СОДЕРЖАНИЕ

информационные сообщения 2

О вводе в действие документов Комплекса документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации” 2

официальные документы 3

Распоряжение Банка России от 17.05.2014 № Р-399 “О вводе в действие документов, входящих в Комплекс документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации” 3

Распоряжение Банка России от 17.05.2014 № Р-400 “О вводе в действие рекомендаций в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности” 4

Стандарт Банка России СТО БР ИББС-1.0-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” 5

Стандарт Банка России СТО БР ИББС-1.2-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014” 49

Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности 151

ИНФОРМАЦИЯ
о вводе в действие документов Комплекса документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации”

Банк России вводит в действие с 1 июня 2014 года документы Комплекса документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации” (далее — Комплекс БР ИББС):

пятая редакция стандарта Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (СТО БР ИББС-1.0-2014);

четвертая редакция стандарта Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014” (СТО БР ИББС-1.2-2014);

рекомендации в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности” (РС БР ИББС-2.5-2014).

Документы Комплекса БР ИББС подготовлены и введены в действие с целью повышения уровня информационной безопасности организаций банковской системы Российской Федерации в соответствии с Федеральным законом от 27 декабря 2002 года № 184-ФЗ “О техническом регулировании” по решению Подкомитета по стандартизации “Безопасность финансовых (банковских) операций” (ПК1) Технического комитета по стандартизации “Стандарты финансовых операций” (ТК122) Федерального агентства по техническому регулированию и метрологии.

Документы Комплекса БР ИББС рекомендованы для выполнения организациями банковской системы Российской Федерации требований законодательства Российской Федерации в области персональных данных.

С 1 июня 2014 года отменяются следующие документы Комплекса БР ИББС:

рекомендации в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации” (РС БР ИББС-2.3-2010);

рекомендации в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации” (РС БР ИББС-2.4-2010).

Документы Комплекса БР ИББС будут опубликованы на официальном сайте Банка России в сети Интернет в подразделе “Информационная безопасность организаций банковской системы Российской Федерации” раздела “Информация по кредитным организациям”.

30.05.2014

17 мая 2014 года № Р-399

РАСПОРЯЖЕНИЕ

О вводе в действие документов, входящих в Комплекс документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации”

В целях повышения уровня информационной безопасности организаций банковской системы Российской Федерации:

1. Ввести в действие с 1 июня 2014 года документы, входящие в Комплекс документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации” (далее — документы):

пятую редакцию стандарта Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” и присвоить ей регистрационный номер СТО БР ИББС-1.0-2014;

четвертую редакцию стандарта Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014” и присвоить ей регистрационный номер СТО БР ИББС-1.2-2014.

2. Назначить ответственным за ведение контрольных экземпляров документов Главное управление безопасности и защиты информации Банка России.

3. Пресс-службе Банка России (Граник А.В.) в срок до 1 июня 2014 года опубликовать документы и соответствующее информационное сообщение о них в “Вестнике Банка России”, а также разместить на официальном сайте Банка России в информационно-телекоммуникационной сети “Интернет”:

документы;

информационное сообщение о вводе в действие документов с указанием структурного подразделения Банка России, ответственного за ведение контрольных экземпляров документов.

4. Главному управлению безопасности и защиты информации Банка России (Крылов О.В.):

4.1. Осуществлять методическое руководство по применению документов.

4.2. Осуществлять внесение изменений в документы по мере необходимости.

4.3. Направить для ознакомления документы в Федеральную службу безопасности Российской Федерации, Федеральную службу по техническому и экспортному контролю, Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, Ассоциацию российских банков и Ассоциацию региональных банков России.

4.4. Организовать поддержку, сопровождение и совершенствование документов.

5. Территориальным учреждениям Банка России в срок до 15 июня 2014 года довести до сведения всех подведомственных кредитных организаций опубликованные на официальном сайте Банка России в информационно-телекоммуникационной сети “Интернет” документы.

6. Отменить с 1 июня 2014 года распоряжение Банка России от 21 июня 2010 года № Р-705 “О вводе в действие документов Комплекса документов в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации”.

7. Структурным подразделениям Банка России с 1 июня 2014 года в своей работе руководствоваться документами.

8. Контроль за исполнением распоряжения возложить на первого заместителя Председателя Банка России Лунтовского Г.И.

ПРЕДСЕДАТЕЛЬ БАНКА РОССИИ Э.С. НАБИУЛЛИНА

17 мая 2014 года № Р-400

РАСПОРЯЖЕНИЕ

О вводе в действие рекомендаций в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности”

В целях повышения уровня информационной безопасности организаций банковской системы Российской Федерации:

1. Ввести в действие с 1 июня 2014 года рекомендации в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности” и присвоить им регистрационный номер РС БР ИББС-2.5-2014 (далее — Рекомендации).

2. Назначить ответственным за ведение контрольного экземпляра Рекомендаций Главное управление безопасности и защиты информации Банка России.

3. Пресс-службе Банка России (Граник А.В.) в срок до 1 июня 2014 года опубликовать Рекомендации и соответствующее информационное сообщение о них в “Вестнике Банка России”, а также разместить на официальном сайте Банка России в сети Интернет:

Рекомендации;

информационное сообщение о вводе в действие Рекомендаций с указанием структурного подразделения Банка России, ответственного за ведение контрольного экземпляра Рекомендаций.

4. Главному управлению безопасности и защиты информации Банка России (Крылов О.В.):

4.1. Осуществлять методическое руководство по применению Рекомендаций.

4.2. Осуществлять внесение изменений в Рекомендации по мере необходимости.

4.3. Направить для ознакомления Рекомендации в Федеральную службу безопасности Российской Федерации, Федеральную службу по техническому и экспортному контролю, Ассоциацию российских банков и Ассоциацию региональных банков России.

5. Территориальным учреждениям Банка России в срок до 15 июня 2014 года довести до сведения всех подведомственных кредитных организаций опубликованные на официальном сайте Банка России в информационно-телекоммуникационной сети “Интернет” Рекомендации.

6. Структурным подразделениям Банка России с 1 июня 2014 года руководствоваться Рекомендациями.

7. Контроль за исполнением распоряжения возложить на первого заместителя Председателя Банка России Лунтовского Г.И.

ПРЕДСЕДАТЕЛЬ БАНКА РОССИИ Э.С. НАБИУЛЛИНА

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.0-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2014-06-01

Издание официальное

Москва
2014

Предисловие

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

2. ВЗАМЕН СТО БР ИББС-1.0-2010.

Содержание

Введение 9
1. Область применения 10
2. Нормативные ссылки 10
3. Термины и определения 10
4. Обозначения и сокращения 15
5. Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций банковской системы Российской Федерации 15
6. Модели угроз и нарушителей информационной безопасности организаций банковской системы Российской Федерации 19
7. Система информационной безопасности организаций банковской системы Российской Федерации 20
   7.1. Общие положения 20
   7.2. Общие требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу 22
   7.3. Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла 22
   7.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрацией 24
   7.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты 26
   7.6. Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет 27
   7.7. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации 28
   7.8. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов 29
   7.9. Общие требования по обеспечению информационной безопасности банковских информационных технологических процессов 30
   7.10. Общие требования по обработке персональных данных в организации банковской системы Российской Федерации 31
   7.11. Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные 33
8. Система менеджмента информационной безопасности организаций банковской системы Российской Федерации 35
   8.1. Общие положения 35
   8.2. Требования к организации и функционированию службы информационной безопасности организации банковской системы Российской Федерации 36

8.3. Требования к определению/коррекции области действия системы обеспечения информационной безопасности 37
8.4. Требования к выбору/коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков нарушения информационной безопасности 37
8.5. Требования к разработке планов обработки рисков нарушения информационной безопасности 37
8.6. Требования к разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности 38
8.7. Требования к принятию руководством организации банковской системы Российской Федерации решений о реализации и эксплуатации системы обеспечения информационной безопасности 39
8.8. Требования к организации реализации планов внедрения системы обеспечения информационной безопасности 39
8.9. Требования к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности 39
8.10. Требования к организации обнаружения и реагирования на инциденты информационной безопасности 40
8.11. Требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний 40
8.12. Требования к мониторингу информационной безопасности и контролю защитных мер 41
8.13. Требования к проведению самооценки информационной безопасности 42
8.14. Требования к проведению аудита информационной безопасности 42
8.15. Требования к анализу функционирования системы обеспечения информационной безопасности 43
8.16. Требования к анализу системы обеспечения информационной безопасности со стороны руководства организации банковской системы Российской Федерации 43
8.17. Требования к принятию решений по тактическим улучшениям системы обеспечения информационной безопасности 44
8.18. Требования к принятию решений по стратегическим улучшениям системы обеспечения информационной безопасности 45
9. Проверка и оценка информационной безопасности организаций банковской системы Российской Федерации 46
Библиография 47

Введение

Банковская система (БС) Российской Федерации (РФ) включает в себя Банк России, кредитные организации, а также представительства иностранных банков [1]. Развитие и укрепление БС РФ, обеспечение стабильности и развитие национальной платежной системы являются целями деятельности Банка России [2]. Важнейшим условием реализации этих целей является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) организаций БС РФ, их активов (в т.ч. информационных), который во многом определяется уровнем ИБ банковских технологических процессов (платежных, информационных и пр.), автоматизированных банковских систем, эксплуатирующихся организациями БС РФ.

Особенности БС РФ таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов. В случаях наступления инцидентов ИБ значительно возрастают результирующий риск и возможность нанесения ущерба организациям БС РФ. Поэтому для организаций БС РФ угрозы ИБ представляют существенную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционный, репутационный, стратегический и иные риски) в организациях БС РФ следует обеспечить достаточный уровень ИБ. Необходимо также сохранить этот уровень в течение длительного времени. По этим причинам обеспечение ИБ является для организаций БС РФ одним из основополагающих аспектов их деятельности.

Деятельность, относящаяся к обеспечению ИБ, должна контролироваться. В связи с этим Банк России является сторонником регулярной оценки уровня ИБ в организациях БС РФ, оценки риска нарушения ИБ и принятия мер, необходимых для управления этим риском.

Исходя из этого разработан настоящий стандарт по обеспечению ИБ организаций БС РФ, который является базовым для развивающей и обеспечивающей его группы документов в области стандартизации, в целом составляющих комплекс документов в области стандартизации по обеспечению ИБ организаций БС РФ.

Основные цели стандартизации по обеспечению ИБ организаций БС РФ:

- развитие и укрепление БС РФ;
- повышение доверия к БС РФ;
- поддержание стабильности организаций БС РФ и на этой основе — стабильности БС РФ в целом;
- достижение адекватности мер защиты реальным угрозам ИБ;
- предотвращение и (или) снижение ущерба от инцидентов ИБ.

Основные задачи стандартизации по обеспечению ИБ организаций БС РФ:

- установление единых требований по обеспечению ИБ организаций БС РФ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций БС РФ.

СТО БР ИББС-1.0-2014

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения 2014-06-01

1. Область применения

Настоящий стандарт распространяется на организации БС РФ и устанавливает положения по обеспечению ИБ в организациях БС РФ.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах организаций БС РФ, а также в договорах.

Положения настоящего стандарта применяются на добровольной основе, если только в отношении отдельных положений обязательность их применения не установлена законодательством РФ, иными нормативными правовыми актами, в том числе нормативными актами Банка России.

Обязательность применения настоящего стандарта может быть установлена договорами, заключенными организациями БС РФ, или решением организации БС РФ о присоединении к стандарту. В этих случаях требования настоящего стандарта, содержащие положения долженствования, применяются на обязательной основе, а рекомендации применяются по решению организации БС РФ.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

Стандарт Банка России СТО БР ИББС-1.2 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”;

Рекомендации в области 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”;

Рекомендации в области 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”.

3. Термины и определения

Термины, установленные настоящим стандартом, применяются во всех видах документации и во всех видах деятельности по обеспечению ИБ в рамках Комплекса БР ИББС[1].

3.1. **Банковская система Российской Федерации**: Банк России, кредитные организации, а также представительства иностранных банков [1].

3.2. **Стандарт**: Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг [3].

[1] См. п. 3.4.

Примечание.

Стандарт также может содержать правила и методы исследований (испытаний) и измерений, правила отбора образцов, требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

3.3. **Рекомендации в области стандартизации**: Документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего стандарта.

3.4. **Комплекс БР ИББС**: Взаимоувязанная совокупность документов в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации".

3.5. **Менеджмент**: Скоординированная деятельность по руководству и управлению.

3.6. **Система**: Множество (совокупность) материальных объектов (элементов) любой, в том числе различной физической, природы и информационных объектов, взаимодействующих между собой для достижения общей цели, обладающее системным свойством (свойствами).

Примечание.

Системным свойством (свойствами) является свойство, которого не имеет ни один из элементов и ни одно из подмножеств элементов при любом способе членения. Системное свойство не выводимо непосредственно из свойств элементов и частей.

3.7. **Информация**: Сведения (сообщения, данные) независимо от формы их представления [4].

3.8. **Инфраструктура**: Комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи).

3.9. **Информационная инфраструктура**: Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

Примечание.

Информационная инфраструктура:

включает совокупность информационных центров, банков данных и знаний, систем связи;

обеспечивает доступ потребителей к информационным ресурсам.

3.10. **Документ**: Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

[ГОСТ Р 52069.0-2003]

Примечание.

Под материальным носителем подразумевается изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.

3.11. **Процесс**: Совокупность взаимосвязанных ресурсов и деятельности, преобразующая входы в выходы.

3.12. **Технология**: Совокупность взаимосвязанных методов, способов, приемов предметной деятельности.

3.13. **Технологический процесс**: Процесс, реализующий некоторую технологию.

3.14. **Автоматизированная система**: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

[ГОСТ 34.003-90]

3.15. **Авторизация**: Предоставление прав доступа.

3.16. **Идентификация**: Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

3.17. **Аутентификация**: Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

3.18. **Регистрация**: Фиксация данных о совершенных действиях (событиях).

3.19. **Роль**: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом.

Примечания.

1. К субъектам относятся лица из числа руководителей организации банковской системы Российской Федерации, ее персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.

2. Объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

3.20. **Угроза**: Опасность, предполагающая возможность потерь (ущерба).

3.21. **Риск**: Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

3.22. **Актив**: Все, что имеет ценность для организации БС РФ и находится в ее распоряжении.

Примечание.

К активам организации БС РФ могут относиться:

работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;

различные виды банковской информации — платежная, финансово-аналитическая, служебная, управляющая, персональные данные и пр.;

банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы);

банковские продукты и услуги, предоставляемые клиентам.

3.23. **Информационный актив**: Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации БС РФ; находящаяся в распоряжении организации БС РФ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

3.24. **Классификация информационных активов**: Разделение существующих информационных активов организации БС РФ по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

3.25. **Объект среды информационного актива**: Материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

3.26. **Ресурс**: Актив организации БС РФ, который используется или потребляется в процессе выполнения некоторой деятельности.

3.27. **Банковский технологический процесс**: Технологический процесс, реализующий операции по изменению и (или) определению состояния активов организации БС РФ, используемых при функционировании или необходимых для реализации банковских услуг.

Примечания.

1. Операции над активами организации БС РФ могут выполняться вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем.

2. В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, банковский информационный технологический процесс и др.

3.28. **Банковский платежный технологический процесс**: Часть банковского технологического процесса, реализующая действия с информацией, связанные с осуществлением переводов денежных средств, платежного клиринга и расчета, и действия с архивами указанной информации.

3.29. **Банковский информационный технологический процесс**: Часть банковского технологического процесса, реализующая действия с информацией, необходимые для выполнения организацией БС РФ своих функций, и не являющаяся банковским платежным технологическим процессом.

3.30. **Платежная информация**: Информация, на основании которой совершаются операции, связанные с осуществлением переводов денежных средств.

3.31. **Неплатежная информация**: Информация, необходимая для функционирования организации БС РФ, не являющаяся платежной информацией, которая может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.

3.32. **Автоматизированная банковская система**: Автоматизированная система, реализующая банковский технологический процесс.

3.33. **Комплекс средств автоматизации автоматизированной банковской системы**: Совокупность всех компонентов автоматизированной банковской системы организации БС РФ за исключением людей.

3.34. **Безопасность**: Состояние защищенности интересов (целей) организации БС РФ в условиях угроз.

3.35. **Информационная безопасность, ИБ**: Безопасность, связанная с угрозами в информационной сфере.

Примечания.

1. Защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) организации БС РФ.

2. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

3.36. **Доступность информационных активов**: Свойство ИБ организации БС РФ, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

3.37. **Целостность информационных активов**: Свойство ИБ организации БС РФ сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

3.38. **Конфиденциальность информационных активов**: Свойство ИБ организации БС РФ, состоящее в том, что обработка, хранение и передача информационных активов осуществляется таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

3.39. **Система информационной безопасности; СИБ**: Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

3.40. **Система менеджмента информационной безопасности; СМИБ**: Часть менеджмента организации БС РФ, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

3.41. **Система обеспечения информационной безопасности; СОИБ**: Совокупность СИБ и СМИБ организации БС РФ.

3.42. **Область действия системы обеспечения информационной безопасности; область действия СОИБ**: Совокупность информационных активов и элементов информационной инфраструктуры организации БС РФ.

3.43. **Осознание необходимости обеспечения информационной безопасности; осознание ИБ**: Понимание руководством организации БС РФ необходимости самостоятельно на основе принятых в этой организации ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по обеспечению ИБ, а также поддерживать эту деятельность адекватно прогнозу.

Примечание.

Осознание ИБ является внутренней побудительной причиной для руководства БС РФ инициировать и поддерживать деятельность по обеспечению ИБ в отличие от побуждения или принуждения, когда решение об инициировании и поддержке деятельности по обеспечению ИБ определяется соответственно либо возникшими проблемами организации, либо внешними факторами, например требованиями законов.

3.44. **Защитная мера**: сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ организации БС РФ.

3.45. **Угроза информационной безопасности; угроза ИБ**: Угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации БС РФ.

3.46. **Уязвимость информационной безопасности; уязвимость ИБ**: Слабое место в инфраструктуре организации БС РФ, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.

3.47. **Ущерб**: Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации БС РФ, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

3.48. **Инцидент информационной безопасности; инцидент ИБ**: Событие или комбинация событий, указывающая на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

- нарушение или возможное нарушение работы средств защиты информации в составе СОИБ организации БС РФ;
- нарушение или возможное нарушение требований законодательства РФ, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение или возможное нарушение в выполнении процессов СОИБ организации БС РФ;
- нарушение или возможное нарушение в выполнении банковских технологических процессов организации БС РФ;
- нанесение или возможное нанесение ущерба организации БС РФ и (или) ее клиентам.

3.49. **Нарушитель информационной безопасности; нарушитель ИБ**: Субъект, реализующий угрозы ИБ организации БС РФ, нарушая предоставленные ему полномочия по доступу к активам организации БС РФ или по распоряжению ими.

3.50. **Модель нарушителя информационной безопасности; модель нарушителя ИБ**: Описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.

3.51. **Модель угроз информационной безопасности; модель угроз ИБ**: Описание актуальных для организации БС РФ источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

3.52. **Риск нарушения информационной безопасности; риск нарушения ИБ**: Риск, связанный с угрозой ИБ.

3.53. **Оценка риска нарушения информационной безопасности**: Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации БС РФ на всех стадиях их жизненного цикла.

3.54. **Обработка риска нарушения информационной безопасности**: Процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

3.55. **Остаточный риск нарушения информационной безопасности**: Риск, остающийся после обработки риска нарушения ИБ.

3.56. **Допустимый риск нарушения информационной безопасности**: Риск нарушения ИБ, предполагаемый ущерб от которого организация БС РФ в данное время и в данной ситуации готова принять.

3.57. **Документация**: Совокупность взаимосвязанных документов, объединенных общей целевой направленностью.

3.58. **План работ по обеспечению информационной безопасности**: Документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению ИБ организации БС РФ, их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей.

3.59. **Свидетельства выполнения деятельности по обеспечению информационной безопасности**: Документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ организации БС РФ.

3.60. **Политика информационной безопасности; политика ИБ**: Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации БС РФ в целом.

3.61. **Частная политика информационной безопасности; частная политика ИБ**: Документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности БС РФ.

3.62. **Мониторинг ИБ**: Постоянное наблюдение за объектами и субъектами, влияющими на ИБ организации БС РФ, а также сбор, анализ и обобщение результатов наблюдений.

3.63. **Оценка соответствия информационной безопасности; оценка соответствия ИБ**: Систематический и документируемый процесс получения свидетельств деятельности организации БС РФ по реализации требований ИБ и установлению степени выполнения в организации БС РФ критериев оценки (аудита) ИБ.

3.64. **Аудит информационной безопасности; аудит ИБ**: Независимая оценка соответствия ИБ, выполняемая работниками организации, являющейся внешней по отношению к организации БС РФ, допускающая возможность формирования профессионального аудиторского суждения о состоянии ИБ организации БС РФ.

3.65. **Самооценка информационной безопасности; самооценка ИБ**: Оценка соответствия информационной безопасности, выполняемая работниками организации БС РФ.

3.66. **Критерии оценки (аудита) информационной безопасности; критерии оценки (аудита) ИБ**: Совокупность требований к обеспечению ИБ, определенных стандартом Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций БС РФ. Общие положения” или его частью.

3.67. **Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям; свидетельства оценки соответствия (аудита) ИБ**: Записи, изложение фактов или другая информация, которые имеют отношение к критериям оценки соответствия (самооценки соответствия, аудита) ИБ и могут быть проверены.

Примечание.

Свидетельства оценки соответствия (самооценки соответствия, аудита) ИБ могут быть качественными или количественными.

3.68. **Выводы аудита информационной безопасности; выводы аудита ИБ**: Результат оценки собранных свидетельств аудита ИБ.

3.69. **Заключение по результатам аудита информационной безопасности (аудиторское заключение); заключение по результатам аудита ИБ**: Качественная или количественная оценка соответствия установленным критериям аудита ИБ, представленная аудиторской группой после рассмотрения всех выводов аудита ИБ в соответствии с целями аудита ИБ.

3.70. **Область аудита информационной безопасности; область аудита ИБ**: Содержание и границы аудита ИБ.

Примечание.

Область аудита ИБ обычно включает местонахождение, организационную структуру, виды деятельности проверяемой организации и процессы, которые подвергаются аудиту ИБ, а также охватываемый период времени.

3.71. **Программа аудита информационной безопасности; программа аудита ИБ**: План деятельности по проведению одного или нескольких аудитов ИБ (и других проверок ИБ), запланированных на конкретный период времени и направленных на достижение конкретной цели.

Примечание.

Программа аудита ИБ включает всю деятельность, необходимую для планирования, проведения, контроля, анализа и совершенствования аудитов ИБ (и других проверок ИБ).

4. Обозначения и сокращения

АБС — автоматизированная банковская система;
БС — банковская система;
ЖЦ — жизненный цикл;
ИБ — информационная безопасность;
ИСПДн — информационная система персональных данных;
НСД — несанкционированный доступ;
НРД — нерегламентированные действия в рамках предоставленных полномочий;
РФ — Российская Федерация;
СКЗИ — средство криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
СИБ — система информационной безопасности;
СОИБ — система обеспечения информационной безопасности;
ЭВМ — электронная вычислительная машина;

5. Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций банковской системы Российской Федерации

5.1. Сущность бизнеса заключается в вовлечении актива, принадлежащего собственнику (организации БС РФ), в бизнес-процесс. Эта деятельность всегда подвержена рискам, так как и на сам актив, и на бизнес-процесс могут воздействовать различного рода угрозы.

Угрозы реализуются через их источники и имеют соответствующую вероятность реализации.

Выделяют источники угроз природного, техногенного и антропогенного характера. Источники угроз антропогенного характера могут быть как злоумышленные, так и незлоумышленные.

5.2. В основе исходной концептуальной схемы ИБ организаций БС РФ лежит противоборство собственника[1] и злоумышленника[2] с целью получения контроля над информационными активами. Однако другие, незлоумышленные действия или источники угроз также лежат в сфере рассмотрения настоящего стандарта.

Если злоумышленнику удается установить такой контроль, то как самой организации БС РФ, так и клиентам, которые доверили ей свои собственные активы, наносится ущерб.

5.3. Руководство организации БС РФ должно знать, что защищать. Для этого необходимо определить и защитить все информационные активы (ресурсы), реализация угроз в отношении которых может нанести ущерб организации БС РФ.

5.4. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое нецелевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности.

Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ.

---

[1] Под собственником здесь понимается субъект хозяйственной деятельности, имеющий права владения, распоряжения или пользования активами, который заинтересован или обязан (согласно требованиям законов или иных законодательных или нормативно-правовых актов) обеспечивать защиту активов от угроз, которые могут снизить их ценность или нанести ущерб собственнику.

[2] Под злоумышленником здесь понимается лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий (адаптировано из ст. 27 УК РФ).

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности информационного актива или параметры системы, которая этот актив поддерживает.

5.5. Практически никогда не известно о готовящемся нападении, оно, как правило, бывает неожиданным. Нападения, как правило, носят локальный и конкретный по месту, цели и времени характер.

5.6. Злоумышленник изучает объект нападения, как правило, не только теоретически, никак не проявляя себя, но и практически, путем выявления уязвимостей ИБ. Путем поиска или создания уязвимостей ИБ он отрабатывает наиболее эффективный метод нападения (получения контроля над активом).

С целью управления рисками нарушения ИБ собственник создает уполномоченный орган — свою службу ИБ (подразделение (лица) в организации БС РФ, ответственные за обеспечение ИБ), организует создание и эксплуатацию СОИБ, а также организует эксплуатацию АБС в соответствии с правилами и требованиями, задаваемыми СОИБ. Одна из задач службы ИБ — выявление следов активности нарушителя.

5.7. Один из главных инструментов собственника в обеспечении ИБ — основанный на опыте прогноз (составление модели угроз и модели нарушителя)[1].

Чем обоснованнее и точнее сделан прогноз в отношении актуальных для организации БС РФ рисков нарушения ИБ, тем адекватнее и эффективнее будут планируемые и предпринимаемые усилия по обеспечению требуемого уровня ИБ. При этом следует учитывать, что со временем угрозы, их источники и риски могут изменяться. Поэтому модели следует периодически пересматривать.

5.8. Наиболее правильный и эффективный способ добиться недопущения проявления в деятельности организации БС РФ неприемлемых для нее рисков нарушения ИБ — разработать политику ИБ организации БС РФ и в соответствии с ней реализовать, эксплуатировать и совершенствовать СОИБ организации БС РФ.

5.9. Политика ИБ организаций БС РФ разрабатывается на основе накопленного в организации БС РФ опыта в области обеспечения ИБ, результатов идентификации активов, подлежащих защите, результатов оценки рисков с учетом особенностей бизнеса и технологий, требований законодательства РФ, нормативных актов Банка России, а также интересов и бизнес-целей конкретной организации БС РФ.

5.10. Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ организации БС РФ серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или менеджментом организации БС РФ, представляющим интересы собственника. Поэтому этими отношениями необходимо управлять. Понимая, что наиболее критичным элементом безопасности организации БС РФ является ее персонал, собственник должен поощрять заинтересованность и осведомленность персонала в решении проблем ИБ.

5.11. Далеко не каждая организация БС РФ располагает потенциалом для самостоятельного составления моделей угроз и нарушителя, а также политики ИБ. В этом случае эти документы должны составляться с привлечением сторонних организаций.

Модели угроз и нарушителя должны учитывать требования законодательства РФ в области ИБ, разработки ведущих специалистов банковской системы, а также международный опыт в этой сфере.

5.12. При разработке моделей угроз и моделей нарушителя необходимо учитывать, что из всех возможных объектов атак с наибольшей вероятностью нарушитель выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все операции в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации, должны особенно тщательно контролироваться.

5.13. Стратегия обеспечения ИБ организаций БС РФ, таким образом, заключается как в эффективном использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников, так и в регулярном пересмотре моделей и политик ИБ, а также корректировке СОИБ. В случае реализации угроз должен быть использован дополнительный (специально разработанный) план действий, позволяющий свести к минимуму возможные потери и восстановить СОИБ.

