружении нетипичных событий ИБ и порядке информирования о данных событиях?							0,17	
М17.4	Существует ли документ, в котором определены процедуры оценки ущерба, нанесенного инцидентом ИБ?							0,135	
М17.5	Поддерживается ли в организации централизованная база инцидентов ИБ?							0,135	
М17.6	Существуют ли в организации при выявлении инцидентов ИБ процедуры, допускающие обсуждение и расследование инцидентов с участием внешних экспертов в области ИБ?							0,085	
М17.7	Осуществляется ли периодический контроль наличия уязвимостей в программных и технических средствах АБС?							0,135	
Итоговая оценка группового показателя М17									

Групповой показатель М18 “Обеспечение непрерывности бизнеса и восстановления после прерываний”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М18.1	Существует ли в организации документ, содержащий план восстановления бизнеса после прерываний?							0,18	
М18.2	Реализована ли в организации программа обучения пользователей и персонала по обеспечению непрерывности бизнес-процессов и их восстановлению после сбоев?							0,14	
М18.3	Проходит ли весь персонал и службы/подразделения обеспечения непрерывности бизнеса периодическое обучение процедурам действий в чрезвычайных ситуациях?							0,14	
М18.4	Определены ли в организации роли, обязанности и полномочия персонала и служб/подразделений в части обеспечения непрерывности бизнеса?							0,18	
М18.5	Назначены ли лица, выполняющие роли в части реализации плана восстановления бизнеса после прерываний?							0,18	
М18.6	Обладает ли организация БС необходимым резервным комплектом оборудования, предназначенным для реализации процедур оперативного восстановления нарушенных бизнес-процессов?							0,18	
Итоговая оценка группового показателя М18									

Групповой показатель М19 “Мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М19.1	**Существуют ли документы, определяющие процедуры мониторинга и контроля защитных мер, включая регистрацию действий и событий, связанных со СМИБ?**							0,0926	
М19.2	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля изменений и использования прав доступа пользователей?**							0,0926	
М19.3	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля средств и подсистем управления доступом и регистрации?**							0,0926	
М19.4	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля использования оборудования и выявления нештатных (или злоумышленных) действий в организации, а также выявления потенциальных нарушений ИБ?**							0,0926	
М19.5	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля функционирования средств антивирусной защиты?**							0,0926	
М19.6	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля использования ресурсов сети Интернет?**							0,0926	
М19.7	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля использования средств криптографической защиты информации?**							0,0926	
М19.8	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля банковских платежных технологических процессов?**							0,0926	
М19.9	**Определены ли в документах организации и выполняются ли процедуры мониторинга и контроля банковских информационных технологических процессов?**							0,0926	
М19.10	**Осуществляется ли мониторинг выполнения соглашений о качестве услуг, предоставляемых по договору сторонними организациями (при наличии таких услуг)?**							0,0833	
М19.11	**Осуществляются ли в организации процедуры по управлению данными мониторинга и контроля?**							0,0833	
Итоговая оценка группового показателя М19									

Групповой показатель М20 “Анализ эффективности СМИБ, включая анализ уровней остаточного и приемлемого рисков ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М20.1	Определены ли в документах организации и выполняются ли процедуры по анализу эффективности СМИБ (полноте и адекватности процессов менеджмента ИБ)?							0,2	
М20.2	Используются ли при анализе эффективности СМИБ результаты мониторинга ИБ и сведения относительно инцидентов ИБ?							0,2	
М20.3	Используются ли результаты оценки рисков ИБ при анализе эффективности СМИБ, включая анализ уровней остаточного и приемлемого рисков ИБ?							0,2	
М20.4	Определены ли в документах организации и выполняются ли процедуры по подготовке отчетности для руководства по вопросам эффективности СМИБ?							0,2	
М20.5	Отражаются ли в отчетах руководству по вопросам эффективности СМИБ результаты оценки рисков ИБ при изменениях в процессах и технологиях?							0,2	
Итоговая оценка группового показателя М20									