---

[1] Модели ИБ (угроз и нарушителей) предназначены отражать будущее, вследствие чего они носят прогнозный характер. Модели ИБ разрабатываются на основе фактов прошлого и опыта, но ориентированы на будущее. При разработке моделей (прогнозе) используется имеющийся опыт и знания, поэтому чем выше знания, тем точнее прогноз.

5.14. Любой целенаправленной деятельности (бизнесу) свойственны риски. Это объективная реальность, и понизить эти риски можно лишь до определенного остаточного уровня. Оставшаяся (остаточная) часть риска, определяемая в том числе факторами среды деятельности организации БС РФ, должна быть признана приемлемой и принята либо отклонена. В этом случае от риска следует либо уклониться (изменить среду деятельности), либо перевести на кого-нибудь (например, застраховать). Таким образом, уровень защищенности интересов (целей) организации БС РФ определяется, во-первых, величиной принятых ею остаточных рисков, а во-вторых, эффективностью работ по поддержанию принятых рисков на допустимом, низком (остаточном) уровне.

5.15. Риски нарушения ИБ должны быть согласованы и иерархически связаны с рисками основной (бизнес) деятельности организации БС РФ через возможный ущерб.

Допускается оценка рисков информационной безопасности в составе операционных рисков с целью создания единой карты рисков и оценки стоимости ущерба по организации в целом.

Риски нарушения ИБ выражаются в возможности потери состояния защищенности интересов (целей) организации БС РФ в информационной сфере и возникновения ущерба бизнесу организации БС РФ или убытков.

Потеря состояния защищенности интересов (целей) организации БС РФ в информационной сфере заключается в утрате свойств доступности, целостности или конфиденциальности информационных активов, утрате заданных целями бизнеса параметров или доступности сервисов инфраструктуры организации БС РФ.

5.16. Уязвимость ИБ создает предпосылки к реализации угрозы через нее (инцидент ИБ). Реализация угрозы нарушения ИБ приводит к утрате защищенности интересов (целей) организации БС РФ в информационной сфере, в результате чего организации БС РФ наносится ущерб. Тяжесть ущерба совместно с вероятностью приводящего к нему инцидента ИБ определяют величину риска.

5.17. Постоянный анализ и изучение инфраструктуры организации БС РФ с целью выявления и устранения уязвимостей ИБ — основа эффективной работы СОИБ.

5.18. Идентификация, анализ и оценивание рисков нарушения ИБ должны основываться на идентификации активов организации БС РФ, на их ценности для целей и задач организации БС РФ, на моделях угроз и нарушителей ИБ организации БС РФ.

5.19. При принятии решений о внедрении защитных мер для противодействия идентифицированным угрозам (рискам) необходимо учитывать, что тем самым одновременно может увеличиваться сложность СОИБ организации БС РФ, что, в свою очередь, как правило, порождает новые риски. Поэтому при выборе решения о внедрении защитных мер для обработки существующих рисков должны учитываться вопросы эксплуатации защитных мер и их влияния на общую структуру рисков организации.

5.20. Организация БС РФ осуществляет свою деятельность путем реализации совокупности процессов, среди которых возможно выделение следующих групп:

- основные процессы, обеспечивающие достижение целей и задач организации БС РФ;
- вспомогательные процессы, обеспечивающие качество, в том числе обеспечение ИБ организации БС РФ;
- процессы менеджмента (управления), обеспечивающие поддержку параметров основных и вспомогательных процессов в заданных пределах и их корректировку в случае изменения внешних или внутренних условий.

Такое разделение процессов является условным, так как основные и вспомогательные процессы нередко образуют единое целое, например, функционирование защитных мер составляет часть группы основных процессов. В то же время процессы менеджмента отделены от основных и вспомогательных процессов, которые являются объектами менеджмента.

5.21. Совокупность защитных мер, реализующих обеспечение ИБ организации БС РФ, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет СИБ организации БС РФ.

Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет СМИБ организации БС РФ.

Совокупность СИБ и СМИБ составляет СОИБ организации БС РФ.

5.22. Процессы эксплуатации защитных мер функционируют в реальном времени. Совокупность защитных мер и процессов их эксплуатации должна обеспечивать текущий требуемый уровень ИБ в условиях штатного функционирования, а также в условиях реализации угроз, учтенных в моделях организации БС РФ и приводящих к возникновению:

- локальных инцидентов ИБ;
- широкомасштабных катастроф и аварий различной природы, последствия которых могут иметь отношение к ИБ организации БС РФ.

5.23. СОИБ должна быть определена, спланирована и регламентирована в организации БС РФ. Однако даже правильно выстроенные процессы и используемые защитные меры в силу объективных причин со временем имеют тенденцию к ослаблению своей эффективности. Это неминуемо ведет к деградации системы защиты и возрастанию рисков нарушения ИБ.

Для поддержания системы защиты на должном уровне в качестве оперативной меры используется мониторинг событий и инцидентов в СИБ. Менеджмент событий и инцидентов безопасности, полученных в результате мониторинга ИБ, позволяет избежать деградации и обеспечить требуемый уровень безопасности активов.

Для оценки состояния ИБ защищаемого актива и выявления признаков деградации используемых защитных мер проводится оценка (самооценка) соответствия системы требованиям настоящего стандарта.

5.24. Для реализации и поддержания ИБ в организации БС РФ необходима реализация четырех групп процессов:

— планирование СОИБ организации БС РФ (“планирование”);
— реализация СОИБ организации БС РФ (“реализация”);
— мониторинг и анализ СОИБ организации БС РФ (“проверка”);
— поддержка и улучшение СОИБ организации БС РФ (“совершенствование”).

Указанные группы процессов составляют СМИБ организации БС РФ.

5.25. Менеджмент ИБ есть часть общего корпоративного менеджмента организации БС РФ, которая ориентирована на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы.

Группы процессов СМИБ организации БС РФ следует организовывать в виде циклической модели Деминга “... — планирование — реализация — проверка — совершенствование — планирование — ...”, которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 [5] и ИБ ISO/IEC IS 27001-2005 [6]. Организация и выполнение процессов СМИБ необходимы в том числе для обеспечения уверенности в том, что хороший практический опыт организации БС РФ документируется, становится обязательным к применению, а СОИБ совершенствуется.

5.26. Основой для построения СОИБ организации БС РФ являются требования законодательства РФ, нормативные акты Банка России, контрактные требования организации БС РФ, а также условия ведения бизнеса, выраженные на основе идентификации активов организации БС РФ, построения модели нарушителей и угроз.

5.27. Рисунок 1 иллюстрирует взаимосвязь СИБ, СМИБ и СОИБ организации БС РФ.

Рисунок 1. СОИБ организации БС РФ

5.28. Руководству организации БС РФ необходимо инициировать, поддерживать и контролировать выполнение процессов СОИБ. Степень выполнения указанной деятельности со стороны руководства организации определяется осознанием необходимости обеспечения ИБ организации БС РФ. Осознание необходимости обеспечения ИБ организации БС РФ проявляется в использовании руководством организации БС РФ бизнес-преимуществ обеспечения ИБ, способствующих формированию условий для дальнейшего развития бизнеса организации с допустимыми рисками.

5.29. Осознание необходимости обеспечения ИБ является внутренним побудительным мотивом руководства организации БС РФ постоянно инициировать, поддерживать, анализировать и контролировать СОИБ в отличие от ситуации, когда решение о выполнении указанных видов деятельности либо принимается в результате возникших проблем, либо определяется внешними факторами.

5.30. Осознание необходимости обеспечения ИБ организации БС РФ выражается посредством выполнения в рамках СМИБ деятельности со стороны руководства, направленной на инициирование, поддержание, анализ и контроль СОИБ организации БС РФ.

6. Модели угроз и нарушителей информационной безопасности организаций банковской системы Российской Федерации

6.1. Модели угроз и нарушителей должны быть основным инструментом организации БС РФ при развертывании, поддержании и совершенствовании СОИБ.

6.2. Деятельность организации БС РФ поддерживается входящей в ее состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- банковских технологических процессов и приложений;
- бизнес-процессов организации.

6.3. На каждом из уровней угрозы и их источники (в т.ч. злоумышленники), методы и средства защиты и подходы к оценке эффективности являются различными.

6.4. Главной целью злоумышленника является получение контроля над информационными активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов, например путем раскрытия конфиденциальной банковской аналитической информации, более эффективно для злоумышленника и опаснее для собственника, чем нападение, осуществляемое через иные уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективно по соотношению “затраты / получаемый результат”.

Другой целью злоумышленника может являться нарушение функционирования бизнес-процессов организации БС РФ, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

6.5. Организация должна определить конкретные объекты среды информационных активов на каждом из уровней информационной инфраструктуры.

6.6. Основными источниками угроз ИБ являются:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;
- работники организации БС РФ, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
- работники организации БС РФ, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками организации БС РФ, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

6.7. Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

— внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;
— внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;
— комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;
— сбои, отказы, разрушения/повреждения программных и технических средств.

6.8. Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

— внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;
— комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре[1].

6.9. Наиболее актуальные источники угроз на уровне бизнес-процессов:

— внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;
— комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;
— несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

6.10. Источники угроз используют для реализации угрозы уязвимости ИБ.

6.11. Хорошей практикой в организациях БС РФ является разработка моделей угроз и нарушителей ИБ для организации в целом, а также при необходимости для ее отдельных банковских процессов.

Степень детализации параметров моделей угроз и нарушителей ИБ может быть различной и определяется реальными потребностями для каждой организации в отдельности.

6.12. В организации БС РФ рекомендуется устанавливать процедуры регулярного анализа необходимости пересмотра модели угроз и нарушителей ИБ.

7. Система информационной безопасности организаций банковской системы Российской Федерации

7.1. Общие положения

7.1.1. Выполнение требований к СИБ организации БС РФ является основой для обеспечения должного уровня ИБ. Формирование требований к СИБ организации БС РФ должно проводиться на основе:

— положений настоящего раздела стандарта;
— выполнения деятельности в рамках СМИБ организации БС РФ, определенной в разделе 8 настоящего стандарта (в частности, деятельности по разработке планов обработки рисков нарушения ИБ).

Требования к СИБ организации БС РФ должны быть оформлены документально в соответствии с Рекомендациями в области стандартизации Банка России РС БР ИББС-2.0 “Обеспечение информационной безопасности организаций БС РФ. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0”.

7.1.2. Положения подразделов 7.2—7.11 настоящего стандарта образуют базовый набор требований к СИБ, применимый к большинству организаций БС РФ. В соответствии с особенностями конкретной организации БС РФ данный базовый набор требований может быть расширен путем выполнения деятельности в рамках процессов СМИБ организации БС РФ, например, определения области действия СОИБ организации БС РФ, анализа и оценки рисков нарушения ИБ.

---

[1] На данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями ИБ, действующими самостоятельно без соучастия внутренних, практически невозможна.

7.1.3. Требования к СИБ должны быть сформированы в том числе для следующих областей:

- назначения и распределения ролей и обеспечения доверия к персоналу;
- обеспечения ИБ на стадиях ЖЦ АБС;
- защиты от НСД и НРД, управления доступом и регистрацией всех действий в АБС, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д.;
- антивирусной защиты;
- использования ресурсов сети Интернет;
- использования СКЗИ;
- защиты банковских платежных и информационных технологических процессов, в том числе банковских технологических процессов, в рамках которых обрабатываются персональные данные.

В конкретной организации БС РФ требования к СИБ могут формироваться и для других областей и направлений деятельности.

7.1.4. При распределении прав доступа работников и клиентов к информационным активам организации БС РФ следует руководствоваться принципами:

- "знать своего клиента"[1];
- "знать своего служащего"[2];
- "необходимо знать"[3],

а также рекомендуется использовать принцип "двойное управление"[4].

7.1.5. Формирование ролей должно осуществляться на основании существующих бизнес-процессов организации БС РФ и проводиться с целью исключения концентрации полномочий и снижения риска инцидентов ИБ, связанных с потерей информационными активами свойств доступности, целостности или конфиденциальности.

Формирование ролей не должно выполняться по принципу фиксации фактически сложившихся прав и полномочий персонала организации БС РФ.

7.1.6. Для обеспечения ИБ и контроля за качеством обеспечения ИБ в организации БС РФ должны быть определены роли, связанные с деятельностью по обеспечению ИБ. Руководство организации БС РФ должно осуществлять координацию своевременности и качества выполнения ролей, связанных с обеспечением ИБ.

7.1.7. ИБ АБС должна обеспечиваться на всех стадиях ЖЦ АБС, автоматизирующих банковские технологические процессы, с учетом интересов всех сторон, вовлеченных в процессы ЖЦ (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих и надзорных подразделений организации БС РФ).

7.1.8. При принятии руководством организации БС РФ решений об использовании сети Интернет, при формировании документов, регламентирующих порядок использования сети Интернет, а также иных документов, связанных с обеспечением ИБ при использовании сети Интернет, необходимо учитывать следующие положения:

- сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные из сети Интернет;
- гарантии по обеспечению ИБ при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

7.1.9. В рамках банковских платежных технологических процессов в качестве активов, защищаемых в первую очередь, следует рассматривать:

---

[1] "Знать своего клиента" (Know your Customer): принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов.

[2] "Знать своего служащего" (Know your Employee): принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью.

[3] "Необходимо знать" (Need to Know): принцип, ограничивающий полномочия по доступу к информации и ресурсам по обработке информации на уровне минимально необходимых для выполнения определенных обязанностей.

[4] "Двойное управление" (Dual Control): принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий дублирования (алгоритмического, временного, ресурсного или иного) действий до завершения определенных транзакций.

— банковский платежный технологический процесс;
— платежную информацию;
— информацию, отнесенную к защищаемой информации в соответствии с пунктом 2.1 Положения Банка России от 09.06.2012 №382-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств” в редакции Указания Банка России от 05.06.2013 № 3007-У [7].

7.2. Общие требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу

7.2.1. В организации БС РФ должны быть выделены роли ее работников.

Формирование ролей, связанных с выполнением деятельности по обеспечению ИБ, среди прочего, следует осуществлять на основании требований 7 и 8 разделов настоящего стандарта.

Формирование и назначение ролей работников организации БС РФ следует осуществлять с учетом соблюдения принципа предоставления минимальных прав и полномочий, необходимых для выполнения служебных обязанностей.

7.2.2. Роли следует персонифицировать с установлением ответственности за их выполнение. Ответственность должна быть зафиксирована, например, в должностных инструкциях или организационно-распорядительных документах организации БС РФ.

7.2.3. С целью предупреждения возникновения и снижения рисков нарушения ИБ не допускается совмещения в рамках одной роли следующих функций: разработки и сопровождения АБС/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в АБС и контроля их выполнения.

7.2.4. В организации БС РФ должны быть определены, выполняться и регистрироваться процедуры контроля деятельности работников, обладающих совокупностью полномочий, определяемых их ролями, позволяющими получить контроль над защищаемым информационным активом организации БС РФ.

7.2.5. В организации БС РФ должны быть определены, выполняться и регистрироваться процедуры приема на работу, влияющую на обеспечение ИБ, включающие:
— проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;
— проверку в части профессиональных навыков и оценку профессиональной пригодности.

Указанные процедуры должны предусматривать фиксацию результатов проводимых проверок.

7.2.6. Рекомендуется определить, выполнять и регистрировать с фиксацией результатов процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки — при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии.

7.2.7. Все работники организации БС РФ должны давать письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов.

При взаимодействии с внешними организациями и клиентами требования по обеспечению ИБ должны регламентироваться положениями, включаемыми в договоры (соглашения) с ними.

7.2.8. Обязанности персонала по выполнению требований по обеспечению ИБ должны включаться в трудовые контракты (соглашения, договоры) и (или) должностные инструкции.

Невыполнение работниками организации БС РФ требований по обеспечению ИБ должно приравниваться к невыполнению должностных обязанностей и приводить как минимум к дисциплинарной ответственности.

7.3. Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла

7.3.1. В части вопросов обеспечения ИБ следует рассматривать следующие общие стадии модели ЖЦ АБС:

1. разработка технических заданий;
2. проектирование;
3. создание и тестирование;
4. приемка и ввод в действие;

5. эксплуатация;

6. сопровождение и модернизация;

7. снятие с эксплуатации.

В случае самостоятельной разработки АБС в организации БС РФ следует рассматривать все стадии ЖЦ АБС, а в случае приобретения готовых АБС следует рассматривать стадии 4—7 ЖЦ АБС.

7.3.2. Выполнение работ на всех стадиях жизненного цикла АБС в части вопросов обеспечения ИБ должно осуществляться по согласованию и под контролем службы ИБ.

7.3.3. Организации, привлекаемые на договорной основе для обеспечения ИБ на стадиях ЖЦ АБС, должны иметь лицензии на деятельность по технической защите конфиденциальной информации в соответствии с законодательством РФ.

7.3.4. В технические задания на разработку или модернизацию АБС следует включать требования к обеспечению информационной безопасности, установленные и используемые организацией БС РФ для обеспечения ИБ в рамках технологических процессов организации БС РФ, реализуемых создаваемой или модернизированной АБС.

7.3.5. На стадии создания и тестирования АБС и (или) их компонентов организация БС РФ обеспечивает реализацию запрета использования защищаемой информации в качестве тестовых данных, анонимность данных и контроль адекватности предоставления и разграничения доступа.

7.3.6. Эксплуатируемые АБС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных в АБС защитных мер, в том числе описание состава и требований к реализации организационных защитных мер, состава и требований к эксплуатации технических защитных мер.

Организации БС РФ следует проводить анализ принятия разработчиком АБС защитных мер, направленных на обеспечение безопасности разработки АБС и безопасности ее поставки.

7.3.7. В договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов организациям БС РФ должны включаться положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных положений должен быть приобретен полный комплект документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости или позиции фирмы-поставщика (разработчика), руководство организации БС РФ должно оценить и зафиксировать допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов.

7.3.8. При разработке технических заданий на системы дистанционного банковского обслуживания должно быть учтено, что защита данных должна обеспечиваться в условиях:

- попыток несанкционированного доступа к информации анонимных, неавторизованных злоумышленников с использованием сетей общего пользования;
- возможности ошибок авторизованных пользователей систем;
- возможности ненамеренного или неадекватного использования защищаемой информации авторизованными пользователями.

7.3.9. На стадии эксплуатации АБС должны быть определены, выполняться и регистрироваться процедуры:

- контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер;
- контроля отсутствия уязвимостей в оборудовании и программном обеспечении АБС;
- контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер;
- контроля необходимого обновления программного обеспечения АБС, включая программное обеспечение технических защитных мер.

7.3.10. На стадии эксплуатации АБС должны быть определены, выполняться, регистрироваться и контролироваться процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ.

7.3.11. На стадии эксплуатации АБС должны быть определены, выполняться и регистрироваться процедуры контроля состава устанавливаемого и (или) используемого ПО АБС.

7.3.12. В организации БС РФ должны быть выделены и назначены роли, связанные с эксплуатацией и контролем эксплуатации АБС и применяемых технических защитных мер, в том числе с внесением изменений в параметры их настройки.

Для всех АБС должны быть определены и выполняться процедуры контроля ее эксплуатации со стороны службы ИБ. Проведение мероприятий по контролю эксплуатации АБС и их результаты должны регистрироваться.

7.3.13. На стадии эксплуатации АБС должны быть определены, выполняться и контролироваться процедуры, необходимые для обеспечения сохранности носителей защищаемой информации.

7.3.14. На стадии сопровождения (модернизации) должны быть определены, выполняться и регистрироваться процедуры контроля, обеспечивающие защиту от:

- умышленного несанкционированного раскрытия, модификации или уничтожения информации;
- неумышленной модификации, раскрытия или уничтожения информации;
- отказа в обслуживании или ухудшения обслуживания.

7.3.15. На стадии сопровождения (модернизации) АБС, отнесенных решением организацией БС РФ к критичным, в том числе АБС, задействованных в реализации банковского платежного технологического процесса, и в ИСПДн должны быть определены, выполняться и регистрироваться процедуры:

- фиксации внесенных изменений;
- проверки функциональности АБС, в том числе применяемых мер защиты информации, после внесения изменений.

7.3.16. На стадии снятия с эксплуатации должны быть определены, выполняться и регистрироваться процедуры, обеспечивающие удаление информации с использованием алгоритмов и (или) методов, обеспечивающих невозможность восстановления удаленной информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой техническими защитными мерами, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены законодательством РФ, нормативными актами Банка России и (или) договорными документами.

7.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрацией

7.4.1. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры выявления, учета и классификации (отнесение к одному из типов) информационных активов организации БС РФ. Права доступа работников и клиентов организации БС РФ к информационным активам и (или) их типам должны быть учтены и зафиксированы.

7.4.2. В составе АБС должны применяться встроенные защитные меры от НСД и НРД, а также могут применяться средства защиты информации, сертифицированные по требованиям безопасности информации.

Защитные меры от НСД должны обеспечивать сокрытие вводимых субъектами доступа аутентификационных данных на устройствах отображения информации. Размещение устройств отображения информации АБС должно препятствовать ее несанкционированному просмотру.

7.4.3. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры:

- идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС РФ, и программных процессов (сервисов);
- разграничения доступа к информационным активам на основе ролевого метода, с определением для каждой роли полномочий по доступу к информационным активам;
- управления предоставлением/отзывом и блокированием доступа, в том числе доступа, осуществляемого через внешние информационно-телекоммуникационные сети;
- регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации;
- управления идентификационными данными, аутентификационными данными и средствами аутентификации;
- управления учетными записями субъектов доступа;
- выявления и блокирования неуспешных попыток доступа;
- блокирования сеанса доступа после установленного времени бездействия или по запросу субъекта доступа, требующего выполнения процедур повторной аутентификации и авторизации для продолжения работы;

— ограничения действий пользователей по изменению настроек их автоматизированных мест (использование ограничений на изменение BIOS);
— управления составом разрешенных действий до выполнения идентификации и аутентификации;
— ограничения действий пользователей по изменению параметров настроек АБС и реализации контроля действий эксплуатационного персонала по изменению параметров настроек АБС;
— выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин;
— использования технологий беспроводного доступа к информации, в случае их применения, и защиты внутренних беспроводных соединений;
— использования мобильных устройств для доступа к информации в случае их применения.

Процедуры управления доступом должны исключать возможность “самосанкционирования”.

7.4.4. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры мониторинга ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции, для чего, среди прочего, следует:

— определить действия и операции, подлежащие регистрации;
— определить состав и содержание данных о действиях и операциях, подлежащих регистрации, сроки их хранения;
— обеспечить резервирование необходимого объема памяти для записи данных;
— обеспечить реагирование на сбои при регистрации действий и операций, в том числе аппаратные и программные ошибки, сбои в технических средствах сбора данных;
— обеспечить генерацию временных меток для регистрируемых действий и операций и синхронизацию системного времени на технических средствах, используемых для целей мониторинга ИБ, анализа и хранения данных.

В организации БС РФ должно быть реализовано ведение журналов действия и операций автоматизированных рабочих мест, серверного и сетевого оборудования, межсетевых экранов и АБС с целью их использования при реагировании на инциденты ИБ.

Рекомендуется обеспечить хранение данных о действиях и операциях не менее трех лет, а для данных, полученных в результате выполнения банковского платежного технологического процесса, — не менее пяти лет, если иные сроки хранения не установлены законодательством РФ, нормативными актами Банка России.

Для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях следует использовать специализированные программные и (или) технические средства.

Процедуры мониторинга ИБ и анализа данных о действиях и операциях должны использовать зафиксированные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга ИБ и анализа должны применяться на регулярной основе, например ежедневно, ко всем выполненным действиям и операциям (транзакциям).

7.4.5. В организации БС РФ необходимо определить и контролировать выполнение требований:

— к разделению сегментов вычислительных сетей, в том числе создаваемых с использованием технологии виртуализации;
— к межсетевому экранированию;
— к информационному взаимодействию между сегментами вычислительных сетей.

Разделение сегментов вычислительных сетей следует осуществлять с целью обеспечения независимого выполнения банковских платежных технологических процессов организации БС РФ, а также банковских информационных технологических процессов организации БС РФ разной степени критичности, в том числе банковских информационных технологических процессов, в рамках которых осуществляется обработка персональных данных в ИСПДн.

В документах БС РФ должны быть регламентированы и контролироваться процедуры внесения изменений в конфигурацию сетевого оборудования, предусматривающие согласование вносимых изменений со службой ИБ. Работникам службы ИБ рекомендуется предоставлять доступ к конфигурации сетевого оборудования без возможности внесения изменений.

7.4.6. Должен быть определен, выполняться, регистрироваться и контролироваться порядок доступа к объектам среды информационных активов, в том числе в помещения, в которых размещаются объекты среды информационных активов.

7.4.7. Используемые в организации БС РФ АБС, в том числе системы дистанционного банковского обслуживания, должны обеспечивать, среди прочего, 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.

7.4.8. В организации БС РФ должен быть определен, выполняться и контролироваться порядок использования съемных носителей информации.

7.4.9. Системы дистанционного банковского обслуживания должны реализовывать защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций.

Протоколам операций, выполняемых посредством систем дистанционного банковского обслуживания, следует придать свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание.

7.4.10. При заключении договоров со сторонними организациями рекомендуется предусматривать необходимый уровень взаимодействия в случае выхода инцидента ИБ за рамки отдельной организации БС РФ. Примером такого взаимодействия может служить приостановка выполнения распределенной между несколькими организациями транзакции в случае, если имеющиеся данные мониторинга ИБ и анализа протоколов операций позволяют предположить, что выполнение данной транзакции является частью замысла злоумышленников.

7.4.11. Должны быть определены и доведены до сведения работников и клиентов организации БС РФ процедуры, определяющие действия 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.

Эти процедуры должны предусматривать регистрацию работниками и клиентами всех своих действий и их результатов.

7.4.12. В системах дистанционного банковского обслуживания должны быть реализованы механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имен.

7.4.13. В организации БС РФ должны применяться меры, направленные на обеспечение защиты от НСД, повреждения или нарушения целостности данных о действиях и операциях, а также меры по защите информации, необходимой для идентификации, аутентификации и (или) авторизации клиентов и работников организации БС РФ. Все попытки НСД к такой информации должны регистрироваться. Доступ к данным о действиях и операциях предоставляется только с целью выполнения служебных обязанностей.

При увольнении или изменении должностных обязанностей работников организации БС РФ, имевших доступ к указанным данным, необходимо выполнить регламентированные процедуры соответствующего пересмотра прав доступа.

7.4.14. При осуществлении доступа на участке телекоммуникационных каналов и линий связи, в том числе беспроводных, не контролируемых организацией БС РФ, должны использоваться сетевые протоколы, обеспечивающие защиту сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии двухсторонней аутентификации.

7.4.15. Передача защищаемых данных по каналам связи, имеющим выход за пределы контролируемой организацией БС РФ зоны, должна осуществляться только при условии обеспечения их защиты от раскрытия и модификации.

7.4.16. Работа всех работников и клиентов организации БС РФ в АБС должна осуществляться под уникальными и персонифицированными учетными записями.

7.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

7.5.1. На всех автоматизированных рабочих местах и серверах АБС организации БС РФ должны применяться средства антивирусной защиты, если иное не предусмотрено реализацией технологического процесса.

В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС.

7.5.2. Рекомендуется организовать функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных.

7.5.3. Перед подключением съемных носителей информации к средствам вычислительной техники, задействованным в рамках осуществления банковских технологических процессов, рекомендуется проводить их антивирусную проверку на специально выделенном автономном средстве вычислительной техники.

7.5.4. Должны быть разработаны и введены в действие инструкции и рекомендации по антивирусной защите, учитывающие особенности банковских технологических процессов.

7.5.5. В организации БС РФ должна быть организована антивирусная фильтрация всего трафика электронного почтового обмена.

7.5.6. В организации БС РФ должна быть организована эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей на:

— рабочих станциях;
— серверном оборудовании, в том числе серверах электронной почты;
— технических средствах межсетевого экранирования.

7.5.7. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка.

7.5.8. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать:

— необходимые меры по отражению и устранению последствий вирусной атаки;
— порядок официального информирования руководства;
— порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

7.5.9. Должны быть определены, выполняться и регистрироваться процедуры контроля за отключением и обновлением антивирусных средств на всех технических средствах АБС.

7.5.10. Ответственность за выполнение требований по антивирусной защите должна быть возложена на руководителя функционального подразделения организации БС РФ, а обязанности по выполнению предписанных мер антивирусной защиты должны быть возложены на каждого работника организации, имеющего доступ к ЭВМ и (или) АБС.

7.6. Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет

7.6.1. Решение об использовании сети Интернет для производственной и (или) собственной хозяйственной деятельности должно приниматься руководством организации БС РФ. При этом цели использования сети Интернет должны быть явно перечислены и зафиксированы, например, сеть Интернет в организации БС РФ может использоваться для:

— ведения дистанционного банковского обслуживания;
— получения и распространения информации, связанной с банковской деятельностью (например, путем создания информационных web-сайтов организации БС РФ);
— информационно-аналитической работы в интересах организации;
— обмена электронными сообщениями между организациями БС РФ и иными субъектами национальной платежной системы;
— обмена электронными сообщениями, например почтовыми.

Использование сети Интернет в неустановленных целях должно быть запрещено.

С целью ограничения использования сети Интернет в неустановленных целях в организации БС РФ рекомендуется провести выделение ограниченного числа пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников организации БС РФ правами пользователя конкретного пакета должно регистрироваться и выполняться в соответствии с его должностными обязанностями, в частности в соответствии с назначенными ему ролями.

7.6.2. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры подключения и использования ресурсов сети Интернет.

7.6.3. Передача защищаемых данных с использованием сети Интернет должна осуществляться только при условии обеспечения их защиты от раскрытия и модификации.

7.6.4. В организациях БС РФ в связи с повышенными рисками нарушения ИБ при взаимодействии с сетью Интернет должны применяться защитные меры, в том числе межсетевые экраны, антивирусные средства, средства обнаружения вторжений, средства криптографической защиты информации, обеспечивающие, среди прочего, прием и передачу информации только в установленном формате и только для конкретной технологии.

Должны быть разработаны и введены в действие инструкции и рекомендации по использованию сети Интернет, учитывающие особенности банковских технологических процессов.

Должны быть определены и выполняться процедуры протоколирования посещения ресурсов сети Интернет работниками организации БС РФ. Данные о посещенных работниками организации БС РФ ресурсов сети Интернет должны быть доступны работникам службы ИБ.

7.6.5. Рекомендуется выполнить выделение и организовать физическую изоляцию от внутренних сетей тех ЭВМ, с помощью которых осуществляется непосредственное взаимодействие с сетью Интернет.

7.6.6. При осуществлении дистанционного банковского обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы. Все попытки таких подмен должны регистрироваться регламентированным в установленном в организации БС РФ порядке.

7.6.7. Все операции клиентов в течение всего сеанса работы с системами дистанционного банковского обслуживания, в том числе операции по переводу денежных средств, должны выполняться только после выполнения процедур идентификации, аутентификации и авторизации. В случаях нарушения или разрыва соединения необходимо обеспечить закрытие текущей сессии и повторное выполнение процедур идентификации, аутентификации и авторизации.

Для доступа пользователей к системам дистанционного банковского обслуживания рекомендуется использовать специализированное клиентское программное обеспечение.

7.6.8. Должны быть определены состав и порядок применения мер защиты, применяемых для организации почтового обмена через сеть Интернет.

Рекомендуется организовать 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).

7.6.9. Электронная почта должна архивироваться. Целями создания архивов электронной почты являются:

— контроль информационных потоков, в том числе с целью предотвращение утечек информации;
— использование архивов при проведении разбирательств по фактам утечек информации.

Должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры доступа к информации архива и ее изменения, предусматривающие возможность доступа работников службы ИБ к информации архива.

7.6.10. Рекомендуется не применять практику хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которых осуществляется непосредственное взаимодействие с сетью Интернет. Наличие банковской информации на таких ЭВМ должно определяться бизнес-целями организации БС РФ и санкционироваться ее руководством.

7.6.11. Должны быть определены состав и порядок применения мер защиты, применяемых при взаимодействии с сетью Интернет и позволяющих обеспечить противодействие атакам злоумышленников и распространению спама[1].

7.7. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации

7.7.1. Средства криптографической защиты информации или шифровальные (криптографические) средства (далее — СКЗИ) предназначены для защиты информации при ее обработке, хранении и передаче по каналам связи.

Необходимость использования СКЗИ определяется организацией БС РФ самостоятельно, если иное не предусмотрено законодательством РФ.

7.7.2. Применение СКЗИ в организации БС РФ должно проводиться в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией БС РФ. Рекомендуется утвердить частную политику ИБ, касающуюся применения СКЗИ в организации БС РФ.

7.7.3. СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2.

7.7.4. Работы по обеспечению с помощью СКЗИ безопасности информации проводятся в соответствии с законодательством РФ, нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России.

---

[1] Спам – общее наименование не запрошенных пользователями электронных посланий и рекламных писем, рассылаемых в сети Интернет по ставшим известными рассылающей стороне адресам пользователей.

7.7.5. Для обеспечения безопасности необходимо использовать СКЗИ, которые:

— допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;
— обладают полным комплектом эксплуатационной документации, предоставляемых разработчиком СКЗИ, включая описание ключевой системы, правил работы с ней и обоснование необходимого организационно-штатного обеспечения;
— сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

7.7.6. Установка и ввод в эксплуатацию, а также эксплуатация СКЗИ должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

7.7.7. При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы СКЗИ в соответствии с технической документацией на СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

7.7.8. ИБ процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты, предусмотренных технической документацией на СКЗИ.

7.7.9. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем рекомендуется реализовать процедуры мониторинга ИБ, регистрирующие все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и все инциденты ИБ.

7.7.10. Порядок применения СКЗИ определяется руководством организации БС РФ на основании указанных выше в данном разделе документов и должен включать:

— 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.

7.7.11. Криптографические ключи могут изготавливаться организациями БС РФ и (или) клиентом организации БС РФ самостоятельно. Отношения, возникающие между организациями БС РФ и их клиентами, регулируются заключаемыми договорами.

7.8. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов

7.8.1. СИБ банковского платежного технологического процесса должна соответствовать требованиям пунктов 7.2—7.7, 7.8 настоящего стандарта.

7.8.2. Банковский платежный технологический процесс должен быть регламентирован (описан) в организации БС РФ.

7.8.3. Порядок обмена платежной информацией должен быть зафиксирован в договорах между участниками, осуществляющими обмен платежной информацией.

7.8.4. Работники организации БС РФ, в том числе администраторы автоматизированных систем и средств защиты информации, не должны обладать полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения несанкционированных операций по изменению состояния банковских счетов.

7.8.5. Результаты технологических операций по обработке платежной информации должны контролироваться (проверяться) и удостоверяться лицами/автоматизированными процессами.

Рекомендуется, чтобы обработку платежной информации и контроль (проверку) результатов обработки осуществляли разные работники/автоматизированные процессы.

7.8.6. Комплекс защитных мер банковского платежного технологического процесса должен предусматривать, в том числе:

— защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;

— доступ работника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
— контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
— аутентификацию входящих электронных платежных сообщений;
— двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
— возможность ввода платежной информации в АБС только для авторизованных пользователей;
— контроль, направленный на исключение возможности совершения злоумышленных действий, в частности двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций;
— восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
— сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;
— возможность блокирования приема к исполнению распоряжений клиентов;
— доставку электронных платежных сообщений участникам обмена.

Кроме того, в организации БС РФ рекомендуется организовать авторизованный ввод платежной информации в АБС двумя работниками с последующей программной сверкой результатов ввода на совпадение (принцип “двойного управления”).

7.8.7. Для систем дистанционного банковского обслуживания должны применяться защитные механизмы, реализующие:
— снижение вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;
— доведение информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

Клиенты систем дистанционного банковского обслуживания должны быть обеспечены детальными инструкциями, описывающими процедуры выполнения операций или транзакций.

7.8.8. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры обслуживания средств вычислительной техники, используемых в банковском платежном технологическом процессе, включая замену их программных и (или) аппаратных частей.

7.8.9. Должны быть определены, выполняться и регистрироваться процедуры периодического контроля всех реализованных защитными мерами функций (требований) по обеспечению ИБ платежной информации.

7.8.10. Должны быть определены, выполняться и регистрироваться процедуры контроля отсутствия размещения на устройствах, задействованных в осуществлении банковского платежного технологического процесса, находящихся в общедоступных местах вне зоны постоянного контроля организации БС РФ, в том числе банкоматов и платежных терминалов, специализированных средств, используемых для несанкционированного съема информации.

7.8.11. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации.

7.9. Общие требования по обеспечению информационной безопасности банковских информационных технологических процессов

7.9.1. СИБ банковского информационного технологического процесса должна соответствовать требованиям пунктов 7.2.—7.7, 7.9 настоящего стандарта.

7.9.2. В организации БС РФ следует провести классификацию неплатежной информации и определить перечень ее типов.

Классификацию неплатежной информации следует проводить в соответствии со степенью тяжести последствий потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности.

7.9.3. Для каждого из типов неплатежной информации, полученных в результате классификации, должен быть документально определен набор требований по ее защите.

7.9.4. Банковские информационные технологические процессы должны быть регламентированы (описаны) в организации БС РФ. Указанные технологические процессы должны быть

реализованы в рамках созданных для этих целей АБС. Не входящие в состав данных АБС серверы, офисные ЭВМ и другое оборудование рекомендуется изолировать от АБС на уровне локальных вычислительных сетей способом, согласованным со службой ИБ.

7.9.5. Должны быть определены, выполняться и контролироваться требования к обеспечению ИБ в процессе взаимодействия АБС организаций БС РФ с информационными системами сторонних организаций (внешними информационными системами).

7.10. Общие требования по обработке персональных данных в организации банковской системы Российской Федерации

7.10.1. Руководство организации БС РФ должно установить цели обработки персональных данных (далее — ПДн).

7.10.2. В организации БС РФ должна быть установлена необходимость осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн и организована деятельность по своевременному направлению указанного уведомления в соответствии с требованиями Федерального закона “О персональных данных” [8] в случае наличия такой необходимости.

7.10.3. В организации БС РФ должны быть установлены критерии отнесения АБС к ИСПДн.

7.10.4. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета ресурсов ПДн[1], в том числе учета ИСПДн.

7.10.4.1. Для каждого ресурса ПДн должно быть обеспечено:

- установление цели обработки ПДн;
- установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;
- определение перечня и категорий обрабатываемых ПДн (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн);
- выполнение процедур учета количества субъектов ПДн, в том числе субъектов ПДн, не являющихся работниками организации БС РФ;
- выполнение ограничения обработки ПДн достижением цели обработки ПДн;
- соответствие содержания и объема обрабатываемых ПДн установленным целям обработки;
- точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;
- выполнение установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”;
- выполнение установленных процедур получения согласия субъектов ПДн на передачу обработки их ПДн третьим лицам, в случае если получение такого согласия необходимо в соответствии с требованиями Федерального закона “О персональных данных”;
- прекращение обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн в случаях, предусмотренных Федеральным законом “О персональных данных”, в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

7.10.4.2. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры прекращения обработки ПДн и их уничтожения либо обезличивания в сроки, установленные Федеральным законом “О персональных данных”, в следующих случаях:

- по достижении цели обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией БС РФ и субъектом ПДн);
- отзыва субъектом ПДн согласия на обработку его ПДн и в случае, если сохранение ПДн более не требуется для целей обработки ПДн (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между организацией БС РФ и субъектом ПДн);
- если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- выявления неправомерной обработки ПДн, осуществляемой организацией БС РФ или обработчиком, действующим по ее поручению, если обеспечить правомерность обработки ПДн невозможно;
- выявления неправомерной обработки ПДн без согласия субъекта ПДн.

---

[1] Ресурс ПДн – совокупность ПДн, обрабатываемых в организации БС РФ с использованием или без использования средств автоматизации и АБС, в том числе ИСПДн, объединенных общими целями обработки.

7.10.4.3. В случае отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного Федеральным законом “О персональных данных”, организация БС РФ обеспечивает их блокирование с последующим обеспечением уничтожения ПДн. Уничтожение ПДн производится не позднее шести месяцев со дня их блокирования.

7.10.5. В организации БС РФ должна быть определена, выполняться и контролироваться политика в отношении обработки ПДн, а также, в случае необходимости, установлены порядки обработки ПДн для отдельных ресурсов ПДн. Для ресурсов ПДн, обрабатываемых в АБС организации БС РФ, в том числе ИСПДн, порядок обработки ПДн может являться частью эксплуатационной документации на АБС и разрабатывается на этапе создания или модернизации АБС.

7.10.5.1. Указанные документы:

- определяют процедуры предоставления доступа к ПДн;
- определяют процедуры внесения изменений в ПДн с целью обеспечения их точности, достоверности и актуальности, в том числе по отношению к целям обработки ПДн;
- определяют процедуры уничтожения, обезличивания либо блокирования ПДн в случае необходимости выполнения таких процедур;
- определяют процедуры обработки обращений субъектов ПДн (их законных представителей) для случаев, предусмотренных Федеральным законом “О персональных данных”, в частности порядок подготовки информации о наличии ПДн, относящихся к конкретному субъекту ПДн, информации, необходимой для предоставления возможности ознакомления субъектом ПДн (их законными представителями) с его ПДн, а также процедуры обработки обращений об уточнении ПДн, их блокировании или уничтожении, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для установленной цели обработки;
- определяют процедуры обработки запроса уполномоченного органа по защите прав субъектов ПДн;
- определяют процедуры получения согласия субъекта ПДн на обработку его ПДн и на передачу обработки его ПДн третьим лицам;
- определяют процедуры передачи ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками организации БС РФ, имеющими доступ к ПДн;
- определяют процедуры передачи ПДн третьим лицам;
- определяют процедуры работы с материальными носителями ПДн;
- определяют процедуры, необходимые для осуществления уведомления уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в сроки, установленные Федеральным законом “О персональных данных”;
- определяют необходимость применения типовых форм документов для осуществления обработки ПДн и процедуры работы с ними. Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, используемая организацией БС РФ с целью сбора ПДн.

7.10.5.2. Организация БС РФ должна опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему ее политику в отношении обработки ПДн, а также к сведениям о реализуемых требованиях по обеспечению безопасности персональных данных.

7.10.6. В организации БС РФ должно быть установлено, в каких случаях необходимо получение согласия субъектов ПДн, при этом форма и порядок получения согласия субъектов ПДн должны быть регламентированы.

7.10.7. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета лиц, имеющих доступ к ПДн.

Документ, определяющий перечень лиц, имеющих доступ к ПДн, утверждается руководителем организации БС РФ.

Обработка ПДн работниками организации БС РФ должны осуществляться только с целью выполнения их должностных обязанностей.

В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры ознакомления работников организации БС РФ, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ и внутренними документами организации БС РФ, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей. Организация БС РФ может проводить указанное ознакомление работников в ходе проведения мероприятий по их обучению или повышению осведомленности.

7.10.8. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета помещений, в которых осуществляется обработка ПДн, а также доступа работников организации БС РФ и иных лиц в помещения, в которых ведется обработка ПДн.

7.10.9. При работе с материальными носителями ПДн должно быть обеспечено:

- обособление ПДн от иной информации, в частности, путем фиксации их на отдельных съемных носителях ПДн, в специальных разделах или на полях форм документов (при обработке ПДн на бумажных носителях);
- учет съемных носителей ПДн;
- установление, выполнение и контроль выполнения порядка хранения съемных, в том числе машинных, носителей ПДн и доступа к ним;
- хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных съемных носителях;
- регистрация и учет мест хранения материальных носителей ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн) включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями;
- назначение работников, ответственных за организацию хранения материальных носителей ПДн;
- установление и выполнение порядка уничтожения (стирания) информации с машинных носителей ПДн.

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

7.10.10. Общедоступные источники ПДн создаются и публикуются организацией БС РФ только для цели выполнения требований законодательства РФ. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры публикации ПДн в общедоступных источниках ПДн.

7.10.11. Поручение обработки ПДн третьему лицу (далее — обработчик) должно осуществляться на основании договора. В указанном договоре должны быть определены перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки, должна быть установлена обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн. При поручении обработки персональных данных обработчику организация БС РФ должна получить согласие субъекта ПДн, если иное не предусмотрено законодательством РФ.

7.10.12. В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться процедуры, выполняемые в случаях необходимости осуществления трансграничной передачи ПДн.

7.10.13. В организации БС РФ должно быть назначено лицо, ответственное за организацию обработки ПДн. Полномочия лица, ответственного за организацию обработки ПДн, а также его права и обязанности должны быть установлены руководством организации БС РФ.

7.11. Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные

7.11.1. СИБ банковского платежного технологического процесса, в рамках которого обрабатываются персональные данные, должна соответствовать требованиям пункта 7.8 настоящего стандарта.

СИБ банковского информационного технологического процесса, в рамках которого обрабатываются персональные данные, должна соответствовать требованиям пункта 7.9 и 7.11 настоящего стандарта.

7.11.2. Реализация требований по обеспечению ИБ, установленных в разделе 7 и разделе 8 настоящего стандарта, рекомендуется для обеспечения выполнения требований к защите персональных данных для третьего и четвертого уровня защищенности ПДн при их обработке в ИСПДн, установленных Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных” [9].

7.11.3. Требования по обеспечению информационной безопасности, установленные в разделе 7 и разделе 8 настоящего стандарта, направлены на нейтрализацию актуальных[1] (применительно к большинству организаций БС РФ) угроз безопасности персональных данных.

7.11.4. С учетом специфики обработки и обеспечения безопасности персональных данных в организациях БС РФ, угрозы утечки персональных данных по техническим каналам, а также угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн, рекомендуется признавать неактуальными для организаций БС РФ.

7.11.5. Результатом оценки рисков нарушения безопасности персональных данных является Модель угроз безопасности персональных данных, содержащая актуальные для организации БС РФ угрозы безопасности персональных данных, на основе которой вырабатываются требования, учитывающие особенности обработки персональных данных в конкретной организации БС РФ и расширяющие требования разделов 7 и 8 настоящего стандарта.

7.11.6. Для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, рекомендуется реализовывать следующие меры:

в части обеспечения ИБ АБС на стадиях жизненного цикла:

— определение, выполнение и регистрация процедур контроля целостности и обеспечения доверенной загрузки программного обеспечения, в том числе программного обеспечения технических защитных мер, на средствах вычислительной техники, входящих в ИСПДн;
— определение, выполнение, регистрация и контроль процедур доступа к эксплуатационной документации и архивным файлам, содержащим параметры настройки ИСПДн, в том числе настройки применяемых технических защитных мер;
— определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления ПДн;
— определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, в том числе программного обеспечения технических защитных мер, входящего в состав ИСПДн;

в части обеспечения ИБ при управлении доступом и регистрации:

— идентификация и аутентификация устройств, используемых для осуществления доступа;
— размещение технических средств, предназначенных для администрирования ИСПДн, автоматизированных мест пользователей и серверных компонент ИСПДн в отдельных выделенных сегментах вычислительных сетей;
— мониторинг сетевого трафика, выявление вторжений и сетевых атак и реагирование на них;
— определение, выполнение, регистрация и контроль процедур обновления сигнатурных баз технических защитных мер, мониторинг сетевого трафика, выявление вторжений и сетевых атак;

в части обеспечения ИБ банковских информационных технологических процессов:

— определение, выполнение, регистрация и контроль процедур использования коммуникационных портов, устройств ввода-вывода информации, съемных машинных носителей и внешних накопителей информации;
— определение, выполнение, регистрация и контроль процедур доступа к архивам ПДн.

7.11.7. В организации БС РФ должны быть реализованы защита периметров сегментов вычислительной сети, в которых расположены ИСПДн, и контроль информационного взаимодействия между сегментами вычислительных сетей.

В организации БС РФ должны быть определены и контролироваться правила информационного взаимодействия ИСПДн с иными АБС.

7.11.8. Использование в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации осуществляется в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных” [10].

7.11.9. Для каждой ИСПДн должен быть назначен работник организации БС РФ, ответственный за обеспечение безопасности персональных данных в ИСПДн.

---

[1] Актуальными являются те угрозы, риск реализации которых в организации БС РФ является недопустимым.

8. Система менеджмента информационной безопасности организаций банковской системы Российской Федерации

8.1. Общие положения

8.1.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ в организации БС РФ следует реализовать ряд процессов СМИБ, сгруппированных в виде циклической модели Деминга: *"... — планирование — реализация — проверка — совершенствование — планирование — ..."*.

8.1.2. Целью выполнения деятельности в рамках группы процессов "планирование" является запуск "цикла" СМИБ путем определения первоначальных планов построения, ввода в действие и контроля СОИБ, а также определения планов по совершенствованию СОИБ на основании решений, принятых на этапе "совершенствование". Выполнение деятельности на стадии "планирование" заключается в определении/корректировке области действия СОИБ, формализации подхода к оценке рисков ИБ и распределении ресурсов, проведении оценки рисков ИБ и определении/коррекции планов их обработки. Важно, чтобы все решения по реализации/корректировке СОИБ были приняты руководством организации БС РФ (далее — руководство).

8.1.3. Этап "реализация" выполняется по результатам выполнения этапов "планирование" и (или) "совершенствование" и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СОИБ, определенных на этапе "планирование" и (или) реализации решений, определенных на этапе "совершенствование" и не требующих выполнения деятельности по планированию соответствующих улучшений. В том числе важным является выполнение таких видов деятельности, как организация обучения и повышение осведомленности в области ИБ, реализация обнаружения и реагирования на инциденты ИБ, обеспечение непрерывности бизнеса организации БС РФ.

Организация БС РФ должна выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз. Организация БС РФ должна применять только те защитные меры, правильность работы которых может быть проверена, при этом организация БС РФ должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели организации.

8.1.4. Целью выполнения деятельности в рамках группы процессов "проверка" является обеспечение достаточной уверенности в том, что СОИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и (или) внешним условиям функционирования организации БС РФ, связанным с ИБ. Кроме того, необходимо рассмотреть любые изменения в допущениях или в области оценки рисков. Указанная деятельность может проводиться в любое время и с любой частотой, в зависимости от того, что является подходящим для конкретной ситуации. На этапе "проверка" необходимо осуществлять мониторинг ИБ и контроль используемых защитных мер, периодически выполнять деятельность по самооценке ИБ организации БС РФ требованиям настоящего стандарта и проводить аудит ИБ, анализировать функционирование СОИБ в целом, в том числе со стороны руководства.

Организация БС РФ должна своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ, потенциально способные повлиять на ее бизнес-цели. Рекомендуется выявлять причинно-следственную связь возможных проблем и строить на этой основе прогноз их развития.

Результат выполнения деятельности на этапе "проверка" является основой для выполнения деятельности по совершенствованию СОИБ.

8.1.5. Группа процессов "совершенствование" включает в себя деятельность по принятию решений о реализации тактических и (или) стратегических улучшений СОИБ. Указанная деятельность, т.е. переход к этапу "совершенствование", реализуется только тогда, когда выполнение процессов этапа "проверка" дало результат, требующий совершенствования СОИБ. При этом сама деятельность по совершенствованию СОИБ должна реализовываться в рамках групп процессов "реализация" и при необходимости "планирование". Пример первой ситуации — введение в действие существующего плана обеспечения непрерывности бизнеса, поскольку на стадии "проверка" определена необходимость в этом. Пример второй ситуации —

идентификация новой угрозы и последующее обновление оценки рисков на стадии “планирование”. При этом важно, чтобы все заинтересованные стороны немедленно извещались о проводимых улучшениях СОИБ и при необходимости проводилось соответствующее обучение.

Организация БС РФ должна накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

8.1.6. Для успешного функционирования СМИБ в организации БС РФ следует выполнить следующие группы требований:

- требования к организации и функционированию службы ИБ организации БС РФ;
- требования к определению/коррекции области действия СОИБ;
- требования к выбору/коррекции подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ;
- требования к разработке планов обработки рисков нарушения ИБ;
- требования к разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- требования к принятию руководством организации БС РФ решений о реализации и эксплуатации СОИБ;
- требования к организации реализации планов обработки рисков нарушения ИБ;
- требования к разработке и организации реализации программ по обучению и повышению осведомленности в области ИБ;
- требования к организации обнаружения и реагирования на инциденты безопасности;
- требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний;
- требования к мониторингу СОИБ и контролю защитных мер;
- требования к проведению самооценки ИБ;
- требования к проведению аудита ИБ;
- требования к анализу функционирования СОИБ;
- требования к анализу СОИБ со стороны руководства организации БС РФ;
- требования к принятию решений по тактическим улучшениям СОИБ;
- требования к принятию решений по стратегическим улучшениям СОИБ.

8.2. Требования к организации и функционированию службы информационной безопасности организации банковской системы Российской Федерации

8.2.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ руководству следует сформировать службу ИБ в составе не менее двух человек (назначить уполномоченных лиц), а также утвердить цели и задачи ее деятельности.

Служба ИБ должна иметь утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач, а также назначенного из числа руководства куратора. При этом служба ИБ и служба информатизации (автоматизации) не должны иметь общего куратора.

Рекомендуется наделить службу ИБ собственным бюджетом.

Организациям БС РФ, имеющим сеть филиалов или региональных представительств, рекомендуется выделять соответствующие подразделения ИБ (уполномоченных лиц) на местах, обеспечив их необходимыми ресурсами и нормативной базой.

8.2.2. Служба ИБ должна быть наделена следующими минимальными полномочиями:

- организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации БС РФ;
- разрабатывать и вносить предложения по изменению политик ИБ организации;
- организовывать изменение существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ;
- определять требования к мерам обеспечения ИБ организации БС РФ;
- контролировать работников организации БС РФ в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам;
- осуществлять мониторинг событий, связанных с обеспечением ИБ;
- участвовать в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ организации БС РФ;
- участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий;

— осуществлять контроль обеспечения ИБ на стадиях ЖЦ АБС, в том числе при тестировании и вводе в эксплуатацию подсистем ИБ АБС организации БС РФ;
— участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации БС РФ.

8.3. Требования к определению/коррекции области действия системы обеспечения информационной безопасности

8.3.1. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета структурированных по классам (типам) защищаемых информационных активов. Классификацию информационных активов рекомендуется проводить на основании оценок ценности информационных активов для интересов (целей) организации БС РФ, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов.

8.3.2. В организации БС РФ должны быть установлены критерии отнесения конкретных информационных активов к одному или нескольким типам информационных активов.

8.3.3. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 настоящего стандарта.

8.3.4. В организации БС РФ должны быть определены роли по учету информационных активов, учету объектов среды и назначены ответственные за выполнение указанных ролей.

8.4. Требования к выбору/коррекции подхода к оценке рисков нарушения информационной безопасности и проведению оценки рисков нарушения информационной безопасности

8.4.1. В организации БС РФ должна быть принята/корректироваться методика оценки рисков нарушения ИБ/подход к оценке рисков нарушения ИБ.

8.4.2. В организации БС РФ должны быть определены критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ.

8.4.3. Методика оценки рисков нарушения ИБ/подход к оценке рисков нарушения ИБ организации БС РФ должна определять 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, зафиксированными в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов организации БС РФ (типов информационных активов);
— степени тяжести последствий от потери свойств ИБ, в частности свойств доступности, целостности и конфиденциальности, для рассматриваемых информационных активов (типов информационных активов).

Порядок оценки рисков нарушения ИБ должен определять необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения.

8.4.4. Оценка рисков нарушения ИБ проводится для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ.

8.4.5. Полученные в результате оценивания рисков нарушения ИБ величины рисков должны быть соотнесены с уровнем допустимого риска, принятого в организации БС РФ. Результатом выполнения указанной процедуры является зафиксированный перечень недопустимых рисков нарушения ИБ.

8.4.6. В организации БС РФ должны быть определены роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ/подхода к оценке рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

8.4.7. В организации БС РФ должны быть определены роли по оценке рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

8.5. Требования к разработке планов обработки рисков нарушения информационной безопасности

8.5.1. По каждому из рисков нарушения ИБ, который является недопустимым, должен быть определен план, устанавливающий один из возможных способов его обработки:

— 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 по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирование планов по их реализации.