Групповой показатель М21 “Внутренний аудит СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М21.1	Определен ли документально порядок проведения внутреннего аудита ИБ в организации?							0,104	
М21.2	Выполняются ли при внутреннем аудите ИБ в организации все следующие действия: – документальная проверка; – опрос и интервью с руководством и персоналом; – проверка на местах?							0,115	
М21.3	Используются ли при проведении внутреннего аудита ИБ данные мониторинга ИБ (в том числе журналы регистрации инцидентов ИБ)?							0,115	
М 21.4	Определен ли документально и выполняется ли порядок подготовки и предоставления исходных данных (источников свидетельств аудита ИБ, свидетельств аудита ИБ) при проведении внутреннего аудита ИБ?							0,115	
М21.5	Определено ли документально руководством организации, что при проведении внутреннего аудита ИБ должно быть обеспечено документально и (при необходимости) технически подтверждено, что: – положения внутренних документов по обеспечению ИБ выполняются; – защитные меры настроены и используются правильно; – замечания (рекомендации) предшествующих аудитов ИБ выполнены?							0,115	
М21.6	Установлена ли форма представления результатов внутреннего аудита ИБ?							0,103	
М21.7	Сообщаются ли результаты внутреннего аудита ИБ руководству организации?							0,115	
М21.8	Используются ли результаты внутреннего аудита ИБ для уточнения планов внедрения и развития СМИБ организации?							0,115	
М21.9	Определен ли порядок хранения, доступа и использования материалов, получаемых в процессе проведения внутреннего аудита?							0,103	
Итоговая оценка группового показателя М21									

Групповой показатель М22 “Анализ СМИБ со стороны высшего руководства”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М22.1	**Определен ли в организации минимальный перечень документов (данных), предоставляемых высшему руководству организации для проведения анализа СМИБ?**							0,2564	
М22.2	**Имеются ли в нормативно-распорядительных документах (приказах, распоряжениях, решениях, протоколах и т.п.), принимаемых (утверждаемых) руководством организации по предоставленным ему материалам, положения и указания, определяющие требования: — по совершенствованию СМИБ; — по изменению процедур, влияющих на ИБ; — по выделению ресурсов для целей СМИБ?**							0,2564	
М22.3	**Используются ли при подготовке нормативно-распорядительных документов организации, касающихся СМИБ, отчеты службы ИБ, в том числе по выявленным инцидентам ИБ?**							0,2564	
М22.4	**Определены ли в документах организации процедуры, допускающие привлечение к анализу функционирования СМИБ организации внешних экспертов и специалистов в данной области?**							0,2308	
Итоговая оценка группового показателя М22									

Групповой показатель М23 “Внешний аудит СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М23.1	Включает ли программа аудита ИБ организации описание деятельности, необходимой для планирования, организации, проведения и совершенствования внешнего аудита ИБ?							0,11	
М23.2	Определен ли документально и выполняется ли порядок подготовки и предоставления исходных данных (источников свидетельств аудита ИБ, свидетельств аудита ИБ) при проведении внешнего аудита ИБ?							0,137	
М23.3	Используются ли результаты внешнего аудита ИБ для уточнения планов внедрения и развития СМИБ организации?							0,137	
М 23.4	Определено ли документально руководством организации, что при проведении внешнего аудита ИБ должно быть обеспечено документально и (при необходимости) технически подтверждено, что: — политика ИБ отражает требования бизнес-целей организации; — организационная структура управления ИБ создана; — процессы выполнения требований ИБ исполняются и удовлетворяют поставленным целям; — защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно; — остаточные риски оценены и остаются приемлемыми для организации; — система управления ИБ соответствует определенному уровню зрелости управления ИБ; — рекомендации предшествующих аудитов ИБ реализованы?							0,137	
М23.5	Проводится ли внешний аудит ИБ на соответствие требованиям СТО БР ИББС-1.0?							0,137	
М23.6	Установлены ли в организации процедуры взаимодействия аудиторской группы и руководства организации, позволяющие представителям аудиторской группы при необходимости непосредственно обращаться к руководству организации?							0,11	
М 23.7	Проводятся ли совещания руководства организации с представителями аудиторской группы, посвященные обсуждению вопроса совершенствования СМИБ по результатам проведения аудита ИБ?							0,122	
М23.8	Определен ли порядок хранения, доступа и использования аудиторского отчета?							0,11	
Итоговая оценка группового показателя М23									