8.5.2. Планы обработки рисков нарушения ИБ должны быть согласованы с руководителем службы ИБ либо лицом, отвечающим в организации БС РФ за обеспечение ИБ, и утверждены руководством.

8.5.3. Планы реализаций требований по обеспечению ИБ должны содержать последовательность и сроки реализации и внедрения организационных, технических и иных мер защиты.

8.5.4. В организации БС РФ должны быть определены роли по разработке планов обработки рисков нарушения ИБ и назначены ответственные за выполнение указанных ролей.

8.6. Требования к разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения информационной безопасности

8.6.1. Разработку/коррекцию внутренних документов, регламентирующих деятельность в области обеспечения ИБ в организации БС РФ, рекомендуется проводить 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”.

8.6.2. В организации БС РФ должны разрабатываться/корректироваться следующие внутренние документы:
— политика ИБ организации БС РФ;
— частные политики ИБ организации БС РФ;
— документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ организации БС РФ.

Кроме того, должен быть определен перечень и формы документов, являющихся свидетельством выполнения деятельности по обеспечению ИБ в организации БС РФ.

Политика ИБ организации БС РФ должна быть утверждена руководством.

8.6.3. В политике (в частных политиках) ИБ должны определяться/корректироваться:
— 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 по 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.

8.6.4. Разработка/корректировка внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна проводиться на основе:
— законодательства РФ;
— комплекса БР ИББС, в частности, требований разделов 7 и 8 настоящего стандарта;
— нормативных актов и предписаний регулирующих и надзорных органов;
— договорных требований организации БС РФ со сторонними организациями;
— результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов или типов информационных активов.

8.6.5. Совокупность внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна содержать требования по обеспечению ИБ всех выявленных информационных активов или типов информационных активов, находящихся в области действия СОИБ организации БС РФ.

8.6.6. Документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, должны детализировать положения политики (частных политик) ИБ и не противоречить им.

8.6.7. В случае наличия в структурных подразделениях организации БС РФ работников, ответственных за обеспечение ИБ, в организации БС РФ должен быть утвержден руководством порядок взаимодействия (координирования работы) службы ИБ с указанными работниками.

8.6.8. В составе внутренних документов, регламентирующих деятельность в области обеспечения ИБ, необходимо определить:

— перечень свидетельств выполнения деятельности;
— ответственность работников организации БС РФ за выполнение этой деятельности.

8.6.9. Должны быть определены процедуры выделения и распределения ролей в области обеспечения ИБ.

8.6.10. Должен быть определен порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации БС РФ.

8.6.11. В организации БС РФ должны быть определены роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ, а также назначены ответственные за выполнение указанных ролей.

8.7. Требования к принятию руководством организации банковской системы Российской Федерации решений о реализации и эксплуатации системы обеспечения информационной безопасности

8.7.1. Решения о реализации и эксплуатации СОИБ должны утверждаться руководством организации БС РФ. В частности, в организации БС РФ требуется зафиксировать решения руководства:

— об анализе и принятии остаточных рисков нарушения ИБ;
— о планировании этапов внедрения СОИБ, в частности требований по обеспечению ИБ, изложенных в разделах 7 и 8 настоящего стандарта;
— о распределении ролей в области обеспечения ИБ организации БС РФ;
— о принятии со стороны руководства планов внедрения защитных мер, направленных на реализацию требований разделов 7 и 8 настоящего стандарта и снижение рисков ИБ;
— о выделении ресурсов, необходимых для реализации и эксплуатации СОИБ.

8.7.2. Все планы внедрения СОИБ, в частности планы реализации требований разделов 7 и 8 настоящего стандарта, планы обработки рисков нарушения ИБ и внедрения защитных мер, должны быть утверждены руководством. Указанные планы должны определять:

— последовательность выполнения мероприятий в рамках указанных планов;
— сроки начала и окончания запланированных мероприятий;
— должностных лиц (подразделения), ответственных за выполнение каждого указанного мероприятия.

8.7.3. Должен быть определен порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации БС РФ.

8.7.4. В организации БС РФ должны быть зафиксированы решения руководства, связанные с назначением и распределением ролей для всех структурных подразделений в соответствии с положениями внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ.

8.8. Требования к организации реализации планов внедрения системы обеспечения информационной безопасности

8.8.1. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры проектирования/приобретения/развертывания, внедрения, эксплуатации, контроля и сопровождения эксплуатации защитных мер (СИБ), предусмотренных планами реализаций требований по обеспечению ИБ.

8.8.2. Для построения элементов СИБ применительно к конкретной области или сфере деятельности организации БС РФ должны быть реализованы конкретные защитные меры, применяемые к объектам среды в соответствии с существующими в организации БС РФ требованиями по обеспечению ИБ, сформулированными в политике ИБ и других внутренних документах организации БС РФ.

8.8.3. В организации БС РФ должны быть определены роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер, и назначены ответственные за выполнение указанных ролей.

8.9. Требования к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности

8.9.1. Должна быть организована санкционированная руководством организации БС РФ работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ.

8.9.2. Должны быть разработаны планы, программы обучения и повышения осведомленности в области ИБ. По результатам выполнения указанных планов должна осуществляться проверка полученных знаний.

8.9.3. В планах обучения и повышения осведомленности должны быть установлены требования к периодичности обучения и повышения осведомленности.

8.9.4. Программы обучения и повышения осведомленности должны разрабатываться для различных групп сотрудников с учетом их должностных обязанностей и выполняемых ролей и включать информацию:

— по существующим политикам ИБ;
— по применяемым в организации БС РФ защитным мерам;
— по правильному использованию защитных мер в соответствии с внутренними документами организации БС РФ;
— о значимости и важности деятельности работников для обеспечения ИБ организации БС РФ.

8.9.5. В организации БС РФ должен быть определен перечень свидетельств выполнения программ обучения и повышения осведомленности в области ИБ. В частности, такими свидетельствами могут являться:

— документы (журналы), подтверждающие прохождение руководителями и работниками организации БС РФ обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых;
— документы, содержащие результаты проверок обучения работников организации БС РФ;
— документы, содержащие результаты проверок осведомленности в области ИБ в организации БС РФ.

8.9.6. Для работника, получившего новую роль, должно быть организовано обучение или инструктаж в области ИБ, соответствующее полученной роли.

8.9.7. В организации БС РФ должны быть определены роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю результатов, а также назначены ответственные за выполнение указанных ролей.

8.10. Требования к организации обнаружения и реагирования на инциденты информационной безопасности

8.10.1. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры обработки инцидентов, включающие:

— процедуры обнаружения инцидентов ИБ;
— процедуры информирования об инцидентах, в том числе информирования службы ИБ;
— процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ;
— процедуры реагирования на инцидент;
— процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ).

8.10.2. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры хранения и распространения информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

8.10.3. Должны быть определены, выполняться, регистрироваться и контролироваться действия работников организации БС РФ при обнаружении нетипичных событий, связанных с ИБ, и информировании о данных событиях. Работники организации должны быть осведомлены об указанных порядках.

8.10.4. Процедуры расследования инцидентов ИБ должны учитывать законодательство РФ, положения нормативных актов Банка России, а также внутренних документов организации БС РФ в области ИБ.

8.10.5. В организациях БС РФ должны приниматься, фиксироваться и выполняться решения по всем выявленным инцидентам ИБ.

8.10.6. В организации БС РФ должны быть определены роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ и назначены ответственные за выполнение указанных ролей.

8.11. Требования к организации обеспечения непрерывности бизнеса и его восстановления после прерываний

8.11.1. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры учета информационных активов или типов информационных активов, существенных для обеспечения непрерывности бизнеса организации БС РФ.

8.11.2. В организации БС РФ должны быть установлены требования по обеспечению ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания, в том числе требования к мероприятиям по восстановлению необходимой информации, программного обеспечения, технических средств, а также каналов связи.

8.11.3. Должен быть определен план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания. План должен содержать инструкции и порядок действий работников организации БС РФ по восстановлению бизнеса. В частности, в состав плана должны быть включены:

- условия активации плана;
- действия, которые должны быть предприняты после инцидента ИБ;
- процедуры восстановления;
- процедуры тестирования и проверки плана;
- план обучения и повышения осведомленности работников организации БС РФ;
- обязанности работников организации с указанием ответственных за выполнение каждого из положений плана.

8.11.4. Разработка планов обеспечения непрерывности бизнеса и его восстановления после прерывания должна основываться на результатах оценки рисков нарушения ИБ организации БС РФ применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

8.11.5. В организации БС РФ должны применяться защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

Применение защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания должно основываться на соответствующих требованиях по обеспечению ИБ.

8.11.6. План обеспечения непрерывности бизнеса и его восстановления после прерывания должен быть согласован с существующими в организации процедурами обработки инцидентов ИБ.

8.11.7. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры периодического тестирования плана обеспечения непрерывности бизнеса и его восстановления после прерывания. По результатам тестирования при необходимости проводится соответствующая корректировка плана. Сценарий тестирования должен быть составлен с учетом существующей в организации БС РФ модели угроз и нарушителей, а также результатов оценки рисков.

8.11.8. В организации БС РФ должна быть реализована программа обучения и повышения осведомленности работников в области обеспечения непрерывности бизнеса и его восстановления после прерываний.

8.11.9. В организации БС РФ должны быть определены роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания и назначены ответственные за выполнение указанных ролей.

8.12. Требования к мониторингу информационной безопасности и контролю защитных мер

8.12.1. Должны быть определены, выполняться и регистрироваться процедуры мониторинга ИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Выполнение указанных процедур должно организовываться службой ИБ, охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ.

8.12.2. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры сбора и хранения информации о действиях работников организации БС РФ, событиях и параметрах, имеющих отношение к функционированию защитных мер.

8.12.3. Информация обо всех инцидентах, выявленных в процессе мониторинга ИБ и контроля защитных мер, должна быть учтена в рамках выполнения процедур хранения информации об инцидентах ИБ.

8.12.4. Процедуры мониторинга ИБ и контроля защитных мер должны подвергаться регулярным, регистрируемым пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ.

8.12.5. В организации БС РФ должны быть определены роли, связанные с выполнением процедур мониторинга ИБ и контроля защитных мер, а также пересмотром указанных процедур, и назначены ответственные за выполнение указанных ролей.

8.13. Требования к проведению самооценки информационной безопасности

8.13.1. Самооценка ИБ проводится собственными силами и по инициативе руководства организации БС РФ.

8.13.2. Самооценка ИБ должна проводиться в соответствии со стандартом Банка России СТО БР ИББС-1.2 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”. Порядок проведения самооценки ИБ рекомендуется организовывать 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”.

8.13.3. Должна быть установлена и реализована 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.

8.13.4. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры:

— формирования, сбора и хранения свидетельств самооценки ИБ;
— соблюдения периодичности проведения самооценки ИБ;
— хранения и распространения результатов самооценки ИБ.

8.13.5. Для каждой проводимой в организации БС РФ самооценки ИБ необходимо установить план проведения самооценки, определяющий:

— цель самооценки ИБ;
— объекты и деятельность, подвергающиеся самооценке ИБ;
— порядок и сроки выполнения мероприятий самооценки ИБ;
— распределение ролей среди работников организации БС, связанных с проведением самооценки ИБ.

8.13.6. По результатам проведения самооценок ИБ должны быть подготовлены отчеты. Результаты самооценок ИБ, а также соответствующие отчеты должны быть доведены до руководства организации БС РФ.

8.13.7. В организации БС РФ должны быть определены роли, связанные с выполнением программы самооценок ИБ, и назначены ответственные за выполнение указанных ролей.

8.14. Требования к проведению аудита информационной безопасности

8.14.1. Аудит ИБ организации БС РФ должен проводиться в соответствии с требованиями стандартов Банка России СТО БР ИББС-1.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности” и СТО БР ИББС-1.2 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”.

8.14.2. Должна быть установлена и реализована 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.

8.14.3. Для каждого проводимого в организации БС РФ аудита ИБ необходимо установить 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;
— распределение ресурсов при проведении аудита.

8.14.4. В организации БС РФ должны быть оформлены договоры с аудиторскими организациями, а также установлены процедуры:

— хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;
— взаимодействия с аудиторской организацией в процессе проведения аудита ИБ;

— взаимодействия аудиторской группы и руководства, позволяющего представителям аудиторской группы при необходимости непосредственно обращаться к руководству;
— организации опроса работников;
— организации наблюдения за деятельностью работников организации БС РФ со стороны представителей аудиторской организации.

8.14.5. По результатам проведения аудита должны быть подготовлены отчеты. Результаты аудитов, а также соответствующие отчеты должны быть доведены до руководства.

8.14.6. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности отчетов аудитов.

8.14.7. В организации БС РФ должны быть определены роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов, и назначены ответственные за выполнение указанных ролей.

8.15. Требования к анализу функционирования системы обеспечения информационной безопасности

8.15.1. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры анализа функционирования СОИБ, использующие в том числе:
— результаты мониторинга ИБ и контроля защитных мер;
— сведения об инцидентах ИБ;
— результаты проведения аудитов ИБ, самооценок ИБ;
— данные об угрозах, возможных нарушителях и уязвимостях ИБ;
— данные об изменениях внутри организации БС РФ, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации БС РФ;
— данные об изменениях вне организации БС РФ, например, данные об изменениях в законодательстве РФ, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах организации.

8.15.2. Анализ функционирования СОИБ должен включать в том числе:
— анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации БС РФ, требованиям законодательства РФ, требованиям стандартов Банка России, в частности требованиям настоящего стандарта, контрактным требованиям организации;
— анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в организации БС РФ, требованиям политик ИБ организации БС РФ;
— оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска, а также оценку адекватности модели угроз организации БС РФ существующим угрозам ИБ;
— проверку адекватности используемых мер защиты требованиям внутренних документов организации БС РФ и результатам оценки рисков;
— анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании мер защиты.

8.15.3. В организации БС РФ должны быть определены роли, связанные с процедурами анализа функционирования СОИБ, и назначены ответственные за выполнение указанных ролей.

8.16. Требования к анализу системы обеспечения информационной безопасности со стороны руководства организации банковской системы Российской Федерации

8.16.1. В организации БС РФ должен быть установлен перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ. В частности, в указанный перечень документов должны входить:
— отчеты с результатами мониторинга ИБ и контроля защитных мер;
— отчеты с результатами анализа функционирования СОИБ;
— отчеты с результатами аудитов ИБ;
— отчеты с результатами самооценок ИБ;
— документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;

— документы, содержащие информацию о новых, выявленных уязвимостях и угрозах ИБ;
— документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
— документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве РФ и (или) в положениях стандартов Банка России;
— документы, содержащие информацию по выявленным инцидентам ИБ;
— документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например выполнение планов обработки рисков;
— документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

8.16.2. В организации БС РФ должен быть установлен план выполнения деятельности по контролю и анализу СОИБ. В частности, указанный план должен содержать положения по проведению совещаний на уровне руководства, на которых в том числе производится поиск и анализ проблем ИБ, влияющих на бизнес организации БС РФ.

8.16.3. В организации БС РФ должны быть определены роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством, и назначены ответственные за выполнение указанных ролей.

8.17. Требования к принятию решений по тактическим улучшениям системы обеспечения информационной безопасности[1]

8.17.1. Для принятия решений, связанных с тактическими улучшениями СОИБ, необходимо рассмотреть, среди прочего, результаты:
— аудитов ИБ;
— самооценок ИБ;
— мониторинга ИБ и контроля защитных мер;
— анализа функционирования СОИБ;
— обработки инцидентов ИБ;
— выявления новых угроз и уязвимостей ИБ;
— оценки рисков;
— анализа перечня защитных мер, возможных для применения;
— стратегических улучшений СОИБ;
— анализа СОИБ со стороны руководства;
— анализа успешных практик в области ИБ (собственных или других организаций).

8.17.2. Решения по тактическим улучшениям СОИБ должны быть зафиксированы и содержать либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо должны быть указаны направления тактических улучшений СОИБ в виде корректирующих или превентивных действий, например:
— пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;
— пересмотр процедур эксплуатации отдельных видов защитных мер;
— пересмотр процедур обнаружения и обработки инцидентов;
— уточнение описи информационных активов;
— пересмотр программы обучения и повышения осведомленности персонала;
— пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;
— пересмотр планов обработки рисков;
— вынесение санкций в отношении персонала;
— пересмотр процедур мониторинга ИБ и контроля защитных мер;
— пересмотр программ аудитов;
— корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;
— ввод новых или замена используемых защитных мер.

8.17.3. Деятельность по реализации тактических улучшений должна регистрироваться. Должны быть установлены планы реализации тактических улучшений СОИБ и документы, в которых фиксируются результаты выполнения указанных планов.

---

[1] К тактическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром отдельных процедур выполнения деятельности в рамках СОИБ организации БС РФ и не требующие пересмотра политики ИБ и частных политик ИБ организации БС РФ. Как правило, тактические улучшения СОИБ не требуют выполнения деятельности в рамках этапа “планирование” СМИБ.

8.17.4. Деятельность, связанная с реализацией тактических улучшений СОИБ, должна быть санкционирована и контролироваться руководством службы ИБ организации БС РФ.

8.17.5. Должны быть определены, выполняться, регистрироваться и контролироваться 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 по обеспечению ИБ.

8.17.6. В случаях принятия решений по тактическим улучшениям СОИБ должны быть установлены роли и назначены ответственные за их реализацию.

8.18. Требования к принятию решений по стратегическим улучшениям системы обеспечения информационной безопасности[1]

8.18.1. Для принятия решений, связанных со стратегическими улучшениями СОИБ, необходимо рассмотреть, среди прочего, результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга ИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых информационных активов организации БС РФ или их типов;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- пересмотра основных рисков ИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций), а также изменения:
- в законодательстве РФ;
- в нормативных актах Банка России, в частности требованиях настоящего стандарта;
- интересов, целей и задач бизнеса организации БС РФ;
- контрактных обязательств организации БС РФ.

8.18.2. Решения по стратегическим улучшениям СОИБ должны быть зафиксированы и содержать либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо указывать направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например:

- уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ или частных политик ИБ организации БС РФ;
- изменение в области действия СОИБ;
- пересмотр моделей угроз и нарушителей;
- изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ.

8.18.3. Вся деятельность по реализации стратегических улучшений должна регистрироваться. Должны быть установлены планы реализации стратегических улучшений СОИБ и документы, в которых фиксируются результаты выполнения указанных планов.

8.18.4. Деятельность, связанная с реализацией стратегических улучшений СОИБ, должна быть согласована службой ИБ, санкционирована и контролироваться руководством организации БС РФ.

8.18.5. В случае стратегических улучшений СОИБ должна быть выполнена деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых мер защиты и соответствующих внутренних документов. В частности необходимо выполнить:

- выработку планов тактических улучшений СОИБ;
- уточнение планов обработки рисков;
- уточнение программы внедрения защитных мер;
- уточнение процедур использования защитных мер.

8.18.6. Должны быть определены, выполняться, регистрироваться и контролироваться 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 по обеспечению ИБ.

---

[1] К стратегическим улучшениям СОИБ следует относить корректирующие или превентивные действия, связанные с пересмотром политики ИБ и частных политик ИБ организации БС РФ, с последующим выполнением соответствующих тактических улучшений СОИБ. Стратегические улучшения СОИБ всегда требуют выполнения деятельности в рамках этапа “планирование” СМИБ.

8.18.7. В случаях принятия решений по стратегическим улучшениям СОИБ должны быть установлены роли и назначены ответственные за их реализацию.

9. Проверка и оценка информационной безопасности организаций банковской системы Российской Федерации

9.1. Проверка и оценка ИБ организаций БС РФ проводится путем выполнения следующих процессов:

— мониторинга ИБ и контроля защитных мер;
— самооценки ИБ;
— аудита ИБ;
— анализа функционирования СОИБ (в том числе со стороны руководства).

Указанные процессы являются частью группы процессов “проверка” СМИБ, требования к которым приведены в разделе 8 настоящего стандарта.

9.2. Основными целями мониторинга ИБ и контроля защитных мер в организации БС РФ являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели. Такими целями анализа могут быть:

— контроль за реализацией положений внутренних документов по обеспечению ИБ в организации БС РФ;
— выявление нештатных, в том числе злоумышленных, действий в АБС организации;
— выявление инцидентов ИБ.

Мониторинг и контроль защитных мер проводится персоналом организации БС РФ, ответственным за ИБ.

Требования к проведению мониторинга и контроля защитных мер в организации БС РФ определены в подразделе 8.12 настоящего стандарта.

9.3. При подготовке к аудиту ИБ рекомендуется проведение самооценки ИБ.

9.4. Аудит ИБ, проводимый внешними по отношению к организации БС РФ независимыми проверяющими организациями, является одной из форм проверки и оценки (контроля) выполнения организацией БС РФ требований настоящего стандарта.

Аудит ИБ проводится как для собственных целей самой организации БС РФ, так и с целью повышения доверия к ней со стороны других организаций.

В качестве проверяющих организаций рекомендуется привлекать организации, имеющие квалификацию и опыт проведения оценки соответствия ИБ требованиям настоящего стандарта.

9.5. Анализ функционирования СОИБ проводится персоналом организации БС РФ, ответственным за обеспечение ИБ, а также руководством, в том числе на основании подготовленных для руководства документов (данных).

Основными целями проведения анализа функционирования СОИБ являются:

— оценка эффективности СОИБ;
— оценка соответствия СОИБ требованиям законодательства РФ и стандартов Банка России;
— оценка соответствия СОИБ существующим и возможным угрозам ИБ;
— оценка следования принципам ИБ и выполнения требований по обеспечению ИБ, закрепленным в политике ИБ организации БС РФ, а также в иных внутренних документах организации БС РФ.

Результаты, полученные в ходе анализа функционирования СОИБ, являются среди прочего, основой для совершенствования СОИБ.

9.6. В настоящем стандарте требование получения лицензии на деятельность по технической защите конфиденциальной информации (информации ограниченного доступа) при проведении мероприятий по обеспечению безопасности в специальных ИСПДн для собственных нужд организаций БС РФ, а также требование проведения аттестации ИСПДн не устанавливаются. В случае введения в действие стандарта в организации БС РФ указанные требования не являются обязательными при проведении комплекса мероприятий по обеспечению безопасности персональных данных в ИСПДн организаций БС РФ.

9.7. Получение организацией БС РФ лицензии ФСБ России — в соответствии с требованиями законодательства РФ.

9.8. Оценка соответствия ИБ в виде аудита ИБ или самооценки ИБ проводится организацией БС РФ не реже одного раза в два года.

Библиография

1. Федеральный закон от 1 декабря 1990 года № 395-1 “О банках и банковской деятельности”.
2. Федеральный закон от 10 июля 2002 года № 86-ФЗ “О Центральном Банке Российской Федерации (Банке России)”.
3. Федеральный закон от 27 декабря 2002 года № 184-ФЗ “О техническом регулировании”.
4. Федеральный закон от 27 июля 2006 года № 149-ФЗ “Об информации, информационных технологиях и о защите информации”.
5. ГОСТ Р ИСО 9001-2008 Система менеджмента качества. Требования.
6. ISO/IEC IS 27001:2013 Information technology. Security techniques. Information security management systems. Requirements.
7. Положение Банка России от 9 июня 2012 года № 382-П “О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств” в редакции Указания Банка России от 5 июня 2013 года № 3007-У.
8. Федеральный закон от 27 июля 2006 года № 152-ФЗ “О персональных данных”.
9. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”.
10. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 “Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных”.

Ключевые слова: банковская система Российской Федерации, система менеджмента информационной безопасности, политика информационной безопасности.

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Дата введения: 2014-06-01

Издание официальное

Москва
2014

Предисловие

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

2. ВЗАМЕН СТО БР ИББС-1.2-2010.

Содержание

Введение ... 52
1. Область применения ... 53
2. Нормативные ссылки ... 53
3. Термины и определения ... 53
4. Обозначения и сокращения ... 53
5. Общие положения ... 54
6. Показатели информационной безопасности. Способы оценивания показателей ... 55
7. Оценка текущего уровня информационной безопасности организации банковской системы Российской Федерации ... 57
8. Оценка менеджмента информационной безопасности организации банковской системы Российской Федерации ... 60
9. Оценка уровня осознания информационной безопасности организации банковской системы Российской Федерации ... 61
10. Правила определения корректирующих коэффициентов ... 63
11. Определение уровня соответствия информационной безопасности организации банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Отображение оценок ... 63

Приложение А (обязательное). Показатели информационной безопасности ... 66

Приложение Б (обязательное). Форма листов для сбора свидетельств аудита ИБ ... 128

Приложение В (обязательное). Таблица соответствия частных показателей и требований к обеспечению защиты информации при осуществлении переводов денежных средств, указанных в приложении 2 к Положению Банка России от 9 июня 2012 года № 382-П и учитываемых при оценивании частных показателей ... 129

СТО БР ИББС-1.2-2014

Введение

Стандартом Банка России СТО БР ИББС-1.0-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” с целью проверки уровня информационной безопасности (ИБ) как самого Банка России, так и организаций банковской системы (БС) Российской Федерации (РФ) определено требование проведения регулярного аудита ИБ и самооценки ИБ.

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

СТО БР ИББС-1.2-2014

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Дата введения: 2014-06-01

1. Область применения

Настоящий стандарт распространяется на организации БС РФ, а также на организации, проводящие оценку соответствия ИБ организации БС РФ требованиям стандарта Банка России СТО БР ИББС-1.0-2014 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0).

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

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

2. Нормативные ссылки

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

3. Термины и определения

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

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

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

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

4. Обозначения и сокращения

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

НСД — несанкционированный доступ;
НРД — нерегламентированные действия в рамках предоставленных полномочий;
РФ — Российская Федерация;
СКЗИ — средство криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
СИБ — система информационной безопасности;
СОИБ — система обеспечения информационной безопасности;
ЭВМ — электронная вычислительная машина;
ЭП — электронная подпись;
EV_1 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "текущий уровень ИБ организации";
EV_2 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "менеджмент ИБ организации";
EV_3 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "уровень осознания ИБ организации";
$EV_{ООПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных;
$EV^1_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;
$EV^2_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;
$EV_{БИТП}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс;
$EV_{БПТП}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс;
EV_{Mi} — оценка степени выполнения требований СТО БР ИББС-1.0 для группового показателя;
EV_{Mij} — оценка степени выполнения требований СТО БР ИББС-1.0 для частного показателя;
i — номер группового показателя;
j — номер частного показателя;
M_{ij} — обозначение частного показателя;
R — итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0.

5. Общие положения

5.1. Целью настоящей методики является стандартизация подходов и способов оценки соответствия обеспечения ИБ организации БС РФ требованиям СТО БР ИББС-1.0 по направлениям оценки:

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

5.2. Задачами настоящей методики являются:

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

6. Показатели информационной безопасности. Способы оценивания показателей

6.1. Для оценки степени соответствия обеспечения ИБ организации требованиям СТО БР ИББС-1.0 используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ организации, менеджмента и уровня осознания ИБ. Оценки групповых показателей (EV_{Mi}) используются для получения оценки по направлениям (EV_1,EV_2 и EV_3). Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки (EV_{Mij}), которые затем формируют оценки EV_{Mi} групповых показателей.

Приложение А содержит формы, предназначенные для заполнения при проведении оценки. Каждая из форм содержит групповой показатель ИБ, входящие в него частные показатели ИБ.

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

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

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

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

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

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

Если частный показатель предназначен для оценки требований, которые не относятся к деятельности организации или на момент оценки не являются актуальными для организации, что зафиксировано документами организации, то данный частный показатель определяется как неоцениваемый (должна быть заполнена графа “н/о” — нет оценки) и не учитывается в формировании дальнейших результатов оценки.

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

— “да” — оценке присваивается значение, равное единице;
— “нет” — частный показатель определяется как неоцениваемый (должна быть заполнена графа “н/о” — нет оценки) и не учитывается в формировании дальнейших результатов оценки.

6.7. При проведении оценки частных показателей, для которых оценивается как степень их установления (определения) в организации БС РФ, так и степень выполнения (частный показатель категории проверки 1), используется следующий общий подход:

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

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не установлены (определены) во внутренних документах проверяемой организации
0,25	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации, но не выполняются
0,5	Требования частного показателя ИБ установлены (определены) во внутренних документах проверяемой организации, но выполняются в неполном объеме

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

6.8. При проведении оценки частных показателей, для которых оценивается только степень документированности (частный показатель категории проверки 2), используется следующий общий подход:

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

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования частного показателя ИБ не установлены во внутренних документах проверяемой организации
1	Требования частного показателя ИБ полностью установлены во внутренних документах проверяемой организации

6.9. При проведении оценки частных показателей, для которых оценивается только степень выполнения (частный показатель категории проверки 3), используется следующий общий подход:

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

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

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

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

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

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

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

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

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

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

6.13. Если в рамках группового показателя все входящие в него частные показатели определены как неоцениваемые, указанный групповой показатель также определяется как неоцениваемый и не учитывается в формировании дальнейших результатов оценки. В этом случае групповой показатель не учитывается в формулах расчета для $EV_{БИТП}$, $EV_{БПТП}$, $EV_{ООПД}$, $EV^{1}_{ОЗПД}$, $EV^{2}_{ОЗПД}$, EV_1, EV_2 и EV_3 (см. разделы 7, 8, 9) с соответствующей корректировкой в формулах расчета количества оцениваемых групповых показателей. Оценки для таких групповых показателей не отображаются на круговой диаграмме (см. раздел 11).

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

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

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

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

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

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

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M8	Обеспечение ИБ банковских информационных технологических процессов	п. 7.9
M9	Общие требования по обработке персональных данных в организации БС РФ	п. 7.10
M10	Общие требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются персональные данные	п. 7.11

7.3. Частные показатели по направлению оценки “текущий уровень ИБ организации” отражают отдельные требования ИБ СТО БР ИББС-1.0, предъявляемые по каждой из областей. Частные показатели по направлению оценки “текущий уровень ИБ организации” (показатели M1÷M10) в приложении А.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$EV_{ООПД} = k_{ООПД} \cdot EV_{M9},$$

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

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

7.10. Оценка EV_1 отображается на круговой диаграмме (см. раздел 11) в секторах с 1-го по 10-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению EV_1.

8. Оценка менеджмента информационной безопасности организации банковской системы Российской Федерации

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

- организация и функционирование службы ИБ организации БС РФ;
- определение/коррекция области действия СОИБ;
- выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ;
- разработка планов обработки рисков нарушения ИБ;
- разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- принятие руководством организации БС РФ решений о реализации и эксплуатации СОИБ;
- организация реализации планов обработки рисков нарушения ИБ;
- разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ;
- организация обнаружения и реагирования на инциденты ИБ;
- организация обеспечения непрерывности бизнеса и его восстановления после прерываний;
- мониторинг ИБ и контроль защитных мер;
- проведение самооценки ИБ;
- проведение внешнего аудита ИБ;
- анализ функционирования СОИБ;
- анализ СОИБ со стороны руководства организации БС РФ;
- принятие решений по тактическим улучшениям СОИБ;
- принятие решений по стратегическим улучшениям СОИБ.

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

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

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M11	Организация и функционирование службы ИБ организации БС РФ	п. 8.2
M12	Определение/коррекция области действия СОИБ	п. 8.3
M13	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки рисков нарушения ИБ	п. 8.4
M14	Разработка планов обработки рисков нарушения ИБ	п. 8.5
M15	Разработка/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ	п. 8.6
M16	Принятие руководством организации БС РФ решений о реализации и эксплуатации СОИБ	п. 8.7
M17	Организация реализации планов внедрения СОИБ	п. 8.8
M18	Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ	п. 8.9
M19	Организация обнаружения и реагирования на инциденты ИБ	п. 8.10
M20	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний	п. 8.11
M21	Мониторинг ИБ и контроль защитных мер	п. 8.12

Обозначение группового показателя ИБ	Наименование группового показателя ИБ	Структурный элемент СТО БР ИББС-1.0
M22	Проведение самооценки ИБ	п. 8.13
M23	Проведение аудита ИБ	п. 8.14
M24	Анализ функционирования СОИБ	п. 8.15
M25	Анализ СОИБ со стороны руководства организации БС РФ	п. 8.16
M26	Принятие решений по тактическим улучшениям СОИБ	п. 8.17
M27	Принятие решений по стратегическим улучшениям СОИБ	п. 8.18

8.3. Частные показатели по направлению оценки “менеджмент ИБ организации” отражают отдельные требования ИБ СТО БР ИББС-1.0, предъявляемые по каждой из областей. Частные показатели по направлению оценки “менеджмент ИБ организации” (показатели M11÷M27) приведены в приложении А.

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

8.5. Оценивание частных показателей в рамках групповых показателей M11÷M27 следует осуществлять с учетом результатов оценки выполнения организацией требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 9 июня 2012 года № 382-П и используемых для вычисления обобщающего показателя $EV2_{ПС}$, установленного Положением Банка России от 9 июня 2012 года № 382-П.

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

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

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

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

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

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

8.8. Оценка EV_2 отображается на круговой диаграмме (см. раздел 11) в секторах с 11-го по 27-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению EV_2.

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

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

— деятельность руководства организации БС РФ по поддержке функционирования службы ИБ организации;

— деятельность руководства организации БС РФ по принятию решений о реализации и эксплуатации СОИБ;
— деятельность руководства организации БС РФ по поддержке планирования СОИБ;
— деятельность руководства организации БС РФ по поддержке реализации СОИБ;
— деятельность руководства организации БС РФ по поддержке проверки СОИБ;
— деятельность руководства организации БС РФ по анализу СОИБ;
— деятельность руководства организации БС РФ по поддержке совершенствования СОИБ.

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

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

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

9.3. Частные показатели по направлению оценки "уровень осознания ИБ организации" отражают отдельные требования СТО БР ИББС-1.0 к СМИБ организации, относящиеся к деятельности руководства организации. Частные показатели по направлению оценки "уровень осознания ИБ организации" (показатели M28÷M34) приведены в приложении А.

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

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

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

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

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

9.6. Оценки EV_{Mi}, полученные в результате оценивания групповых показателей ИБ M28÷M34, отображаются на круговой диаграмме (см. раздел 11) в секторах с 28-го по 34-й дугами, отстающими от центра круговой диаграммы на величину, соответствующую значению этих оценок.

9.7. Оценка EV_3 отображается на круговой диаграмме (см. раздел 11) в секторах с 28-го по 34-й дугой, отстающей от центра круговой диаграммы на величину, соответствующую значению EV_3.

10. Правила определения корректирующих коэффициентов

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

Таблица 7. Правила определения корректирующих коэффициентов

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

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

11.1. Если оценка EV_1, EV_2 или EV_3 лежит в интервале от 0 до 0,25, то данному направлению оценки присваивается нулевой уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка EV_1, EV_2 или EV_3 лежит в интервале от 0,25 до 0,5, то данному направлению оценки присваивается первый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка EV_1, EV_2 или EV_3 лежит в интервале от 0,5 до 0,7, то данному направлению оценки присваивается второй уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка EV_1, EV_2 или EV_3 лежит в интервале от 0,7 до 0,85, то данному направлению оценки присваивается третий уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка EV_1, EV_2 или EV_3 лежит в интервале от 0,85 до 0,95, то данному направлению оценки присваивается четвертый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

Если оценка EV_1, EV_2 или EV_3 лежит в интервале от 0,95 до 1 включительно, то данному направлению оценки присваивается пятый уровень соответствия ИБ требованиям СТО БР ИББС-1.0.

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

— оценки уровня осознания ИБ организации (EV_3);
— оценки менеджмента ИБ организации (EV_2);
— оценки текущего уровня ИБ организации (EV_1).

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

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

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

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

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

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

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

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

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

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

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

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

Нулевому уровню соответствует круг до окружности радиусом 0,25.

11.6. По результатам проведения оценки соответствия формируется документ — "Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2014".

"Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2014" формируется на основе:

— аудиторского заключения в случае проведения оценки соответствия внешней организацией;

— отчета самооценки в случае проведения оценки соответствия силами организации БС РФ.

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

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

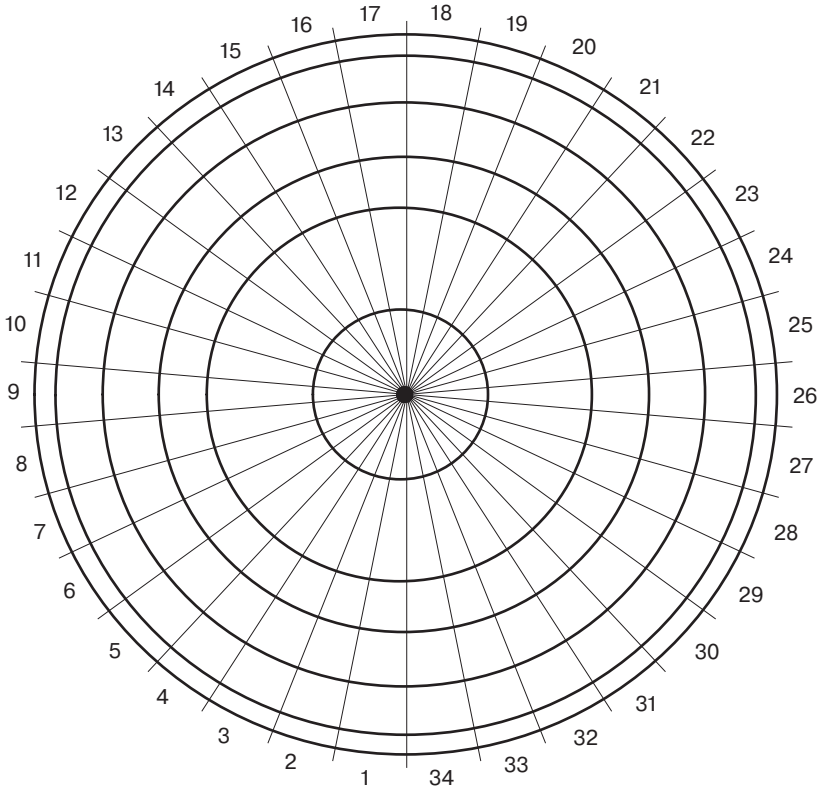
$EV^{1}_{озпд}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации;

$EV_{м6}$ — оценка группового показателя М6 "Обеспечение информационной безопасности при использовании средств криптографической защиты информации", применительно к банковскому технологическому процессу, в рамках которого обрабатываются персональные данные (оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных при использовании средств криптографической защиты информации);

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

С целью направления "Подтверждения соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2014" регуляторам, осуществляющим надзор за выполнением законодательства в области персональных данных, данный документ следует составлять в пяти экземплярах, один из которых предназначен для использования в организации БС РФ.

Рисунок 1. Круговая диаграмма для отображения результатов оценивания



Приложение А
(обязательное)

Показатели информационной безопасности

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М1.12	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры приема на работу, влияющую на обеспечение ИБ, включающие: — проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов; — проверку в части профессиональных навыков и оценку профессиональной пригодности?	обязательный	категория 1						
М1.13	Предусматривают ли указанные в частном показателе М1.12 процедуры фиксацию результатов проводимых проверок?	обязательный	категория 2						
М1.14	Определены ли, выполняются ли и регистрируются, выполняются и регистрируются ли в организации БС РФ процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников?	рекомендуемый	категория 1						
М1.15	Предусматривают ли указанные в частном показателе М1.14 процедуры фиксацию результатов проводимых проверок?	рекомендуемый	категория 2						
М1.16	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры внеплановой проверки работников при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии?	рекомендуемый	категория 1						
М1.17	Предусматривают ли указанные в частном показателе М1.16 процедуры фиксацию результатов проводимых проверок?	рекомендуемый	категория 2						
М1.18	Обязаны ли все работники организации БС РФ давать письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов?	обязательный	категория 3						
М1.19	Регламентируются ли положениями, включенными в договоры (соглашения) с внешними организациями и клиентами, требования по ИБ?	обязательный	категория 2						
М1.20	Определены ли в трудовых контрактах (соглашениях, договорах) и (или) должностных инструкциях обязанности персонала по выполнению требований ИБ?	обязательный	категория 2						
М1.21	Приравнивается ли невыполнение работниками организации БС РФ требований ИБ к невыполнению должностных обязанностей и приводит ли как минимум к дисциплинарной ответственности?	обязательный	категория 1						
Итоговая оценка группового показателя М1									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М2.1	Рассматриваются ли в части вопросов обеспечения ИБ следующие стадии модели ЖЦ АБС: — разработка технических заданий; — проектирование; — создание и тестирование; —приемка и ввод в действие; — эксплуатация; — сопровождение и модернизации; — снятие с эксплуатации?	обязательный	категория 1						
М2.2	Осуществляется ли выполнение работ на всех стадиях жизненного цикла АБС в части вопросов обеспечения ИБ по согласованию и под контролем службы ИБ?	обязательный	категория 1						
М2.3	Имеют ли организации, привлекаемые на договорной основе для обеспечения ИБ на стадиях ЖЦ АБС, лицензии на деятельность по технической защите конфиденциальной информации в соответствии с законодательством РФ?	обязательный	категория 3						
М2.4	Включаются ли требования к обеспечению информационной безопасности, установленные и используемые организацией БС РФ для обеспечения ИБ в рамках технологических процессов организации БС РФ, в технические задания на разработку или модернизацию АБС?	обязательный	категория 3						
М2.5	Обеспечивается ли в организации БС РФ реализация запрета использования защищаемой информации в качестве тестовых данных, анонимность данных и контроль адекватности предоставления и разграничения доступа на стадии создания и тестирования АБС и (или) их компонентов?	обязательный	категория 1						
М2.6	Снабжены ли эксплуатируемые АБС и (или) их компоненты документацией, содержащей описание реализованных в АБС защитных мер, в том числе описание состава и требований к реализации организационных защитных мер, состава и требований к эксплуатации технических защитных мер?	обязательный	категория 2						
М2.7	Проводится ли организацией БС РФ анализ принятия разработчиком АБС защитных мер, направленных на обеспечение безопасности разработки АБС и безопасности ее поставки?	рекомендуемый	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М2.8	Реализуется ли при взаимодействии организации БС РФ с разработчиком АБС и их компонентов одна из трех альтернатив: 1) в договор (контракт) о разработке АБС или поставке готовых АБС и их компонентов включаются положения по сопровождению поставляемых изделий на весь срок их службы; 2) организация БС РФ приобретает полный комплект документации, обеспечивающий возможность сопровождения АБС и их компонентов без участия разработчика; 3) руководство организации БС РФ оценивает и фиксирует допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов?	обязательный	категория 3						
М2.9	Учитывается ли при разработке технических заданий на системы дистанционного банковского обслуживания, что защита данных должна обеспечиваться в условиях: — попыток несанкционированного доступа к информации анонимных, неавторизованных злоумышленников с использованием сетей общего пользования; — возможности ошибок авторизованных пользователей систем; — возможности ненамеренного или неадекватного использования защищаемой информации авторизованными пользователями?	обязательный	категория 3						
М2.10	Определены ли в организации БС РФ, выполняются ли и регистрируются ли на стадии эксплуатации АБС процедуры: — контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер, в том числе контроль реализации организационных защитных мер, контроль состава и параметров настройки применяемых технических защитных мер; — контроля отсутствия уязвимостей в оборудовании и программном обеспечении АБС; — контроля внесения изменений в параметры настройки АБС и применяемых технических защитных мер; — контроля необходимого обновления программного обеспечения АБС, включая программное обеспечение технических защитных мер?	обязательный	категория 1						
М2.11	Определены ли, выполняются ли, регистрируются ли и контролируется ли на стадии эксплуатации АБС процедуры, необходимые для обеспечения восстановления всех реализованных функций по обеспечению ИБ?	обязательный	категория 1						
М2.12	Определены ли, выполняются ли и регистрируются ли на стадии эксплуатации АБС процедуры контроля состава устанавливаемого и (или) используемого ПО АБС?	обязательный	категория 1						
М2.13	Выделены ли и назначены ли роли, связанные с эксплуатацией и контролем эксплуатации АБС и применяемых технических защитных мер, в том числе с внесением изменений в параметры их настройки?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М2.14	Определены ли, выполняются ли для всех АБС процедуры контроля ее эксплуатации со стороны службы ИБ, регистрируется ли процесс и результаты их выполнения?	обязательный	категория 1						
М2.15	Определены ли, выполняются ли и контролируются ли на стадии эксплуатации АБС процедуры, необходимые для обеспечения сохранности носителей защищаемой информации?	обязательный	категория 1						
М2.16	Определены ли, выполняются ли и регистрируются ли в организации БС РФ на стадии сопровождения (модернизации) АБС процедуры контроля, обеспечивающие защиту от: — умышленного несанкционированного раскрытия, модификации или уничтожения информации; — неумышленной модификации, раскрытия или уничтожения информации; — отказа в обслуживании или ухудшения обслуживания?	обязательный	категория 1						
М2.17	Определены ли, выполняются ли и регистрируются ли на стадии сопровождения (модернизации) АБС, отнесенных решением организацией БС РФ к критичным, в том числе АБС, задействованных в реализации банковского платежного технологического процесса, и в ИСПДн, процедуры фиксации внесенных изменений?	обязательный	категория 1						
М2.18	Определены ли, выполняются ли и регистрируются ли на стадии сопровождения (модернизации) АБС, отнесенных решением организацией БС РФ к критичным, в том числе АБС, задействованных в реализации банковского платежного технологического процесса, и в ИСПДн, процедуры проверки функциональности АБС, в том числе применяемых мер защиты информации, после внесения изменений?	обязательный	категория 1						
М2.19	Определены ли, выполняются ли, регулируются ли и выполняются ли на стадии снятия с эксплуатации процедуры, обеспечивающие удаление информации с использованием алгоритмов и (или) методов, обеспечивающих невозможность восстановления удаленной информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой техническими защитными мерами, из постоянной памяти АБС и с внешних носителей (за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены законодательством РФ, нормативными актами Банка России и (или) договорными документами)?	обязательный	категория 1						
Итоговая оценка группового показателя М2									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры выявления, учета и классификации (отнесение к одному из типов) информационных активов?	обязательный	категория 1						
М3.2	Учтены ли и зафиксированы ли права доступа работников и клиентов организации БС РФ к информационным активам и (или) их типам?	обязательный	категория 1						
М3.3	Применяются ли в составе АБС встроенные защитные меры от НСД и НРД?	обязательный	категория 1						
М3.4	Применяются ли в составе АБС сертифицированные по требованиям безопасности информации средства защиты информации?	рекомендуемый	категория 3						
М3.5	Обеспечивается ли защитными мерами от НСД сокрытие вводимых субъектами доступа аутентификационных данных на устройствах отображения информации?	обязательный	категория 3						
М3.6	Препятствует ли размещение устройств отображения информации АБС ее несанкционированному просмотру?	обязательный	категория 3						
М3.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС РФ, и программных процессов (сервисов)?	обязательный	категория 1						
М3.8	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры разграничения доступа к информационным активам на основе ролевого метода с определением для каждой роли полномочий по доступу к информационным активам?	обязательный	категория 1						
М3.9	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления предоставлением/отзывом и блокированием доступа, в том числе доступа, осуществляемого через внешние информационно-телекоммуникационные сети?	обязательный	категория 1						
М3.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры регистрации действий субъектов доступа с обеспечением контроля целостности и защиты данных регистрации?	обязательный	категория 1						
М3.11	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления идентификационными данными, аутентификационными данными и средствами аутентификации?	обязательный	категория 1						
М3.12	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры управления учетными записями субъектов доступа?	обязательный	категория 1						

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М3.35	Осуществляется ли разделение сегментов вычислительных сетей с целью обеспечения независимого выполнения банковских платежных технологических процессов организации БС РФ, а также банковских информационных технологических процессов организации БС РФ разной степени критичности, в том числе банковских информационных технологических процессов, в рамках которых осуществляется обработка персональных данных в ИСПДн?	обязательный	категория 1						
М3.36	Регламентированы ли и контролируются ли процедуры внесения изменений в конфигурацию сетевого оборудования, предусматривающие согласование вносимых изменений со службой ИБ?	обязательный	категория 2						
М3.37	Предоставлен ли работникам службы ИБ доступ к конфигурации сетевого оборудования без возможности внесения изменений?	рекомендуемый	категория 3						
М3.38	Определен ли, выполняется ли, регистрируется ли и контролируется ли порядок доступа к объектам среды информационных активов, в том числе в помещения, в которых размещаются объекты среды информационных активов?	обязательный	категория 1						
М3.39	Обеспечивают ли используемые в организации БС РФ АБС, в том числе системы дистанционного банковского обслуживания, возможность регистрации: — операций с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов; — проводимых транзакций, имеющих финансовые последствия; — операций, связанных с назначением и распределением прав пользователей?	обязательный	категория 3						
М3.40	Определен ли, выполняется ли и контролируется ли в организации БС РФ порядок использования съемных носителей информации?	обязательный	категория 1						
М3.41	Реализованы ли в системах дистанционного банковского обслуживания, используемых в организации БС РФ, защитные меры, обеспечивающие невозможность отказа от авторства проводимых клиентами операций и транзакций?	обязательный	категория 3						
М3.42	Придано ли протоколам операций, выполняемых посредством дистанционного банковского обслуживания, свойство юридической значимости, например, путем внесения соответствующих положений в договоры на дистанционное банковское обслуживание?	обязательный	категория 1						
М3.43	Производится ли при заключении договоров со сторонними организациями юридическое оформление договоренностей, определяющих необходимый уровень взаимодействия в случае выхода инцидента ИБ за рамки отдельной организации?	рекомендуемый	категория 2						

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

Групповой показатель М4 “Обеспечение информационной безопасности средствами антивирусной защиты”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М4.1	Применяются ли на всех автоматизированных рабочих местах и серверах АБС организации БС РФ, если иное не предусмотрено технологическим процессом, средства антивирусной защиты?	обязательный	категория 1						
М4.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС?	обязательный	категория 1						
М4.3	Организовано ли функционирование постоянной антивирусной защиты в автоматическом режиме и автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных?	рекомендуемый	категория 1						
М4.4	Проводится ли антивирусная проверка съемных носителей информации перед их подключением к средствам вычислительной техники, задействованным в рамках осуществления банковских технологических процессов, на специально выделенном автономном средстве вычислительной техники?	рекомендуемый	категория 1						
М4.5	Разработаны ли и введены ли в действие инструкции и рекомендации по антивирусной защите, учитывающие особенности банковских технологических процессов?	обязательный	категория 2						
М4.6	Организована ли в организации БС РФ антивирусная фильтрация всего трафика электронного почтового обмена?	обязательный	категория 3						
М4.7	Организована ли в организации БС РФ эшелонированная централизованная система антивирусной защиты, предусматривающая использование средств антивирусной защиты различных производителей на: — рабочих станциях; — серверном оборудовании, в том числе серверах электронной почты; — технических средствах межсетевого экранирования?	обязательный	категория 1						
М4.8	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов?	обязательный	категория 1						
М4.9	Выполняется ли после установки или изменения программного обеспечения антивирусная проверка?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М4.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать: – необходимые меры по отражению и устранению последствий вирусной атаки; – порядок официального информирования руководства; – порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки)?	обязательный	категория 1						
М4.11	Определены ли, выполняются ли и регистрируются ли процедуры контроля за отключением и обновлением антивирусных средств на всех технических средствах АБС?	обязательный	категория 1						
М4.12	Возложена ли обязанность по выполнению предписанных мер антивирусной защиты на каждого работника организации БС РФ, имеющего доступ к ЭВМ и (или) АБС, а ответственность за выполнение требований по антивирусной защите – на руководителей функциональных подразделений организации БС РФ?	обязательный	категория 3						
Итоговая оценка группового показателя М4									

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М5.13	Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный	категория 3						
М5.14	Регистрируются ли регламентированным образом попытки подмены авторизованного клиента злоумышленником в рамках сеанса работы?	обязательный	категория 1						
М5.15	Все ли операции клиентов в течение сеанса работы с системами дистанционного банковского обслуживания, в том числе операции по переводу денежных средств, выполняются только после выполнения процедур идентификации, аутентификации и авторизации?	обязательный	категория 3						
М5.16	Обеспечивается ли закрытие текущей сессии и повторное выполнение процедур идентификации, аутентификации и авторизации в случаях нарушения или разрыва соединения при работе с системами дистанционного банковского обслуживания?	обязательный	категория 3						
М5.17	Используется ли специализированное клиентское программное обеспечение для доступа пользователей к системам дистанционного банковского обслуживания?	рекомендуемый	категория 3						
М5.18	Определены ли состав и порядок применения мер защиты, применяемых для организации почтового обмена через сеть Интернет?	обязательный	категория 2						
М5.19	Организован ли почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации БС РФ) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски)?	рекомендуемый	категория 3						
М5.20	Осуществляется ли архивирование электронной почты с целью: — контроля информационных потоков, в том числе с целью предотвращение утечек информации; — использования архивов при проведении разбирательств по фактам утечек информации?	обязательный	категория 3						
М5.21	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ правила и процедуры доступа к информации архива и ее изменения, предусматривающие возможность доступа работников службы ИБ к информации архива?	обязательный	категория 1						
М5.22	Не применяется ли в организации БС РФ практика хранения и обработки банковской информации (в т.ч. открытой) на ЭВМ, с помощью которой осуществляется непосредственное взаимодействие с сетью Интернет?	рекомендуемый	категория 3						
М5.23	Всегда ли наличие банковской информации на ЭВМ, с помощью которых осуществляется непосредственное взаимодействие с сетью Интернет, определяется бизнес-целями организации БС РФ и санкционируется ее руководством?	обязательный	категория 3						
М5.24	Определены ли состав и порядок применения мер защиты, применяемых при взаимодействии с сетью Интернет и позволяющие обеспечить противодействие атакам злоумышленников и распространению спама?	обязательный	категория 1						
Итоговая оценка группового показателя М5									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М6.1	Проводится ли применение СКЗИ в организации БС РФ в соответствии с моделью угроз ИБ и моделью нарушителя ИБ, принятыми организацией БС РФ?	обязательный	категория 1						
М6.2	Имеют ли СКЗИ, применяемые для защиты персональных данных, класс не ниже КС2?	обязательный	категория 3						
М6.3	Проводятся ли работы по обеспечению безопасности информации с помощью СКЗИ в соответствии с действующими законодательством, нормативными документами, регламентирующими вопросы эксплуатации СКЗИ, технической документацией на СКЗИ и лицензионными требованиями ФСБ России?	обязательный	категория 1						
М6.4	Утверждена ли частная политика, касающаяся применения СКЗИ в организации БС РФ?	рекомендуемый	категория 2						
М6.5	Допускают ли СКЗИ возможность встраивания в технологические процессы обработки электронных сообщений?	обязательный	категория 3						
М6.6	Обеспечивают ли СКЗИ взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов?	обязательный	категория 3						
М6.7	Обладают ли СКЗИ полным комплектом эксплуатационной документации, предоставляемым разработчиком, включающей описание ключевой системы, правил работы с ней и обоснование необходимого организационно-штатного обеспечения?	обязательный	категория 3						
М6.8	Сертифицированы ли СКЗИ уполномоченным государственным органом или имеют ли СКЗИ разрешение ФСБ России?	обязательный	категория 3						
М6.9	Осуществляется ли установка и ввод в эксплуатацию, а также эксплуатация СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам?	обязательный	категория 3						
М6.10	Поддерживается ли непрерывность процессов протоколирования работы СКЗИ в соответствии с технической документацией на СКЗИ при применении СКЗИ?	обязательный	категория 3						
М6.11	Поддерживается ли непрерывность процессов обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющую собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М6.12	Обеспечивается ли ИБ процессов изготовления криптографических ключей СКЗИ комплексом технологических, организационных, технических и программных мер и средств защиты, предусмотренных технической документацией на СКЗИ?	обязательный	категория 3						
М6.13	Реализованы ли процедуры мониторинга ИБ, регистрирующие все значимые события, состоявшиеся в процессе обмена криптографически защищенными данными, и всех инцидентов ИБ?	рекомендуемый	категория 1						
М6.14	Определен ли руководством на основании указанных в разделе 7.7 СТО БР ИББС-1.0 документов порядок применения СКЗИ, включающий: – порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС; – порядок эксплуатации; – порядок восстановления работоспособности в аварийных случаях; – порядок внесения изменений; – порядок снятия с эксплуатации; – порядок управления ключевой системой; – порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей?	обязательный	категория 1						
М6.15	Самостоятельно ли изготавливаются в организации БС РФ и (или) клиентом организации ключи СКЗИ?	рекомендуемый	категория 3						
М6.16	Регулируются ли заключаемыми договорами отношения, возникающие между организациями и их клиентами?	обязательный	категория 2						
Итоговая оценка группового показателя М6									