Групповой показатель М24 “Реализация тактических улучшений в СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М24.1	Основываются ли принимаемые службой ИБ решения по совершенствованию СМИБ на результатах аудита ИБ, мониторинга, обработки инцидентов ИБ и потребностях в корректирующих и превентивных действиях?							0,208	
М24.2	Регистрируются ли принимаемые службой ИБ решения, направленные на совершенствование СМИБ?							0,208	
М24.3	Контролируется ли выполнение принятых службой ИБ решений, направленных на совершенствование СМИБ?							0,208	
М24.4	Выполняется ли анализ результатов реализации принятых службой ИБ решений по совершенствованию СМИБ?							0,188	
М24.5	Осуществляет ли служба ИБ согласование планов развития СМИБ с планами развития бизнеса организации?							0,188	
Итоговая оценка группового показателя М24									

Групповой показатель М25 “Реализация стратегических улучшений СМИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М25.1	Осуществляется ли руководством организации анализ соответствия реализации и/или эксплуатации СМИБ политике ИБ?							0,176	
М25.2	Существуют ли документы (база данных), содержащие описание изменений, внесенных в политику ИБ (частные политики ИБ) и план обработки рисков ИБ?							0,14	
М25.3	Основаны ли решения, принимаемые руководством, о реализации корректирующих и превентивных действий в отношении СМИБ организации на результатах оценки рисков ИБ?							0,176	
М25.4	Используются ли руководством при принятии решений о реализации корректирующих и превентивных действий в отношении СМИБ успешные практики (собственные и других организаций)?							0,156	
М25.5	Поддерживается ли руководством организации процесс оценки эффективности результатов реализации принятых решений по совершенствованию СМИБ?							0,176	
М25.6	Назначены ли ответственные за реализацию решений о стратегических улучшениях СМИБ?							0,176	
Итоговая оценка группового показателя М25									

Групповой показатель М26 “Информирование об изменениях СМИБ и их согласование с заинтересованными сторонами”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М26.1	Определены ли в документах организации и выполняются ли процедуры информирования заинтересованных сторон об изменениях в СМИБ (в политиках ИБ, процедурах, относящихся к ИБ, ответственности в области ИБ, требованиях ИБ и т.п.) в части, их касающейся?							0,167	
М26.2	Определены ли в документах организации и выполняются ли процедуры согласования изменений в СМИБ с заинтересованными сторонами в части, их касающейся?							0,167	
М26.3	Определены ли в документах организации роли по исполнению процедур информирования и согласования изменений СМИБ с заинтересованными сторонами?							0,333	
М26.4	Назначены ли лица, выполняющие роли по исполнению процедур информирования и согласования изменений СМИБ с заинтересованными сторонами?							0,333	
Итоговая оценка группового показателя М26									

Групповой показатель М27 “Оценка достижения поставленных целей”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М27.1	Рассматриваются ли (обсуждаются ли) варианты реализации задач по совершенствованию СМИБ (например, с целью минимизации затрат) и имеется ли соответствующее документальное подтверждение?							0,28	
М27.2	Осуществляется ли оценка того, что поставленные цели по совершенствованию СМИБ приведут к решению выявленных проблем?							0,28	
М27.3	Определен ли перечень предоставляемых руководству документов, позволяющих оценить достижение поставленных целей и выявить несоответствия в реализации и/или эксплуатации СМИБ этим целям?							0,16	
М27.4	Осуществляется ли руководством оценка того, что поставленные цели по совершенствованию СМИБ достигнуты?							0,28	
Итоговая оценка группового показателя М27									