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

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

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

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М8.1	Проведена ли в организации БС РФ классификация неплатежной информации?	обязательный	категория 2						
М8.2	Проводится ли классификация неплатежной информации в соответствии со степенью тяжести последствий потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности?	обязательный	категория 3						
М8.3	Определен ли документально набор требований по защите каждого из типов неплатежной информации, полученных в результате классификации?	обязательный	категория 2						
М8.4	Регламентированы (описаны) ли в организации БС РФ банковские информационные технологические процессы?	обязательный	категория 1						
М8.5	Реализованы ли банковские информационные технологические процессы в рамках созданных для этих целей АБС?	обязательный	категория 3						
М8.6	Изолированы ли серверы, офисные ЭВМ и другое оборудование, не входящее в состав АБС, реализующих банковские информационные технологические процессы, от указанных АБС на уровне локальных вычислительных сетей способом, согласованным со службой ИБ?	рекомендуемый	категория 3						
М8.7	Определены ли, выполняются ли и контролируются ли требования к взаимодействию АБС организаций БС РФ с информационными системами сторонних организаций (внешними информационными системами)?	обязательный	категория 1						
Итоговая оценка группового показателя М8									

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

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

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

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М9.48	Обеспечено ли при работе со съемными носителями ПДн регистрация и учет мест хранения материальных носителей ПДн с фиксацией категории обрабатываемых персональных данных (специальные категории ПДн, биометрические ПДн, ПДн, полученные из общедоступных источников, или иные ПДн), включая раздельное хранение ресурсов ПДн, обработка которых осуществляется с различными целями?	обязательный	категория 3						
М9.49	Обеспечено ли при работе со съемными носителями ПДн назначение работников, ответственных за организацию их хранения?	обязательный	категория 3						
М9.50	Обеспечено ли при работе со съемными носителями ПДн установление и выполнение порядка уничтожения (стирания) информации на съемных носителях ПДн?	обязательный	категория 3						
М9.51	Осуществляется ли хранение ПДн в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн?	обязательный	категория 3						
М9.52	Создаются ли и публикуются ли организацией БС РФ общедоступные источники ПДн только для цели выполнения требований законодательства РФ?	обязательный	категория 3						
М9.53	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры публикации ПДн в общедоступных источниках ПДн?	обязательный	категория 1						
М9.54	Осуществляется ли на основании договора поручение обработки ПДн третьему лицу (далее – обработчик)?	обязательный	категория 2						
М9.55	Определен ли в указанном договоре перечень действий (операций) с ПДн, которые будут совершаться обработчиком, и цели обработки?	обязательный	категория 2						
М9.56	Установлена ли в указанном договоре обязанность обработчика обеспечивать безопасность ПДн (в том числе соблюдать конфиденциальность ПДн) при их обработке, не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом, а также должны быть указаны требования по обеспечению безопасности ПДн?	обязательный	категория 2						
М9.57	Получено ли организацией БС РФ согласие субъекта ПДн, если иное не предусмотрено федеральным законом, при поручении обработки персональных данных обработчику?	обязательный	категория 3						
М9.58	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры, выполняемые в случаях необходимости осуществления трансграничной передачи ПДн?	обязательный	категория 1						
М9.59	Назначено ли в организации БС РФ лицо, ответственное за организацию обработки ПДн?	обязательный	категория 3						
М9.60	Установлены ли руководством организации БС РФ полномочия лица, ответственного за организацию обработки ПДн, а также его права и обязанности?	обязательный	категория 2						
Итоговая оценка группового показателя М9									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М10.1	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение и регистрация процедур контроля целостности и обеспечения доверенной загрузки программного обеспечения, в том числе программного обеспечения технических защитных мер, на средствах вычислительной техники, входящих в ИСПДн?	обязательный	категория 1						
М10.2	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение, регистрация и контроль процедур доступа к эксплуатационной документации и архивным файлам, содержащим параметры настройки ИСПДн, в том числе настройки применяемых технических защитных мер?	обязательный	категория 1						
М10.3	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления ПДн?	обязательный	категория 1						
М10.4	Реализуется ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”, определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, в том числе программного обеспечения технических защитных мер, входящего в состав ИСПДн?	обязательный	категория 1						

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М10.10	Реализуются ли в организации БС РФ для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн, установленного Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", в части обеспечения ИБ банковских информационных технологических процессов определение, выполнение, регистрация и контроль процедур доступа к архивам ПДн?	обязательный	категория 1						
М10.11	Реализованы ли в организации БС РФ защита периметров сегментов вычислительной сети, в которых расположена ИСПДн, и контроль информационного взаимодействия между сегментами вычислительных сетей?	обязательный	категория 3						
М10.12	Определены ли и контролируются ли в организации БС РФ правила информационного взаимодействия между ИСПДн с иными АБС?	обязательный	категория 1						
М10.13	Осуществляется ли использование в организации БС РФ в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"?	обязательный	категория 3						
М10.14	Назначен ли для каждой ИСПДн работник организации БС РФ, ответственный за обеспечение безопасности персональных данных в ИСПДн?	обязательный	категория 2						
Итоговая оценка группового показателя М10									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М11.1	Сформирована ли руководством служба ИБ в составе не менее двух человек (назначены ли уполномоченные лица) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный	категория 3						
М11.2	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный	категория 3						
М11.3	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный	категория 3						
М11.4	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый	категория 3						
М11.5	Сформированы ли для организаций БС РФ, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	обязательный	категория 1						
М11.6	Наделена ли служба ИБ полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М11.7	Наделена ли служба ИБ полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации БС РФ?	обязательный	категория 3						
М11.8	Наделена ли служба ИБ полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М11.9	Наделена ли служба ИБ полномочиями определять требования к мерам обеспечения ИБ организации БС РФ?	обязательный	категория 3						
М11.10	Наделена ли служба ИБ полномочиями контролировать работников организации БС РФ в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам?	обязательный	категория 3						
М11.11	Наделена ли служба ИБ полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный	категория 3						
М11.12	Наделена ли служба ИБ полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации БС РФ)?	обязательный	категория 3						

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

Групповой показатель М12 “Определение/коррекция области действия СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М12.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета структурированных по классам (типам) защищаемых информационных активов?	обязательный	категория 1						
М12.2	Проводится ли классификация информационных активов на основании оценок ценности информационных активов для интересов (целей) организации БС РФ, например в соответствии с тяжестью последствий потери свойств ИБ информационных активов?	рекомендуемый	категория 3						
М12.3	Установлены ли в организации БС РФ критерии отнесения конкретных информационных активов к одному или нескольким типам информационных активов?	обязательный	категория 2						
М12.4	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 1						
М12.5	Определены ли в организации БС РФ роли по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
М12.6	Назначены ли в организации БС РФ ответственные за выполнение ролей по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
Итоговая оценка группового показателя М12									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М13.1	Принята ли в организации БС РФ и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный	категория 1						
М13.2	Определены ли в организации БС РФ критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный	категория 2						
М13.3	Определяет ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ организации БС РФ способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания: — степени возможности реализации угроз ИБ выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированных в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов организации БС РФ (типов информационных активов); — степени тяжести последствий от потери свойств ИБ, в частности свойств доступности, целостности и конфиденциальности для рассматриваемых информационных активов (типов информационных активов)?	обязательный	категория 2						
М13.4	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный	категория 2						
М13.5	Проводится ли оценка рисков нарушения ИБ для свойств ИБ всех информационных активов (типов информационных активов) области действия СОИБ?	обязательный	категория 3						
М13.6	Соотносятся ли величины рисков, полученные в результате оценивания рисков нарушения ИБ, с уровнем допустимого риска, принятого в организации БС РФ?	обязательный	категория 3						
М13.7	Зафиксирован ли в организации БС РФ перечень недопустимых рисков нарушения ИБ, сформированный на основе сравнения полученных в результате оценивания рисков нарушения ИБ величин рисков с уровнем допустимого риска, принятого в организации БС РФ?	обязательный	категория 2						
М13.8	Определены ли в организации БС РФ роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М13.9	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М13.10	Определены ли в организации БС РФ роли по оценке рисков нарушения ИБ?	обязательный	категория 3						
М13.11	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный	категория 3						
Итоговая оценка группового показателя М13									

Групповой показатель М14 “Разработка планов обработки рисков нарушения ИБ”

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

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

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М15.16	Детализируют ли документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ, положения политики ИБ и частных политик ИБ?	обязательный	категория 3						
М15.17	Утвержден ли руководством организации БС РФ порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации БС РФ (в случае наличия в структурных подразделениях организации БС РФ работников, ответственных за обеспечение ИБ)?	обязательный	категория 2						
М15.18	Определены ли в составе документов, регламентирующих деятельность в области обеспечения ИБ, перечень свидетельств выполнения указанной деятельности и ответственность работников организации БС РФ за выполнение этой деятельности?	обязательный	категория 2						
М15.19	Определены ли в организации БС РФ процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный	категория 2						
М15.20	Определен ли в организации БС РФ порядок разработки, поддержки, пересмотра и контроля исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 2						
М15.21	Определены ли в организации БС РФ роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М15.22	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
Итоговая оценка группового показателя М15									

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

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

Групповой показатель М17 “Организация реализации планов внедрения СОИБ”

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М18.1	Организована ли санкционированная руководством организации БС РФ работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ?	обязательный	категория 3						
М18.2	Разработаны ли планы, программы обучения и повышения осведомленности в области ИБ, по результатам выполнения которых должна осуществляться проверка полученных знаний?	обязательный	категория 1						
М18.3	Установлены ли в планах обучения и повышения осведомленности требования к периодичности обучения и повышения осведомленности?	обязательный	категория 2						
М18.4	Разрабатываются ли программы обучения и повышения осведомленности для различных групп сотрудников с учетом их должностных обязанностей и выполняемых ролей? Включена ли в них информация: — по существующим политикам ИБ; — по применяемым в организации защитным мерам; — по правильному использованию защитных мер в соответствии с внутренними документами организации БС РФ; — о значимости и важности деятельности работников для обеспечения ИБ организации БС РФ?	обязательный	категория 2						
М18.5	Определен ли в организации БС РФ перечень свидетельств выполнения программ обучения и повышения осведомленности в области ИБ? В частности, такими свидетельствами могут являться: — документы (журналы), подтверждающие прохождение руководителями и работниками организации БС РФ обучения в области ИБ с указанием уровня образования, навыков, опыта и квалификации обучаемых; — документы, содержащие результаты проверок обучения работников организации БС РФ; — документы, содержащие результаты проверок осведомленности в области ИБ в организации БС РФ	обязательный	категория 2						
М18.6	Организуется ли для работника, получившего новую роль, обучение или инструктаж в области ИБ в соответствии с полученной ролью?	обязательный	категория 3						
М18.7	Определены ли в организации БС РФ роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
М18.8	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
Итоговая оценка группового показателя М18									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М19.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры обработки инцидентов, включающие: — процедуры обнаружения инцидентов ИБ; — процедуры информирования об инцидентах, в том числе информирования службы ИБ; — процедуры классификации инцидентов и оценки ущерба, нанесенного инцидентом ИБ; — процедуры реагирования на инцидент; — процедуры анализа причин инцидентов ИБ и оценки результатов реагирования на инциденты ИБ (при необходимости с участием внешних экспертов в области ИБ)?	обязательный	категория 1						
М19.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры хранения и распространения информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ?	обязательный	категория 1						
М19.3	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры действий работников организации БС РФ при обнаружении нетипичных событий, связанных с ИБ, и порядок информирования о данных событиях?	обязательный	категория 1						
М19.4	Осведомлены ли работники организации БС РФ о порядке действий при обнаружении нетипичных событий, связанных с ИБ, и порядке информирования о данных событиях?	обязательный	категория 3						
М19.5	Учитывают ли процедуры расследования инцидентов действующее законодательство РФ, положения нормативных актов Банка России, а также внутренних документов организации БС РФ в области ИБ?	обязательный	категория 3						
М19.6	Принимаются ли, фиксируются ли и выполняются ли в организации БС РФ решения по всем выявленным инцидентам ИБ?	обязательный	категория 1						
М19.7	Определены ли в организации БС РФ роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
М19.8	Назначены ли в организации БС РФ ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
Итоговая оценка группового показателя М19									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М20.1	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета информационных активов или типов информационных активов, существенных для обеспечения непрерывности бизнеса организации БС РФ?	обязательный	категория 1						
М20.2	Установлены ли в организации БС РФ требования обеспечения ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания, в том числе требования к мероприятиям по восстановлению необходимой информации, программного обеспечения, технических средств, а также каналов связи?	обязательный	категория 2						
М20.3	Определен ли в организации БС РФ план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации БС РФ, в состав которого включены: — условия активации плана; — порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персонала); — процедуры восстановления; — процедуры тестирования и проверки плана; — план обучения и повышения осведомленности работников организации БС РФ; — обязанности работников организации БС РФ с указанием ответственных за выполнение каждого из положений плана?	обязательный	категория 2						
М20.4	Основывается ли разработка планов обеспечения непрерывности бизнеса и его восстановления после прерываний на результатах оценки рисков нарушения ИБ организации БС РФ применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М20.5	Применяются ли защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М20.6	Основывается ли применение защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания на соответствующих требованиях по обеспечению ИБ?	обязательный	категория 3						
М20.7	Согласован ли план обеспечения непрерывности бизнеса и его восстановления после прерываний с существующими в организации БС РФ процедурами обработки инцидентов ИБ?	обязательный	категория 2						

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

Групповой показатель М21 “Мониторинг ИБ и контроль защитных мер”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М21.1	Определены ли, выполняются ли и регистрируются ли в организации БС РФ процедуры мониторинга ИБ и контроля защитных мер (включая контроль параметров конфигурации и настроек средств и механизмов защиты), которые охватывают все реализованные и эксплуатируемые защитные меры, входящие в СИБ, и организовываются службой ИБ?	обязательный	категория 1						
М21.2	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры сбора и хранения информации о действиях работников организации БС РФ, событиях и параметрах, имеющих отношение к функционированию защитных мер?	обязательный	категория 1						
М21.3	Учтена ли в рамках выполнения процедур хранения информации об инцидентах ИБ информация обо всех инцидентах ИБ, выявленных в процессе мониторинга ИБ и контроля защитных мер?	обязательный	категория 3						
М21.4	Подвергаются ли процедуры мониторинга ИБ и контроля защитных мер регулярным и регистрируемым пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ?	обязательный	категория 3						
М21.5	Определены ли в организации БС РФ роли, связанные с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
М21.6	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
Итоговая оценка группового показателя М21									

Групповой показатель М22 “Проведение самооценки ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М22.1	Проводится ли самооценка ИБ собственными силами и по инициативе руководства организации БС РФ?	обязательный	категория 3						
М22.2	Проводится ли самооценка ИБ в соответствии с настоящим стандартом?	обязательный	категория 3						
М22.3	Организован ли порядок проведения самооценки ИБ в соответствии с рекомендациями по стандартизации Банка России РС БР ИББС-2.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”?	рекомендуемый	категория 3						
М22.4	Установлена ли в организации БС РФ и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный	категория 1						
М22.5	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры: — формирования, сбора и хранения свидетельств самооценки ИБ; — соблюдения периодичности проведения самооценки ИБ; — хранения и распространения результатов самооценки ИБ?	обязательный	категория 1						
М22.6	Установлен ли в организации БС РФ для каждой проводимой в организации БС РФ самооценки ИБ план ее проведения, определяющий: — цель самооценки ИБ; — объекты и деятельность, подвергающиеся самооценке ИБ; — порядок и сроки выполнения мероприятий самооценки ИБ; — распределение ролей среди работников организации БС РФ, связанных с проведением самооценки ИБ?	обязательный	категория 2						
М22.7	Подготавливаются ли по результатам самооценок ИБ отчеты?	обязательный	категория 3						
М22.8	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М22.9	Определены ли в организации БС РФ роли, связанные с выполнением программы самооценок ИБ?	обязательный	категория 3						
М22.10	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный	категория 3						
М22.11	Проводится ли в организации БС РФ оценка соответствия ИБ в виде самооценки ИБ или аудита ИБ не реже одного раза в два года?	обязательный	категория 1						
Итоговая оценка группового показателя М22									

Групповой показатель М23 “Проведение аудита ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М23.1	Проводится ли аудит ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности” и СТО БР ИББС-1.0?	обязательный	категория 3						
М23.2	Установлена ли в организации БС РФ и реализуется ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки?	обязательный	категория 1						
М23.3	Установлен ли в организации БС РФ для каждого проводимого в организации БС РФ аудита ИБ план аудита, определяющий: — цель аудита ИБ; — критерии аудита ИБ; — область аудита ИБ; — дату и продолжительность проведения аудита ИБ; — состав аудиторской группы; — описание деятельности и мероприятий по проведению аудита ИБ; — распределение ресурсов при проведении аудита ИБ?	обязательный	категория 2						
М23.4	Оформлены ли договоры с аудиторскими организациями с установленными в них процедурами: — хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ; — взаимодействия с аудиторской организацией в процессе проведения аудита ИБ; — взаимодействия аудиторской группы и руководства, позволяющими представителям аудиторской группы при необходимости непосредственно обращаться к руководству; — организации опроса работников; — организации наблюдения за деятельностью работников организации БС РФ со стороны представителей аудиторской организации?	обязательный	категория 2						
М23.5	Подготавливаются ли по результатам аудитов ИБ отчеты?	обязательный	категория 2						
М23.6	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М23.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности отчетов аудитов?	обязательный	категория 1						

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

Групповой показатель М24 “Анализ функционирования СОИБ”

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М25.1	Установлен ли в организации БС РФ перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный	категория 2						
М25.2	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: — мониторинга ИБ и контроля защитных мер; — анализа функционирования СОИБ; — аудитов ИБ; — самооценок ИБ?	обязательный	категория 3						
М25.3	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию: — о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; — о новых, выявленных уязвимостях и угрозах ИБ; — о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством; — об изменениях, которые могли бы повлиять на организацию СОИБ, например изменения в законодательстве РФ и (или) в положениях стандартов Банка России; — о выявленных инцидентах ИБ?	обязательный	категория 3						
М25.4	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например выполнение планов обработки рисков?	обязательный	категория 3						
М25.5	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М25.6	Установлен ли в организации БС РФ план выполнения деятельности по контролю и анализу СОИБ?	обязательный	категория 2						
М25.7	Содержит ли план выполнения деятельности по контролю и анализу СОИБ положения по проведению совещаний на уровне руководства, на которых в том числе производится поиск и анализ проблем ИБ, влияющих на бизнес организации БС РФ?	обязательный	категория 3						
М25.8	Определены ли в организации БС РФ роли, связанные с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный	категория 3						
М25.9	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с подготовкой информации, необходимой для анализа СОИБ руководством?	обязательный	категория 3						
Итоговая оценка группового показателя М25									

Групповой показатель М26 “Принятие решений по тактическим улучшениям СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М26.1	Рассматриваются ли при принятии решений, связанных с тактическими улучшениями СОИБ, результаты: — аудитов ИБ; — самооценок ИБ; — мониторинга ИБ и контроля защитных мер; — анализа функционирования СОИБ; — обработки инцидентов ИБ; — выявления новых угроз и уязвимостей ИБ; — оценки рисков; — анализа перечня защитных мер, возможных для применения; — стратегических улучшений СОИБ; — анализа СОИБ со стороны руководства; — анализа успешных практик в области ИБ (собственных или других организаций)?	обязательный	категория 3						
М26.2	Зафиксированы ли решения по тактическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости тактических улучшений СОИБ, либо направления тактических улучшений СОИБ?	обязательный	категория 2						
М26.3	Регистрируется ли деятельность по реализации тактических улучшений СОИБ?	обязательный	категория 2						
М26.4	Установлены ли в организации БС РФ планы реализации тактических улучшений СОИБ?	обязательный	категория 2						
М26.5	Существуют ли в организации БС РФ документы, в которых фиксируются результаты выполнения планов реализации тактических улучшений СОИБ?	обязательный	категория 3						
М26.6	Санкционирует и контролирует ли руководство службы ИБ организации БС РФ деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный	категория 3						
М26.7	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ?	обязательный	категория 1						
М26.8	Установлены ли роли и назначены ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный	категория 3						
Итоговая оценка группового показателя М26									

Групповой показатель М27 “Принятие решений по стратегическим улучшениям СОИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М27.1	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, результаты: — аудитов ИБ; — самооценок ИБ; — мониторинга ИБ и контроля защитных мер; — анализа функционирования СОИБ; — обработки инцидентов ИБ; — выявления новых информационных активов организации БС РФ или их типов; — выявления новых угроз и уязвимостей ИБ; — оценки рисков; — пересмотра основных рисков ИБ; — анализа СОИБ со стороны руководства; — анализа успешных практик в области ИБ (собственных или других организаций)?	обязательный	категория 3						
М27.2	Рассматриваются ли при принятии решений, связанных со стратегическими улучшениями СОИБ, изменения интересов, целей и задач бизнеса организации БС РФ, контрактных обязательств организации БС РФ, а также изменения в законодательстве РФ и нормативных актах Банка России?	обязательный	категория 2						
М27.3	Фиксируются ли в организации БС РФ решения по стратегическим улучшениям СОИБ, содержащие либо выводы об отсутствии необходимости стратегических улучшений СОИБ, либо направления стратегических улучшений СОИБ?	обязательный	категория 2						
М27.4	Формируются ли направления стратегических улучшений СОИБ в виде корректирующих или превентивных действий, например: — уточнение/пересмотр целей и задач обеспечения ИБ, определенных в рамках политики ИБ (частных политик ИБ) организации БС РФ; — изменения в области действия СОИБ; — пересмотр моделей угроз и нарушителей; — изменение подходов к оценке рисков ИБ, критериев принятия риска ИБ?	обязательный	категория 1						
М27.5	Регистрируется ли деятельность по реализации стратегических улучшений СОИБ?	обязательный	категория 3						
М27.6	Установлены ли в организации БС РФ планы реализации стратегических улучшений СОИБ?	обязательный	категория 2						
М27.7	Существуют ли в организации БС РФ документы, в которых фиксируются результаты выполнения планов реализации стратегических улучшений СОИБ?	обязательный	категория 2						
М27.8	Согласуется ли со службой ИБ, санкционируется ли и контролируется ли руководством организации БС РФ деятельность, связанная с реализацией стратегических улучшений СОИБ?	обязательный	категория 1						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М27.9	В случае стратегических улучшений СОИБ выполняется ли деятельность по реализации соответствующих тактических улучшений СОИБ для всех необходимых процедур обеспечения ИБ, используемых мер защиты и соответствующих внутренних документов, в частности, выполняются ли: — выработка планов тактических улучшений СОИБ; — уточнение планов обработки рисков; — уточнение программы внедрения защитных мер; — уточнение процедур использования защитных мер?	обязательный	категория 3						
М27.10	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям ИБ?	обязательный	категория 1						
М27.11	Установлены ли роли и назначены ли ответственные за реализацию решений по стратегическим улучшениям СОИБ в случае их принятия?	обязательный	категория 2						
Итоговая оценка группового показателя М27									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М28.1 (аналог М11.1)	Сформирована ли руководством служба ИБ в составе не менее двух человек (назначены ли уполномоченные лица) для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ, утверждены ли цели и задачи ее деятельности?	обязательный	категория 3						
М28.2 (аналог М11.2)	Имеет ли служба ИБ утвержденные руководством полномочия и ресурсы, необходимые для выполнения установленных целей и задач?	обязательный	категория 3						
М28.3 (аналог М11.3)	Имеет ли служба ИБ назначенного из числа руководства куратора, который при этом не является куратором службы информатизации (автоматизации)?	обязательный	категория 3						
М28.4 (аналог М11.4)	Наделена ли служба ИБ собственным бюджетом?	рекомендуемый	категория 3						
М28.5 (аналог М11.5)	Сформированы ли для организаций БС РФ, имеющих сеть филиалов или региональных представительств, подразделения ИБ (уполномоченные лица) на местах и обеспечены ли эти подразделения необходимыми ресурсами и нормативной базой?	обязательный	категория 1						
М28.6 (аналог М11.6)	Наделена ли служба ИБ полномочиями организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М28.7 (аналог М11.7)	Наделена ли служба ИБ полномочиями разрабатывать и вносить предложения по изменению политик ИБ организации БС РФ?	обязательный	категория 3						
М28.8 (аналог М11.8)	Наделена ли служба ИБ полномочиями организовывать изменения существующих и принятие руководством новых внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М28.9 (аналог М11.9)	Наделена ли служба ИБ полномочиями определять требования к мерам обеспечения ИБ организации БС РФ?	обязательный	категория 3						
М28.10 (аналог М11.10)	Наделена ли служба ИБ полномочиями контролировать работников организации БС РФ в части выполнения ими требований внутренних документов, регламентирующих деятельность в области обеспечения ИБ, в первую очередь работников, имеющих максимальные полномочия по доступу к защищаемым информационным активам?	обязательный	категория 3						
М28.11 (аналог М11.11)	Наделена ли служба ИБ полномочиями осуществлять мониторинг событий, связанных с обеспечением ИБ?	обязательный	категория 3						

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М28.12 (аналог М11.12)	Наделена ли служба ИБ полномочиями участвовать в расследовании событий, связанных с инцидентами ИБ, и выходить в случае необходимости с предложениями по применению санкций в отношении лиц, осуществивших НСД и НРД (например, нарушивших требования инструкций, руководств по обеспечению ИБ организации БС РФ)?	обязательный	категория 3						
М28.13 (аналог М11.13)	Наделена ли служба ИБ полномочиями участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий?	обязательный	категория 3						
М28.14 (аналог М11.15)	Наделена ли служба ИБ полномочиями участвовать в создании, поддержании, эксплуатации и совершенствовании СОИБ организации БС РФ?	обязательный	категория 3						
Итоговая оценка группового показателя М28									

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

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М30.1 (аналог М12.1)	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ процедуры учета структурированных по классам (типам) защищаемых информационных активов?	обязательный	категория 1						
М30.2 (аналог М12.5)	Определены ли в организации БС РФ роли по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
М30.3 (аналог М12.6)	Назначены ли в организации БС РФ ответственные за выполнение ролей по учету информационных активов и учету объектов среды для каждого информационного актива и (или) типа информационного актива, покрывающие все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 стандарта СТО БР ИББС-1.0?	обязательный	категория 3						
М30.4 (аналог М13.1)	Принята ли в организации БС РФ и корректируется ли методика оценки рисков нарушения ИБ / подход к оценке рисков нарушения ИБ?	обязательный	категория 1						
М30.5 (аналог М13.2)	Определены ли в организации БС РФ критерии принятия рисков нарушения ИБ и уровень допустимого риска нарушения ИБ?	обязательный	категория 2						
М30.6 (аналог М13.4)	Определяет ли порядок оценки рисков нарушения ИБ необходимые процедуры оценки рисков нарушения ИБ, а также последовательность их выполнения?	обязательный	категория 2						
М30.7 (аналог М13.8)	Определены ли в организации БС РФ роли, связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М30.8 (аналог М13.9)	Назначены ли ответственные за выполнение ролей, связанных с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ / подхода к оценке риска нарушения ИБ?	обязательный	категория 3						
М30.9 (аналог М13.10)	Определены ли в организации БС РФ роли по оценке рисков нарушения ИБ?	обязательный	категория 3						
М30.10 (аналог М13.11)	Назначены ли ответственные за выполнение ролей по оценке рисков нарушения ИБ?	обязательный	категория 3						
М30.11 (аналог М14.3)	Утверждены ли руководством организации БС РФ планы обработки рисков нарушения ИБ?	обязательный	категория 2						
М30.12 (аналог М14.5)	Определены ли в организации БС РФ роли по разработке планов обработки рисков нарушения ИБ?	обязательный	категория 3						
М30.13 (аналог М14.6)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке планов обработки рисков нарушения ИБ?	обязательный	категория 3						
М30.14 (аналог М15.2)	Разработана ли политика ИБ организации БС РФ?	обязательный	категория 2						

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М30.22 (аналог М15.13)	Корректируются ли внутренние документы, регламентирующие деятельность в области обеспечения ИБ на основе: — законодательства РФ; — комплекса БР ИББС, в частности требования разделов 7 и 8 стандарта СТО БР ИББС-1.0; — нормативных актов и предписаний регулирующих и надзорных органов; — договорных требований организации БС РФ со сторонними организациями; — результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов или типов информационных активов?	обязательный	категория 3						
М30.23 (аналог М15.17)	Утвержден ли руководством организации БС РФ порядок взаимодействия (координирования работы) службы ИБ с работниками, ответственными за обеспечение ИБ в структурных подразделениях организации БС РФ (в случае наличия в структурных подразделениях организации БС РФ работников, ответственных за обеспечение ИБ)?	обязательный	категория 2						
М30.24 (аналог М15.19)	Определены ли в документах организации БС РФ процедуры выделения и распределения ролей в области обеспечения ИБ?	обязательный	категория 2						
М30.25 (аналог М15.21)	Определены ли в организации БС РФ роли по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М30.26 (аналог М15.22)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, поддержке, пересмотру и контролю исполнения внутренних документов, регламентирующих деятельность по обеспечению ИБ организации БС РФ?	обязательный	категория 3						
М30.27 (аналог М17.3)	Определены ли в организации БС РФ роли, связанные с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный	категория 3						
М30.28 (аналог М17.4)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с реализацией планов обработки рисков нарушения ИБ и с реализацией требуемых защитных мер?	обязательный	категория 3						
Итоговая оценка группового показателя М30									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М31.1 (аналог М18.1)	Организована ли санкционированная руководством организации БС РФ работа с персоналом и клиентами в направлении повышения осведомленности и обучения в области ИБ?	обязательный	категория 3						
М31.2 (аналог М18.2)	Разработаны ли планы, программы обучения и повышения осведомленности в области ИБ, по результатам выполнения которых должна осуществляться проверка полученных знаний?	обязательный	категория 1						
М31.3 (аналог М18.7)	Определены ли в организации БС РФ роли по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
М31.4 (аналог М18.8)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке, реализации планов и программ обучения и повышения осведомленности в области ИБ и по контролю их результатов?	обязательный	категория 3						
М31.5 (аналог М19.7)	Определены ли в организации БС РФ роли по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
М31.6 (аналог М19.8)	Назначены ли в организации БС РФ ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	обязательный	категория 3						
М31.7 (аналог М20.3)	Определен ли в организации БС РФ план обеспечения непрерывности бизнеса и его восстановления после возможного прерывания, содержащий инструкции и порядок действий работников организации БС РФ, в состав которого включены: – условия активации плана; – порядок действий, которые должны быть предприняты после инцидента ИБ (инструкции персоналу); – процедуры восстановления; – процедуры тестирования и проверки плана; – план обучения и повышения осведомленности работников организации БС РФ; – обязанности работников организации БС РФ с указанием ответственных за выполнение каждого из положений плана?	обязательный	категория 2						
М31.8 (аналог М20.12)	Определены ли в организации БС РФ роли по разработке плана обеспечения непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М31.9 (аналог М20.13)	Назначены ли в организации БС РФ ответственные за выполнение ролей по разработке плана, обеспечение непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
Итоговая оценка группового показателя М31									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М32.1 (аналог М21.5)	Определены ли в организации БС РФ роли, связанные с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
М32.2 (аналог М21.6)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением процедур мониторинга ИБ и контроля защитных мер, а также с пересмотром указанных процедур?	обязательный	категория 3						
М32.3 (аналог М22.4)	Установлена ли в организации БС РФ и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный	категория 1						
М32.4 (аналог М22.8)	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М32.5 (аналог М22.9)	Определены ли в организации БС РФ роли, связанные с выполнением программы самооценок ИБ?	обязательный	категория 3						
М32.6 (аналог М22.10)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный	категория 3						
М32.7 (аналог М22.11, М23.10)	Проводится ли в организации БС РФ оценка соответствия ИБ в виде или самооценки ИБ аудита ИБ не реже одного раза в два года?	обязательный	категория 1						
М32.8 (аналог М23.2)	Установлена ли в организации БС РФ и реализована ли программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки?	обязательный	категория 1						
М32.9 (аналог М23.6)	Доводятся ли результаты аудитов ИБ и соответствующие отчеты до руководства организации БС РФ?	обязательный	категория 3						
М32.10 (аналог М23.8)	Определены ли в организации БС РФ роли, связанные с организацией выполнения программ аудитов и планов отдельных аудитов?	обязательный	категория 3						
М32.11 (аналог М23.9)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с организацией выполнения программ аудитов и планов отдельных внешних аудитов?	обязательный	категория 3						
М32.12 (аналог М24.7)	Определены ли в организации БС РФ роли, связанные с процедурами анализа функционирования СОИБ?	обязательный	категория 3						
М32.13 (аналог М24.8)	Назначены ли в организации БС РФ ответственные за выполнение ролей, связанных с процедурами анализа функционирования СОИБ?	обязательный	категория 3						
Итоговая оценка группового показателя М32									

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М33.1 (аналог М25.1)	Установлен ли в организации БС РФ перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ?	обязательный	категория 2						
М33.2 (аналог М25.2)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, отчеты с результатами: — мониторинга ИБ и контроля защитных мер; — анализа функционирования СОИБ; — аудитов ИБ; — самооценок ИБ?	обязательный	категория 3						
М33.3 (аналог М25.3)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, содержащие информацию: — о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ; — о новых, выявленных уязвимостях и угрозах ИБ; — о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством; — об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве РФ и (или) в положениях стандартов Банка России; — о выявленных инцидентах ИБ?	обязательный	категория 3						
М33.4 (аналог М25.4)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например выполнения планов обработки рисков?	обязательный	категория 3						
М33.5 (аналог М25.5)	Входят ли в перечень документов, необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ, документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания?	обязательный	категория 3						
М33.6 (аналог М25.6)	Установлен ли в организации БС РФ план выполнения деятельности по контролю и анализу СОИБ?	обязательный	категория 2						

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

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

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Категория проверки частного показателя	Оценка частного показателя ИБ					
				0	0,25	0,5	0,75	1	н/о
М34.1 (аналог М26.6)	Санкционирует и контролирует ли руководство службы ИБ организации БС РФ деятельность, связанную с реализацией тактических улучшений СОИБ?	обязательный	категория 3						
М34.2 (аналог М26.8)	Установлены ли роли и назначены ли ответственные за реализацию решений по тактическим улучшениям СОИБ?	обязательный	категория 3						
М34.3 (аналог М27.8)	Согласуется ли со службой ИБ, санкционируется ли и контролируется ли руководством организации БС РФ деятельность, связанная с реализацией стратегических улучшений СОИБ?	обязательный	категория 2						
М34.4 (аналог М27.11)	Установлены ли роли и назначены ли ответственные за реализацию решений по стратегическим улучшениям СОИБ в случае их принятия?	обязательный	категория 2						
Итоговая оценка группового показателя М34									

Приложение Б
(обязательное)

Форма листов для сбора свидетельств аудита ИБ

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

_____
(подпись)

_____
(подпись)

_____
(подпись)

Приложение В
(обязательное)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

СТО БР ИББС-1.2-2014

Частный показатель СТО БР ИББС-1.2	Номер пункта таблицы приложения 2 к Положению Банка России от 9 июня 2012 года № 382-П	Номер подпункта Положения Банка России от 9 июня 2012 года № 382-П	Формулировка требования к обеспечению защиты информации при осуществлении переводов денежных средств
	П. 127	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств
	П. 128	2.17.2	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях выявления недостатков при проведении оценки соответствия
M27.7	П. 129	2.17.3	Принятие решений оператора по переводу денежных средств, оператора услуг платежной инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности

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

РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.5-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2014-06-01

Издание официальное

Москва
2014

РС БР ИББС-2.5-2014

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 17 мая 2014 года № Р-400.

Содержание

Введение 154
1. Область применения 155
2. Нормативные ссылки 155
3. Термины и определения 155
4. Обозначения и сокращения 156
5. Общие положения 156
6. Рекомендации по планированию в рамках системы менеджмента инцидентов ИБ 157
   6.1. Рекомендации по разработке и документированию политики менеджмента инцидентов ИБ организации БС РФ 157
   6.2. Рекомендации к определению организационной структуры реагирования на инциденты ИБ 158
   6.3. Рекомендации к определению ролей процесса реагирования на инциденты ИБ 159
   6.4. Рекомендации по установлению и документированию регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ 162
   6.5. Рекомендации по выбору технических средств по обнаружению и реагированию на инциденты ИБ и определению порядка их эксплуатации 164
   6.6. Рекомендации по определению порядка осуществления контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ 166
7. Рекомендации по реализации в рамках системы менеджмента инцидентов ИБ 166
   7.1. Рекомендации по выделению необходимых ресурсов и назначению ролей в рамках процессов реагирования на инциденты ИБ 166
   7.2. Рекомендации по проведению мероприятий по обучению и повышению осведомленности в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ 167
   7.3. Рекомендации по выполнению деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ 168
8. Рекомендации по анализу в рамках системы менеджмента инцидентов ИБ 169
9. Рекомендации к классификации инцидентов ИБ и использованию классификатора инцидентов ИБ в процессе их обработки 170

Приложение 1. Примерный перечень типов событий ИБ 172
Приложение 2. Примерный классификатор инцидентов ИБ 175
Библиография 178

РС БР ИББС-2.5-2014

Введение

Действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) с целью создания и поддержания на должном уровне системы обеспечения информационной безопасности (далее — СОИБ) организаций банковской системы (далее — БС) Российской Федерации (далее — РФ) и снижения степени тяжести последствий от нарушений ИБ определены требования к организации обнаружения и реагирования на инциденты информационной безопасности (далее — ИБ).

Настоящие рекомендации в области стандартизации Банка России устанавливают подходы к реализации организацией БС РФ процесса обнаружения и реагирования на инциденты ИБ, являющегося составной частью системы менеджмента ИБ (СМИБ) организации БС РФ.

РС БР ИББС-2.5-2014

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2014-06-01

1. Область применения

Настоящие рекомендации в области стандартизации Банка России распространяются на организации БС РФ, проводящие деятельность по обнаружению инцидентов ИБ и реагированию на инциденты ИБ в рамках реализации СОИБ в соответствии с требованиями СТО БР ИББС-1.0.

Настоящие рекомендации в области стандартизации Банка России рекомендованы для применения путем прямого использования устанавливаемых в них положений при проведении деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ, а также путем включения ссылок на них и (или) прямого использования содержащихся в них положений во внутренних документах организации БС РФ.

Положения настоящих рекомендаций в области стандартизации Банка России применяются на добровольной основе. В конкретной организации БС РФ для проведения деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ могут использоваться иные рекомендации и (или) требования.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на СТО БР ИББС-1.0.

3. Термины и определения

В настоящих рекомендациях в области стандартизации Банка России применяются термины и определения, установленные СТО БР ИББС-1.0, а также следующие термины и соответствующие определения:

3.1. **Инцидент ИБ** — событие ИБ или их комбинация, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, результатом которой являются:

- нарушение в СОИБ организации БС РФ, включая нарушение работы средств защиты информации;
- нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов организации БС РФ в области обеспечения ИБ, нарушение в выполнении процессов СМИБ организации БС РФ;
- нарушение в выполнении банковских технологических процессов организации БС РФ;
- нанесение ущерба организации БС РФ и (или) ее клиентам.

3.2. **Событие ИБ** — изменение состояния объекта или области мониторинга ИБ, действия работников организации БС РФ и (или) иных лиц, которые указывают на возможный инцидент ИБ.

3.3. **Журнал регистрации событий ИБ** — электронный журнал, содержащий записи о событиях ИБ, в том числе о действиях пользователей и эксплуатирующего персонала автоматизированной банковской системы (далее — АБС).

3.4. **Менеджмент инцидентов ИБ** — деятельность по своевременному обнаружению инцидентов ИБ, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов ИБ для организации БС РФ и (или) ее клиентов.

3.5. **Закрытие инцидента ИБ** — действия работников организации БС РФ в рамках реагирования на инцидент ИБ, результатом которых являются:

- устранение нарушений в СОИБ организации БС РФ, реализованных в результате инцидента ИБ;
- устранение последствий угрозы (угроз) ИБ, реализованн(ой)ых в составе инцидента ИБ;
- выяснение причин нетипичного поведения работников организации БС РФ и (или) иных лиц, нештатного функционирования АБС и иных объектов среды информационных активов организации БС РФ, а также нетипичных событий в выполнении банковских технологических процессов.

3.6. **Группа реагирования на инциденты ИБ** (далее — ГРИИБ) — действующая на постоянной основе группа работников организации БС РФ, которая выполняет установленные в организации БС РФ процедуры реагирования на инциденты ИБ.

3.7. **Классификатор инцидентов ИБ** — документ, определяющий способ описания инцидентов ИБ с помощью набора атрибутов — параметров инцидента ИБ.

3.8. **Запись об инциденте ИБ** — элемент централизованной базы данных об инцидентах ИБ, содержащий описание конкретного инцидента ИБ в соответствии с классификатором инцидентов ИБ.

3.9. **Администратор ИБ** — работник организации БС РФ, на которого возложены обязанности по мониторингу ИБ и контролю защитных мер в АБС, аудиту прав и контролю действий пользователей и эксплуатирующего персонала АБС.

3.10. **Распорядитель доступа информационного актива** — руководитель структурного подразделения организации БС РФ или работник организации БС РФ, осуществляющий распоряжение доступом к информационному активу в пределах полномочий, предоставленных организацией БС РФ.

4. Обозначения и сокращения

АБС — автоматизированная банковская система;
БС РФ — банковская система Российской Федерации;
ГРИИБ — группа реагирования на инциденты ИБ;
ИБ — информационная безопасность;
СОИБ — система обеспечения информационной безопасности;
СМИБ — система менеджмента информационной безопасности.

5. Общие положения

5.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне менеджмента инцидентов ИБ организации БС РФ рекомендуется реализовать ряд процессов системы менеджмента инцидентов ИБ, сгруппированных в виде циклической модели Деминга: "...— планирование — реализация — проверка — совершенствование — планирование — ...".

5.2. Планирование в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:

- разработка и документирование политики менеджмента инцидентов ИБ организации БС РФ;
- определение организационной структуры и ролей процессов реагирования на инциденты ИБ;
- установление и документирование регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- выбор технических средств, включая средства защиты информации, необходимых для использования в рамках процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ, и определение во внутренних документах организации БС РФ порядка эксплуатации указанных технических средств;
- определение порядка осуществления контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ.

5.3. Реализация в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:

- выделение необходимых ресурсов и назначение ролей для выполнения процессов реагирования на инциденты ИБ;

— проведение мероприятий по обучению и повышению осведомленности работников организации БС РФ, представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
— выполнение деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ.

5.4. Анализ в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:
— анализ действий работников организации БС РФ при выполнении процессов реагирования на инцидент ИБ;
— определение направлений и методов совершенствования СОИБ организации БС РФ на основе результатов выполнения процессов менеджмента инцидентов ИБ;
— определение направлений и методов улучшения процессов менеджмента инцидентов ИБ.

5.5. Совершенствование в рамках системы менеджмента инцидентов ИБ включает выполнение следующих основных мероприятий:
— принятие решений и инициирование совершенствования процессов менеджмента инцидентов ИБ;
— принятие решений и инициирование улучшений в СОИБ организации БС РФ.

Непосредственное выполнение деятельности по совершенствованию процессов менеджмента инцидентов ИБ осуществляется путем планирования и реализации в рамках системы менеджмента инцидентов ИБ.

Выполнение решений по совершенствованию СОИБ организации БС РФ реализуется в рамках тактических и стратегических улучшений, требования к выполнению которых установлены СТО БР ИББС-1.0.

6. Рекомендации по планированию в рамках системы менеджмента инцидентов ИБ

6.1. Рекомендации по разработке и документированию политики менеджмента инцидентов ИБ организации БС РФ

6.1.1. Политика менеджмента инцидентов ИБ организации БС РФ является внутренним документом организации БС РФ, устанавливающим принципы и основные положения, регламентирующие деятельность по менеджменту инцидентов ИБ организации БС РФ.

Политика менеджмента инцидентов ИБ организации БС РФ разрабатывается службой ИБ организации БС РФ совместно и (или) по согласованию с подразделением информатизации организации БС РФ, юридической службой организации БС РФ, подразделениями организации БС РФ, в зоне компетенции которых находятся вопросы обеспечения непрерывности выполнения банковских технологических процессов организации БС РФ, службой персонала (кадров) организации БС РФ и утверждается руководством организации БС РФ.

6.1.2. В политике менеджмента инцидентов ИБ организации БС РФ рекомендуется установить следующие положения:

1. Цель и задачи менеджмента инцидентов ИБ.

Основные цели менеджмента инцидентов ИБ, устанавливаемые политикой менеджмента инцидентов ИБ организации БС РФ, должны определять:
— создание условий для осуществления своевременного обнаружения и оперативного реагирования на инциденты ИБ, в том числе их закрытия;
— предотвращение и (или) снижение негативного влияния инцидентов ИБ на выполнение банковских технологических процессов организации БС РФ и (или) ее клиентов;
— оперативное совершенствование СОИБ организации БС РФ.

Основные задачи, устанавливаемые политикой менеджмента инцидентов ИБ организации БС РФ и решаемые в рамках менеджмента инцидентов ИБ, должны обеспечивать достижение установленных целей менеджмента инцидентов ИБ путем:
— своевременного обнаружения инцидентов ИБ;
— оперативного реагирования на инциденты ИБ в соответствии с требованиями законодательства РФ, нормативных актов Банка России и регламентами, установленными внутренними документами организации БС РФ;
— координации деятельности работников структурных подразделений организации БС РФ в рамках процессов реагирования на инциденты ИБ, в том числе их закрытия;

— ведения базы данных зарегистрированных событий ИБ и обнаруженных инцидентов ИБ;
— накопления и повторного использования знаний по обнаружению инцидентов ИБ и реагированию на них;
— анализа, оценки эффективности и совершенствования процессов менеджмента инцидентов ИБ организации БС РФ;
— предоставления руководству организации БС РФ информации и отчетов по результатам выполнения процессов менеджмента инцидентов ИБ, в том числе информации о фактах обнаружения инцидентов ИБ и результатах реагирования на них.

2. Общее описание состава событий ИБ и критериев классификации событий ИБ как инцидентов ИБ. Описание событий ИБ рекомендуется производить путем формирования перечня типов событий ИБ для каждого из уровней информационной инфраструктуры организации БС РФ, определенных СТО БР ИББС-1.0.

3. Общее описание стадий обнаружения инцидентов ИБ и реагирования на инциденты ИБ, ролей работников организации БС РФ, задействованных на стадиях реагирования на инциденты ИБ, с указанием подразделений организации БС РФ, работникам которых назначаются указанные роли.

Рекомендуется рассматривать следующие стадии обнаружения инцидентов ИБ и реагирования на инциденты ИБ:
— стадия обнаружения, оповещения и оценки, на которой путем анализа события ИБ и установленных в организации БС РФ критериев выявляется инцидент ИБ, производится оповещение уполномоченных работников организации БС РФ, оценка инцидента ИБ, принятие решений о дальнейшем реагировании на инцидент ИБ;
— стадия сбора и фиксации информации, относящейся к инциденту ИБ;
— стадия закрытия инцидента ИБ, в том числе локализации (предотвращение распространения) и восстановления штатного выполнения банковских технологических процессов организации БС РФ, на которой происходит устранение негативных последствий от реализации инцидента ИБ (при их наличии);
— стадия анализа собранной информации, относящейся к инциденту ИБ, и принятие управленческих решений по результатам реагирования на инцидент ИБ.

Стадии сбора и фиксации информации, закрытия инцидента ИБ, анализа информации и принятия управленческих решений в рамках настоящих рекомендаций объединяются общим термином “реагирование на инцидент ИБ”.

4. Общее описание организационной структуры процессов реагирования на инциденты ИБ с указанием:
— состава структурных подразделений организации БС РФ, работникам которых назначаются роли, связанные с реагированием на инциденты ИБ;
— требований к ГРИИБ, в том числе к составу лиц, включаемых в ГРИИБ;
— состава ролей участников процессов реагирования на инциденты ИБ;
— принципов и способов взаимодействия ГРИИБ и работников организации БС РФ в рамках реализации процесса реагирования на инциденты ИБ.

6.2. Рекомендации к определению организационной структуры реагирования на инциденты ИБ

6.2.1. Организационная структура реагирования на инциденты ИБ должна обеспечивать достижение установленных целей менеджмента инцидентов ИБ и решение задач менеджмента инцидентов ИБ во всех структурных подразделениях организации БС РФ. Для этого рекомендуется выделение двухуровневой организационной структуры реагирования на инциденты ИБ — центральной и филиальной (региональной).

6.2.2. На центральном уровне реагирования на инциденты ИБ реализуется выполнение следующих основных задач:
— планирование процессов реагирования на инциденты ИБ организации БС РФ;
— установление регламентов реагирования на инциденты ИБ;
— контроль реализации процессов реагирования на инциденты ИБ организации БС РФ;
— планирование, контроль и координация совместной деятельности ГРИИБ разных уровней;
— обобщенный анализ результатов реагирования на инциденты ИБ;
— выработка предложений по принятию управленческих решений по результатам реагирования на инциденты ИБ;
— выработка предложений по совершенствованию и контроль совершенствования процессов менеджмента инцидентов ИБ;

— обнаружение инцидентов ИБ, реагирование на инциденты ИБ головного (центрального) структурного подразделения организации БС РФ, а также реагирование на инциденты ИБ, которые эскалированы с регионального уровня, в соответствии с установленными в организации БС РФ критериями.

6.2.3. На филиальном (региональном) уровне реагирования на инциденты ИБ реализуется выполнение следующих основных задач:

— планирование мероприятий по реагированию на инциденты ИБ на филиальном (региональном) уровне;
— контроль соблюдения установленных регламентов реагирования на инциденты ИБ на филиальном (региональном) уровне;
— обнаружение инцидентов ИБ, реагирование на инциденты ИБ филиального (регионального) уровня, а также эскалация инцидентов ИБ на центральный уровень в соответствии с установленными в организации БС РФ критериями.

Основу организационной структуры реагирования на инциденты ИБ на каждом из уровней составляет ГРИИБ, создаваемая для каждого из уровней.

6.2.4. ГРИИБ центрального уровня координирует и осуществляет реагирование на инциденты ИБ головного (центрального) структурного подразделения организации БС РФ, координирует и контролирует реагирование на инциденты ИБ регионального уровня в случае их эскалации на центральный уровень. Основу ГРИИБ центрального уровня рекомендуется формировать из представителей службы ИБ организации БС РФ и подразделений информатизации организации БС РФ, обладающих необходимыми полномочиями по выделению работников указанных подразделений для осуществления деятельности по реагированию на инциденты ИБ. Организационную структуру, состав, обязанности и полномочия ГРИИБ центрального уровня рекомендуется определять Положением о ГРИИБ.

6.2.5. ГРИИБ филиального (регионального) уровня координирует и осуществляет реагирование на инциденты ИБ в пределах соответствующего филиала (региона), а в случае отсутствия возможности их обработки с привлечением собственных ресурсов и установленными в организации БС РФ критериями осуществляет их эскалацию в ГРИИБ центрального уровня. Основу ГРИИБ регионального уровня рекомендуется формировать из представителей службы ИБ и подразделений информатизации, обладающих необходимыми компетенциями для реагирования на инциденты ИБ.

Типовую организационную структуру, состав, обязанности и полномочия ГРИИБ регионального уровня рекомендуется определять на центральном уровне типовым Положением о ГРИИБ регионального уровня.

6.3. Рекомендации к определению ролей процесса реагирования на инциденты ИБ

6.3.1. В организации БС РФ рекомендуется определить роли работников, связанные с реагированием на инциденты ИБ, и назначить ответственных за их выполнение. Среди прочего, рекомендуется определить роли, связанные с выполнением деятельности на следующих стадиях:

— стадия оповещения и оценки;
— стадия сбора и фиксации информации;
— стадия закрытия инцидента ИБ;
— стадия анализа и принятие управленческих решений по результатам реагирования на инцидент ИБ.

6.3.2. Ответственных за выполнение ролей в рамках реагирования на инциденты ИБ рекомендуется включать в ГРИИБ. При необходимости ГРИИБ может дополняться внешними экспертами, привлекаемыми на временной основе.

Действия членов ГРИИБ в рамках процесса обработки инцидента ИБ рекомендуется определить соответствующими регламентами реагирования на инциденты ИБ.

6.3.3. Рекомендуется установить следующий состав ролей ГРИИБ:

1. Роль куратора ГРИИБ, который организует и курирует выполнение процессов реагирования на инциденты ИБ, работу ГРИИБ, а также обеспечивает общий контроль достаточности и своевременности выполнения деятельности в организации БС РФ по реагированию на инциденты ИБ.

Среди прочего, куратор ГРИИБ:

— инициирует принятие управленческих решений по результатам реагирования на инциденты ИБ;
— информирует руководство организации БС РФ об обнаруженных инцидентах ИБ и результатах реагирования на них;

— принимает решение о проведении расследований по фактам инцидентов ИБ, а также о необходимости взаимодействия со сторонними организациями и правоохранительными органами в рамках расследования инцидентов ИБ.

Рекомендуется назначать куратора ГРИИБ из числа руководства организации БС РФ.

2. Роль руководителя ГРИИБ, который обеспечивает оперативное руководство реагированием на инциденты ИБ.

Руководителя ГРИИБ рекомендуется наделять административными полномочиями, позволяющими обеспечивать управление и координацию участников процесса реагирования на инциденты ИБ в соответствии с установленными регламентами. В обязанности руководителя ГРИИБ входят:

— инициализация реагирования на инцидент ИБ в ГРИИБ;
— назначение ответственного исполнителя ГРИИБ для реагирования на обнаруженный и зарегистрированный инцидент ИБ;
— координирование деятельности членов ГРИИБ при реагировании на инцидент ИБ;
— привлечение необходимой компетенции в рамках ГРИИБ для реагирования на инцидент ИБ;
— контроль соблюдения требований регламентирующих документов в ходе реагирования на инцидент ИБ;
— принятие решения о возможности закрытия инцидента ИБ;
— предоставление консультаций и рекомендаций участникам процесса реагирования на инциденты ИБ.

Кроме того, к обязанностям руководителя ГРИИБ рекомендуется относить формирование предложений по совершенствованию процессов реагирования на инциденты ИБ и пересмотру соответствующих регламентов.

Руководитель ГРИИБ является основным ответственным за исполнение процесса реагирования на инцидент ИБ, а также за результат исполнения данного процесса.

Рекомендуется назначать руководителя ГРИИБ из числа руководства службы ИБ организации БС РФ.

3. Роль оператора-диспетчера ГРИИБ, который в качестве единой точки входа обеспечивает сбор информации о событиях ИБ и инцидентах ИБ, обнаруженных и (или) имевших место в организации БС РФ.

В обязанности оператора-диспетчера ГРИИБ входят:

— отслеживание (мониторинг) событий ИБ с использованием технических средств мониторинга ИБ;
— сбор информации о событиях ИБ и (или) нетипичных событиях, потенциально имеющих отношение к ИБ, от работников организации БС РФ;
— проведение первичной оценки событий ИБ с целью определения, является ли событие ИБ инцидентом ИБ;
— обеспечение и контроль ведения записей о событиях ИБ;
— в случае классификации событий ИБ в качестве инцидента ИБ регистрация инцидента ИБ и информирование руководителя ГРИИБ и (или) членов ГРИИБ.

4. Роль аналитика ГРИИБ, который обладает необходимой компетенцией и назначается ответственным исполнителем ГРИИБ для реагирования на обнаруженный и зарегистрированный инцидент ИБ.