Групповой показатель М28 “Своевременность обнаружения, прогноз развития проблем ИБ и оценка их влияния на бизнес-цели организации”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М28.1	Определена ли в организации классификация ресурсов по степени их критичности для обеспечения непрерывности бизнеса?							0,117	
М28.2	Определены ли в организации модель угроз и модель нарушителя, обеспечивающие прогнозирование развития возможных проблем, связанных с ИБ?							0,117	
М28.3	Определены ли в организации процедуры обработки инцидентов ИБ?							0,0905	
М28.4	Установлены ли процедуры обработки инцидентов ИБ в соответствии с классами ресурсов, затронутых при инцидентах ИБ?							0,0905	
М28.5	Доводится ли службой ИБ до руководства организации информация по инцидентам ИБ?							0,117	
М28.6	Принимаются ли решения по всем инцидентам ИБ?							0,117	
М28.7	Выполняются ли все решения, принятые по инцидентам ИБ?							0,117	
М28.8	Организует ли руководство организации деятельность по управлению рисками ИБ?							0,117	
М28.9	Приняты ли руководством организации решения по обоснованным предложениям службы ИБ по учету и внедрению требований ИБ в бизнес-процессы организации?							0,117	
Итоговая оценка группового показателя М28									

Групповой показатель М29 “Определенность целей, адекватность выбора защитных мер, их эффективность и контролируемость”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М29.1	Зафиксированы ли документально цели и задачи обеспечения ИБ организации?							0,0833	
М29.2	Осуществляется ли при необходимости или периодически уточнение/пересмотр целей и задач обеспечения ИБ организации при изменениях целей и задач бизнеса организации?							0,0833	
М29.3	Осуществляется ли при необходимости или периодически уточнение/пересмотр целей и задач обеспечения ИБ организации при изменениях процедур, технологий?							0,0833	
М29.4	Осуществляется ли при необходимости или периодически уточнение/пересмотр целей и задач обеспечения ИБ организации при изменении угроз ИБ							0,0833	
М29.5	Выбираются ли защитные меры в соответствии с моделями угроз и нарушителей?							0,0833	
М29.6	Выбираются ли защитные меры с учетом оценки затрат на реализацию защитных мер и объема возможных потерь от выполнения угроз?							0,0833	
М29.7	Существует ли утвержденный план реализации защитных мер, включающий порядок тестирования реализованных защитных мер и порядок оценивания достигнутого уровня снижения рисков ИБ организации?							0,0667	
М29.8	Оценивалось ли руководством или службой ИБ организации влияние защитных мер на цели бизнеса организации?							0,0667	
М29.9	Все ли защитные меры, используемые в организации, позволяют осуществлять контроль правильности их реализации и эксплуатации?							0,0667	
М29.10	Определен ли в организации порядок периодического тестирования комплекса защитных мер?							0,0667	
М29.11	Применяются ли в организации механизмы, позволяющие определять ущерб от инцидентов ИБ?							0,0667	
М29.12	Установлена ли в организации ответственность по контролю защитных мер и оценке адекватности и эффективности их реализации?							0,0833	
М29.13	Осуществляется ли в организации контроль за реализацией действующих положений и требований по обеспечению ИБ?							0,0834	
Итоговая оценка группового показателя М29									

Групповой показатель М30 “Непрерывность обеспечения ИБ и использование опыта при принятии и реализации решений”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М30.1	Используется ли опыт организации, других организаций при принятии решений и их реализации (например, опыт, накопленный организацией и другими организациями и отраженный в нормативных актах)?							0,08	
М30.2	Есть ли в организации служба ИБ как отдельная функциональная структура?							0,08	
М30.3	Существует ли отдельная статья бюджета организации для финансирования обеспечения ИБ?							0,08	
М30.4	Имеет ли служба ИБ куратора в руководстве организации?							0,08	
М30.5	Назначены ли лица, ответственные за реализацию политики ИБ организации и поддержание ее в актуальном состоянии?							0,08	
М30.6	Осуществляется ли анализ отсутствия разрывов в технологических процессах обеспечения ИБ организации, представляющих собой, например, нахождение защищаемых активов вне защищаемой оболочки, вне защитных мер, а также несогласованность защитных мер?							0,056	
М30.7	Определены ли процедуры контроля за изменением конфигурации АБС организации?							0,08	
М30.8	Анализируется ли влияние на ИБ организации изменений, коснувшихся бизнес-процессов организации?							0,056	
М30.9	Анализируется ли влияние на ИБ организации изменений технологий?							0,056	
М30.10	Анализируется ли влияние на ИБ организации изменений внешних событий (изменения законодательства, социального климата)?							0,056	
М30.11	Предусматривает ли план действий в нештатных ситуациях возможные последствия нештатных ситуаций?							0,08	
М30.12	Предусматривает ли план обеспечения непрерывности бизнеса организации возможные способы возобновления бизнеса?							0,08	
М30.13	Определены ли документально процедуры, которые должны быть реализованы в нештатных ситуациях для каждого сотрудника?							0,08	
М30.14	Регулярно ли проверяется руководством организации отработка плана действий в нештатных ситуациях и других планов, связанных с восстановлением и непрерывностью бизнеса организации с целью обеспечения их актуальности и эффективности?							0,056	
Итоговая оценка группового показателя М30									

Групповой показатель М31 “Знание своих клиентов и служащих, персонификация и адекватное разделение ролей и ответственности и адекватность ролей функциям и процедурам”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М31.1	Проводятся ли проверки квалификации при приеме и отборе претендентов на рабочие места?							0,1042	
М31.2	Заключает ли администрация соглашение об обязанностях и ответственности по ИБ с каждым сотрудником?							0,1042	
М31.3	Разработаны ли и поддерживаются ли в организации правила корпоративной этики?							0,0832	
М31.4	Включает ли организация в договоры со своими клиентами требования по ИБ, в том числе контроль этих требований со стороны организации?							0,1042	
М.31.5	Персонифицированы ли все роли обеспечения ИБ?							0,1042	
М.31.6	Установлена ли ответственность за исполнение ролей обеспечения ИБ?							0,1042	
М31.7	Отсутствует ли в организации пересечение ролей сотрудников по обеспечению ИБ?							0,1042	
М31.8	Персонифицирована ли ответственность за защиту отдельных активов организации?							0,0832	
М31.9	Персонифицирована ли ответственность руководителей структурных подразделений за обеспечение ИБ в своем структурном подразделении?							0,1042	
М31.10	Соответствуют ли роли обеспечения ИБ всем принятым в организации функциям, связанным с ИБ?							0,1042	
Итоговая оценка группового показателя М31									

Групповой показатель М32 “Доступность услуг и сервисов, наблюдаемость и оцениваемость обеспечения ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
		0	0,25	0,5	0,75	1	н/о		
М32.1	Определен ли в соответствующих договорах (соглашениях) с клиентами и контрагентами порядок обеспечения им доступности банковских услуг и сервисов?							0,1316	
М32.2	Выполняется ли порядок обеспечения доступности банковских услуг и сервисов для клиентов и контрагентов в установленные сроки, если это определено в договорах?							0,1316	
М32.3	Контролируется ли обеспечение доступности услуг и сервисов для клиентов и контрагентов?							0,1316	
М32.4	Определены ли документально требования по наблюдаемости (видимости, регистрации) результатов применения защитных мер, используемых в организации?							0,1316	
М32.5	Выполняются ли рекомендации внутреннего и внешнего аудитов ИБ?							0,1053	
М32.6	Разработана ли и утверждена в организации программа аудита ИБ, включающая процессы внутреннего аудита ИБ и самооценки ИБ?							0,1316	
М32.7	Выполняется ли в организации программа аудита ИБ, включающая процессы внутреннего аудита ИБ и самооценки ИБ?							0,1316	
М32.8	Контролируется (подтверждается) ли руководством организации достоверность свидетельств аудита ИБ, предъявляемых при проведении аудита ИБ?							0,1051	
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.