Аналитик ГРИИБ выполняет следующие основные функции:

— проведение вторичной оценки события ИБ с целью подтвердить, что событие ИБ является инцидентом ИБ, и, в случае такого подтверждения, проведение мероприятий по реагированию на инцидент ИБ и расследованию инцидента ИБ, в том числе сбор и фиксация информации, координирование и контроль закрытия инцидента ИБ;
— оповещение работников организации БС РФ об инциденте ИБ в соответствии с установленными регламентами;
— взаимодействие с оператором-диспетчером ГРИИБ, руководителем ГРИИБ по вопросам реагирования на инцидент ИБ;
— выдвижение предложений о необходимости взаимодействия в рамках расследования инцидентов ИБ со сторонними организациями и правоохранительными органами;
— выдвижение предложений по результатам реагирования на инцидент ИБ, в том числе предложений по совершенствованию СОИБ организации БС РФ, совершенствованию процессов менеджмента инцидентов ИБ, регламентов реагирования на инциденты ИБ, внутренних документов организации БС РФ, связанных с инцидентами ИБ.

Рекомендуется объединять аналитиков ГРИИБ в функциональные группы для решения задач по реагированию на инциденты ИБ определенного вида, например инциденты ИБ, связанные с воздействием вредоносного кода, или инциденты ИБ при осуществлении дистанционного банковского обслуживания.

Рекомендуется назначать аналитиков ГРИИБ из числа работников службы ИБ или работников подразделения информатизации организации БС РФ.

5. Роль секретаря ГРИИБ, основной задачей которого является сбор и анализ информации с целью формирования и предоставления руководителю ГРИИБ и куратору ГРИИБ аналитических отчетов материалов, включая:

- сбор и обобщение сведений об инцидентах ИБ, в том числе событиях ИБ, ошибочно признанных инцидентами ИБ;
- подготовку отчетов о зафиксированных инцидентах ИБ, в том числе событиях ИБ, ошибочно признанных инцидентами ИБ;
- подготовку отчетов о результатах реагирования на инциденты ИБ и расследования инцидентов ИБ.

Ограничений на назначение одному работнику нескольких ролей ГРИИБ в рамках настоящих рекомендаций не устанавливается. В то же время не рекомендуется совмещение в одном лице ролей ГРИИБ и ролей, связанных с разработкой, модернизацией и непосредственной эксплуатацией АБС.

6.3.4. При определении состава ГРИИБ, а также экспертов, привлекаемых к реагированию на инциденты ИБ на временной основе, рекомендуется предусмотреть включение представителей следующих структурных подразделений организации БС РФ:

- служба ИБ организации БС РФ, представители которой участвуют на всех этапах реагирования на инцидент ИБ;
- подразделения информатизации, привлечение представителей которых рекомендуется для оценки влияния (воздействия) инцидентов ИБ на предоставление ИТ-услуг организации БС РФ и для выработки решений по поддержанию и восстановлению ИТ-услуг организации БС РФ в ходе реагирования на инциденты ИБ;
- юридическая служба, привлечение представителей которой следует обеспечить, если есть основания полагать, что инцидент ИБ может иметь правовые последствия, в том числе для участия в сборе доказательной базы, подготовки материалов для правоохранительных органов или для передачи в суд;
- подразделение по связям с общественностью и со средствами массовой информации, привлечение представителей которого следует обеспечить, если есть основания полагать, что возникнет необходимость информирования средств массовой информации и общественности;
- подразделения организации БС РФ, в зоне компетенции которых находятся вопросы обеспечения непрерывности выполнения банковских технологических процессов организации БС РФ, работники которых должны быть осведомлены об инцидентах ИБ и их последствиях. Кроме того, компетенция работников указанных подразделений в минимизации тяжести последствий от нарушений выполнения банковских технологических процессов организации БС РФ при различных обстоятельствах должна быть учтена при планировании действий по реагированию на инциденты ИБ. Необходимо, чтобы регламенты реагирования на инциденты ИБ и регламенты восстановления выполнения банковских технологических процессов организации БС РФ были согласованы и учитывали возможность привлечения работников указанных подразделений к деятельности по реагированию на инциденты ИБ;
- подразделения, в зоне компетенции которых находятся вопросы обеспечения физической безопасности и контроля доступом в здания и помещения организации БС РФ, привлечение представителей которых следует обеспечить, если есть основания полагать, что возникли нарушения физической безопасности или инцидент ИБ включает скоординированные несанкционированные действия по логическому и физическому доступу к защищаемым ресурсам. Кроме того, во время выполнения процедур реагирования на инциденты ИБ членам ГРИИБ может потребоваться предоставление доступа в здания и помещения, для которых установлен отдельный режим доступа;
- служба персонала (кадров) организации БС РФ, привлечение представителей которой следует обеспечить, если есть основания полагать, что в процессе реагирования на инцидент ИБ потребуется применение дисциплинарных мер к работнику организации БС РФ, действия которого привели к реализации инцидента ИБ.

6.4. Рекомендации по установлению и документированию регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ

6.4.1. В организации БС РФ рекомендуется установить и документировать регламенты выполнения деятельности на следующих этапах:

— стадия обнаружения и оповещения о событиях ИБ;
— стадия оценки событий ИБ, обнаружения инцидента ИБ и оповещения об инциденте ИБ;
— стадия сбора и фиксации информации об инциденте ИБ;
— стадия закрытия инцидента ИБ.

Указанные регламенты разрабатываются службой ИБ организации БС РФ совместно и (или) по согласованию с подразделением информатизации организации БС РФ, юридической службой организации БС РФ, подразделениями организации БС РФ, в зоне компетенции которых находятся вопросы обеспечения непрерывности выполнения бизнес-процессов организации БС РФ, службой персонала (кадров) организации БС РФ и утверждаются руководством организации БС РФ, например куратором ГРИИБ.

6.4.2. В регламенты обнаружения и оповещения о событиях ИБ рекомендуется включать:

— детальный перечень событий ИБ, при обнаружении которых работники организации БС РФ осуществляют оповещение оператора-диспетчера ГРИИБ;
— детальное описание способов первичного документирования информации о событиях ИБ работниками организации БС РФ, выявившими событие ИБ;
— детальное описание процедур оповещения оператора-диспетчера ГРИИБ и передачи оператору-диспетчеру ГРИИБ документов, содержащих информацию об обнаруженных событиях ИБ;
— детальное описание процедур регистрации оператором-диспетчером ГРИИБ информации об обнаруженном событии ИБ;
— описание порядка хранения информации о событиях ИБ, в том числе в электронном виде.

6.4.3. При формировании перечня событий ИБ рекомендуется осуществлять группирование событий ИБ по уровням информационной инфраструктуры организации БС РФ.

Основными источниками событий ИБ являются:

— технические и программные средства мониторинга ИБ и контроля эксплуатации применяемых защитных мер;
— работники организации БС РФ, выявляющие события ИБ;
— клиенты и партнеры организации БС РФ, включая работников сторонних организаций, имеющих доступ к информационным активам, находящихся под управлением (в распоряжении) организации БС РФ.

6.4.4. В качестве источников информации о событиях ИБ организации БС РФ, формируемых техническими и программными средствами мониторинга ИБ и контроля эксплуатации применяемых защитных мер, рекомендуется использовать:

— регистрационные журналы систем управления, контроля и мониторинга ИБ;
— системные журналы операционных систем;
— системные журналы систем управления базами данных;
— регистрационные журналы прикладного программного обеспечения;
— регистрационные журналы активного сетевого оборудования;
— регистрационные журналы применяемых средств защиты информации, в том числе средств защиты информации от несанкционированного доступа, средств защиты от воздействия вредоносного кода, регистрационные журналы специализированных программно-технических средств обнаружения вторжений и сетевых атак, программного обеспечения проверки целостности файлов;
— информацию специализированных устройств контроля физического доступа, в том числе телевизионных систем охранного наблюдения, систем контроля и управления доступом и охранной сигнализации.

6.4.5. Перечень событий ИБ, выявляемых работниками организации БС РФ, клиентами и партнерами организации БС РФ, составляется экспертным методом и регулярно пересматривается и корректируется, в том числе в связи с возможным появлением новых угроз ИБ, информационных активов, видов деятельности.

Для определения перечня событий ИБ может быть использован примерный перечень типов событий ИБ, приведенный в Приложении 1 к настоящему документу, который рекомендуется скорректировать применительно к специфике деятельности конкретной организации БС РФ.

6.4.6. Способы первичного документирования информации о событиях ИБ должны обеспечивать придание юридической значимости собираемой информации, для чего рекомендуется руководствоваться следующими принципами:

— хранение собранной информации о событиях ИБ должно осуществляться безопасным образом на носителях “только для чтения”;
— при сборе информации о событиях ИБ должны присутствовать не менее двух лиц, действия которых должны протоколироваться;
— необходимо документировать и хранить вместе с собранной информацией описания сервисных команд, использованных для выполнения сбора информации о событиях ИБ;
— целесообразно осуществлять сбор и анализ данных смежных АБС, сервисов и (или) сетей, например, сетевого оборудования и межсетевых экранов.

6.4.7. Рекомендуется определить единую точку входа для информации о событиях ИБ, происходящих в организации БС РФ, которой является оператор-диспетчер ГРИИБ.

Все работники организации БС РФ должны быть ознакомлены с процедурой оповещения о событиях ИБ. Кроме того, в организации БС РФ должны быть определены и выполняться процедуры информирования клиентов и партнеров организации БС РФ о способах оповещения организации БС РФ об обнаруженных событиях ИБ, имеющих отношение к деятельности организации БС РФ.

Все события ИБ, выявляемые работниками организации БС РФ, клиентами и партнерами организации БС РФ, рекомендуется регистрировать с присвоением каждому событию ИБ уникального идентификационного номера.

6.4.8. Рекомендуется обеспечить следующие сроки хранения информации об обнаруженных событиях ИБ:

— событиях ИБ, обнаруженных в рамках банковских платежных технологических процессов, — не менее 5 лет;
— иных событиях ИБ — не менее 3 лет.

6.4.9. В регламенты оценки событий ИБ, обнаружения инцидента ИБ и оповещения об инциденте ИБ рекомендуется включать:

— порядок первичной оценки и критерии классификации событий ИБ в качестве инцидента ИБ;
— порядок использования классификатора инцидентов ИБ и первичной классификации инцидента ИБ;
— порядок оповещения руководителя и членов ГРИИБ об обнаруженном инциденте ИБ;
— порядок и критерии необходимости эскалации инцидента ИБ на центральный уровень реагирования на инциденты ИБ.

6.4.10. Первичная оценка события ИБ и его классификация в качестве инцидента ИБ осуществляется оператором-диспетчером ГРИИБ на основе установленных организацией БС РФ критериев, а также на основе компетентного суждения оператора-диспетчера ГРИИБ.

Вынесение суждения о классификации события ИБ в качестве инцидента ИБ рекомендуется в следующих случаях:

— событие ИБ указывает на нарушение требований законодательства РФ, нормативных актов Банка России, правил платежной системы, внутренних документов организации БС РФ;
— событие ИБ указывает на несанкционированные и (или) нерегламентированные действия в отношении информационных активов организации БС РФ;
— событие ИБ указывает на возможные нарушения в выполнении банковских технологических процессов организации БС РФ;
— событие ИБ указывает на возможное хищение денежных средств и (или) осуществление несанкционированного перевода денежных средств.

6.4.11. Для использования в процессе реагирования на инцидент ИБ рекомендуется определить единую для всех инцидентов ИБ систему их классификации. В случае классификации события ИБ как инцидента ИБ определяются его атрибуты, и далее они используются для управления процессом реагирования на инцидент ИБ и его контроля посредством ведения записи об инциденте ИБ. Порядок определения атрибутов инцидентов ИБ должен быть описан в документе, регламентирующем использование классификатора инцидентов ИБ.

6.4.12. Для оператора-диспетчера ГРИИБ рекомендуется определить детальные и конкретные инструкции оповещения руководителя и членов ГРИИБ об обнаруженном инциденте ИБ, а также эскалации инцидента ИБ на центральный уровень реагирования на инциденты ИБ.

6.4.13. При регламентировании действий целесообразно предусмотреть назначение в каждый момент времени выполнения процесса реагирования на инцидент ИБ ответственного за выполнение соответствующей операции по реагированию из числа членов ГРИИБ.

6.4.14. В регламенты сбора и фиксации информации об инциденте ИБ рекомендуется включать:

- детальное описание источников информации об инциденте ИБ, которые необходимо использовать для сбора информации;
- порядок использования классификатора инцидентов ИБ членами ГРИИБ;
- детальное описание способов документирования и хранения информации об инцидентах ИБ членами ГРИИБ.

6.4.15. Описание источников информации об инциденте ИБ рекомендуется определять для каждого уровня информационной инфраструктуры организации БС РФ на основе перечня источников событий ИБ организации БС РФ, рекомендации к которым установлены в пп. 6.4.3, пп. 6.4.4 настоящих рекомендаций.

6.4.16. Способы документирования информации об инциденте ИБ должны обеспечивать придание юридической значимости собираемой информации, для чего рекомендуется руководствоваться принципами, установленными в пп. 6.4.5 настоящих рекомендаций.

Рекомендуется обеспечить сроки хранения информации об инцидентах ИБ в соответствии с рекомендациями, установленными пп. 6.4.7 настоящих рекомендаций.

6.4.17. В регламенты закрытия инцидента ИБ рекомендуется включать:

- порядок и условия функциональной эскалации инцидента ИБ и (или) привлечения дополнительной компетенции;
- порядок взаимодействия членов ГРИИБ и лиц, привлекаемых к закрытию инцидента ИБ;
- детальное описание способов документирования и хранения информации о результатах реагирования на инцидент ИБ, в том числе закрытия инцидентах ИБ, а также результатах анализа причин инцидента ИБ;
- порядок информирования руководства организации БС РФ о результатах анализа инцидента ИБ;
- порядок подготовки и направления информации об инциденте ИБ, связанном с осуществлением переводов денежных средств, в адрес оператора платежной системы в соответствии с правилами платежной системы и в адрес Банка России в соответствии с требованиями нормативных актов Банка России.

6.5. Рекомендации по выбору технических средств по обнаружению и реагированию на инциденты ИБ и определению порядка их эксплуатации

6.5.1. В состав технических, в том числе программных, средств, используемых в рамках деятельности по обнаружению и реагированию на инциденты ИБ (далее — технические средства), рекомендуется включить:

- технические средства формирования данных, являющихся источниками информации о событиях ИБ и об инцидентах ИБ, в соответствии с рекомендациями, установленными пп. 6.4.4 настоящего документа;
- технические средства централизованного сбора информации о событиях ИБ, корреляции информации о событиях ИБ и обнаружения на основе установленных правил инцидентов ИБ (далее — средства мониторинга ИБ);
- технические средства контроля применяемых в организации БС РФ защитных мер;
- технические средства автоматизации процессов реагирования на инциденты ИБ, включая хранение информации о событиях ИБ и инцидентах ИБ.

6.5.2. Средства мониторинга ИБ и контроля защитных мер должны выполнять следующие основные функции:

- отслеживание и регистрацию событий ИБ в целях обнаружения инцидентов ИБ;
- агрегирование полученной информации о событиях ИБ, корреляцию информации о событиях ИБ, обнаружение инцидентов ИБ на основе установленных в организации БС РФ критериев и правил;
- текущий контроль функционирования применяемых средств защиты информации и обнаружение отклонений в их работе от штатного режима;
- текущий контроль действий пользователей и эксплуатирующего персонала и обнаружение нарушений в эксплуатации технических средств.

6.5.3. Требования к представлению информации о событиях ИБ со стороны компонент информационной инфраструктуры организации БС РФ для ее использования в рамках системы мониторинга ИБ и контроля защитных мер целесообразно формировать на стадии их создания и (или) модернизации.

Для случаев, когда приобретаемое организацией БС РФ прикладное программное обеспечение не обладает функциональными возможностями ведения регистрационных журналов событий ИБ и его доработка не предусмотрена поставщиком, рекомендуется рассмотреть возможность применения компенсирующих функций по формированию информации о событиях ИБ, реализуемых иными компонентами информационной инфраструктуры организации БС РФ, например операционными системами или системами управления базами данных.

6.5.4. Технические средства автоматизации процессов реагирования на инциденты ИБ должны обеспечивать реализацию следующих функций:

- хранение и защиту информации о событиях ИБ и инцидентах ИБ;
- проведение классификации инцидентов ИБ, определение атрибутов инцидентов ИБ в соответствии с применяемым в организации БС РФ классификатором инцидентов ИБ;
- реализацию ролевого доступа к информации об инцидентах ИБ членов ГРИИБ в соответствии с установленными для них ролями в рамках ГРИИБ;
- отслеживание и контроль выполнения этапов реагирования на инцидент ИБ и контроль выполнения членами ГРИИБ установленных регламентов реагирования на инциденты ИБ.

6.5.5. Порядок эксплуатации технических средств должен предусматривать:

- описание состава (количество), мест установки, параметров настроек технических средств;
- описание состава и требований к реализации организационных мер, необходимых для обеспечения эксплуатации технических средств;
- описание правил и процедур эксплуатации технических средств, включая правила и процедуры обновления программного обеспечения технических средств, управления и контроля (мониторинга) параметров их настройки;
- описание ролей и состава функций эксплуатирующего персонала и персонала, осуществляющего контроль эксплуатации технических средств;
- инструкции пользователей и эксплуатирующего персонала, в том числе персонала, осуществляющего контроль эксплуатации технических средств;
- описание правил и процедур контроля доступа эксплуатационного персонала к техническим средствам;
- требования к составу и содержанию организационно-распорядительных документов, необходимых для обеспечения эксплуатации технических средств;
- требования к составу и содержанию организационных мероприятий, необходимых для обеспечения эксплуатации технических средств, в том числе мероприятий по назначению ролей эксплуатирующего персонала, обучению, информированию и повышению осведомленности эксплуатирующего персонала и пользователей;
- описание правил и процедур по обеспечению информационной безопасности при выводе из эксплуатации АБС или по окончании обработки информации.

6.5.6. В организации БС РФ рекомендуется реализовать процедуры контроля соответствия фактических настроек технических средств заданным в эксплуатационной документации. Не рекомендуется наличие субъектов доступа, обладающих единоличными и бесконтрольными возможностями по изменению настроек технических средств. Все действия по изменению настроек технических средств рекомендуется протоколировать и осуществлять под контролем работников службы ИБ по предварительно согласованной программе.

Доступ к информации протоколов изменений настроек технических средств осуществляется только эксплуатирующим персоналом (только чтение), администраторами ИБ и (или) работниками службы ИБ.

6.5.7. В организации БС РФ рекомендуется реализовать процедуры контроля доступа к журналам, содержащим информацию о событиях ИБ и инцидентах ИБ, используемым в соответствии с рекомендациями, установленными пп. 6.4.4 настоящего документа. Управление указанными журналами должно осуществляться уполномоченными работниками службы ИБ.

6.5.8. В организации БС РФ рекомендуется реализовать процедуры обеспечения целостности журналов, содержащих информацию о событиях ИБ и инцидентах ИБ, используемых в соответствии с рекомендациями, установленными пп. 6.4.4 настоящего документа, на случай возможных сбоев в работе и отказов технических и (или) программных средств.

6.5.9. Полный доступ к данным средств мониторинга ИБ предоставляется только уполномоченным членам ГРИИБ и (или) работникам службы ИБ.

6.5.10. С целью обеспечения ИБ при использовании технических средств рекомендуется реализовать:

- запрет несанкционированного доступа к техническим средствам;
- защиту от несанкционированного отключения технических средств;

— защиту от несанкционированного изменения списка событий ИБ, подлежащих регистрации;
— ведения архива файлов с записями информации мониторинга ИБ и журналов регистрации событий ИБ;
— защиту от несанкционированного редактирования или удаления файлов с записями информации мониторинга ИБ и журналов регистрации событий ИБ.

Периодичность архивирования и резервного копирования рекомендуется устанавливать службе ИБ организации БС РФ по согласованию с подразделением информатизации организации БС РФ.

6.5.11. Обязанности по эксплуатации и контролю эксплуатации технических средств рекомендуется отражать в должностных инструкциях работников организации БС РФ.

6.6. Рекомендации по определению порядка осуществления контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ

6.6.1. В организации БС РФ рекомендуется определить регламенты периодического контроля по следующим направлениям:
— контроль выполнения регламентов обнаружения и своевременного оповещения о событиях ИБ;
— контроль актуальности перечня событий ИБ;
— контроль соблюдения принципов первичного документирования информации о событиях ИБ;
— контроль выполнения своевременной оценки событий ИБ, классификации инцидентов ИБ и оповещения об инцидентах ИБ;
— контроль использования классификатора инцидентов ИБ;
— контроль соблюдения регламентов сбора и фиксации информации об инциденте ИБ;
— контроль своевременности принятия мер по закрытию инцидента ИБ, в том числе своевременности эскалации инцидента ИБ и (или) привлечения дополнительной компетенции;
— контроль осведомленности работников организации БС РФ по вопросам обнаружения и реагирования на инциденты ИБ, в том числе осведомленности членов ГРИИБ;
— контроль эксплуатации технических средств.

6.6.2. Организацию контроля за выполнением процессов обнаружения инцидентов ИБ реагирования на инциденты ИБ рекомендуется возложить на куратора ГРИИБ, а непосредственное выполнение контрольных мероприятий на службу ИБ с привлечением работников организации БС РФ — членов ГРИИБ.

7. Рекомендации по реализации в рамках системы менеджмента инцидентов ИБ

7.1. Рекомендации по выделению необходимых ресурсов и назначению ролей в рамках процессов реагирования на инциденты ИБ

7.1.1. В организации БС РФ должно быть организовано назначение следующих ролей:
— ролей, связанных с выполнением задач центрального уровня реагирования на инциденты ИБ;
— ролей, связанных с выполнением задач регионального уровня реагирования на инциденты ИБ;
— ролей членов ГРИИБ;
— ролей работников организации БС РФ, привлекаемых для закрытия инцидентов ИБ;
— ролей работников организации БС РФ, выполняющих функции по эксплуатации технических средств;
— ролей, связанных с выполнением функций по контролю за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ.

7.1.2. Назначение ролей в рамках процессов реагирования на инциденты ИБ рекомендуется осуществлять под общим управлением куратора ГРИИБ.

7.1.3. При распределении и назначении ролей в процессе реагирования на инциденты ИБ рекомендуется учитывать, что для достижения большей эффективности использования персонала необходимо использовать менее квалифицированный персонал для идентификации и

фильтрации ложных сигналов тревоги, обеспечивая при этом привлечение квалифицированного персонала для тех процессов, где требуются его навыки, и только на той стадии процесса, где его содействие необходимо.

7.1.4. Роли должны быть обеспечены всеми необходимыми ресурсами для их выполнения, в том числе:

- регламентами выполнения соответствующей деятельности;
- необходимыми техническими средствами;
- временными и материальными ресурсами, включая помещения, оргтехнику, рабочие места.

7.1.5. Назначение ролей и полномочий для выполнения ролей рекомендуется осуществлять распорядительным актом организации БС РФ, а права доступа к АБС, необходимые для исполнения ролей, предоставлять в соответствии с заявками, утвержденными соответствующими распорядителями доступа к информационным активам.

7.1.6. Взаимодействие структурных подразделений организаций БС РФ в ходе реагирования на инцидент ИБ осуществляется в виде включения представителей структурных подразделений в ГРИИБ, а также путем их привлечения к процессу реагирования на инциденты ИБ. Порядок привлечения работников организации БС РФ к процессу реагирования на инциденты ИБ, включая полномочия привлекаемых работников, должен быть регламентирован.

7.1.7. Взаимодействие структурных подразделений организаций БС РФ в ходе обработки и расследования инцидентов ИБ организует руководитель ГРИИБ, который должен иметь необходимые полномочия.

7.2. Рекомендации по проведению мероприятий по обучению и повышению осведомленности в области обнаружения инцидентов ИБ и реагирования на инциденты ИБ

7.2.1. В организации БС РФ рекомендуется внедрить программу регулярного обучения и повышения осведомленности по следующим основным направлениям:

- повышение осведомленности работников организации БС РФ по вопросам исполнения регламента обнаружения событий ИБ и оповещения о них, в том числе по составу событий ИБ;
- повышение осведомленности представителей внешних организаций и клиентов организации БС РФ, использующих информационную инфраструктуру организации БС РФ, о порядке и процедурах информирования организации БС РФ об обнаруженных инцидентах ИБ;
- обучение и повышение осведомленности членов ГРИИБ и работников организации БС РФ, привлекаемых к реагированию на инциденты ИБ, по вопросам сбора, фиксации и документирования информации об инцидентах ИБ, использования классификатора инцидентов ИБ;
- обучение и повышение осведомленности членов ГРИИБ и работников организации БС РФ, привлекаемых к реагированию на инциденты ИБ, с целью приобретения знаний по технической эксплуатации информационной инфраструктуры организации БС РФ, позволяющих осуществить оперативное закрытие инцидентов ИБ;
- обучение работников подразделений информатизации организации БС РФ по вопросам эксплуатации технических средств;
- обучение работников службы ИБ организации БС РФ по вопросам контроля эксплуатации технических средств.

7.2.2. Рекомендуется ознакомление работников организации БС РФ с процедурой информирования о событиях ИБ, а также о необходимости незамедлительного сообщения об обнаруженных событиях ИБ оператору-диспетчеру ГРИИБ. В процедуры ознакомления рекомендуется включать:

- перечень или описание событий ИБ, о которых требуется сообщать;
- форму сообщения о событиях ИБ, включая детали, существенные для классификации инцидента ИБ, и описание действий по реагированию (например, о типе несоответствия или нарушения, возникновениях неправильных срабатываний, появлении сообщений на экране, нетипичном поведении);
- способы первичного документирования информации о событиях ИБ;
- рекомендации по поведению в случае явных нарушений ИБ, например о выполнении или, наоборот, запрете каких-либо действий, кроме немедленного оповещения оператора-диспетчера ГРИИБ.

7.3. Рекомендации по выполнению деятельности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ

7.3.1. Рекомендуется организовать деятельность по обнаружению и реагированию на инциденты ИБ в соответствии со следующим общим алгоритмом:

- обнаружение событий ИБ, выполняемое работниками организации БС РФ и (или) техническими средствами. Работник организации БС РФ осуществляет первичное документирование информации об обнаруженном событии ИБ и оповещение оператора-диспетчера ГРИИБ в соответствии с установленным регламентом. Для обнаружения событий ИБ работники организации БС РФ используют доведенный до них перечень событий ИБ. Технические средства эксплуатируются в соответствии с документацией, согласованной со службой ИБ организации БС РФ. Информацию о событиях ИБ, выявляемых клиентами и партнерами организации БС РФ, рекомендуется также доводить до оператора-диспетчера ГРИИБ;
- регистрация информации о событиях ИБ, включая сбор информации, связанной с событием ИБ, первичную оценку собранной информации, выполняемые оператором-диспетчером ГРИИБ. Основная задача при первичной оценке — определение, является ли событие ИБ инцидентом ИБ, в частности, произошло ли нарушение ИБ или требований к обеспечению ИБ, установленных для организации БС РФ. Рекомендуется использование технических средств мониторинга ИБ, осуществляющих автоматическое обнаружение инцидентов ИБ из потока информации о событиях ИБ в соответствии с установленными правилами корреляции событий ИБ;
- оповещение членов и (или) руководителя ГРИИБ об инциденте ИБ, выполняемое оператором-диспетчером ГРИИБ. В зависимости от характера инцидента ИБ на основе критериев, установленных в регламенте работы оператора-диспетчера ГРИИБ, оповещается определенный аналитик ГРИИБ, руководитель определенной функциональной группы ГРИИБ и (или) руководитель ГРИИБ;
- вторичная оценка инцидента ИБ, выполняемая аналитиком ГРИИБ с целью подтвердить или опровергнуть то, что обнаруженное событие ИБ является инцидентом ИБ;
- в случае подтверждения того, что обнаруженное событие ИБ является инцидентом ИБ, принятие конкретных мер по закрытию инцидента ИБ, в том числе принятие решения об эскалации инцидента ИБ, устранение нарушения в СОИБ организации БС РФ, прекращение воздействия реализовавшейся угрозы (угроз) ИБ, восстановление выполнения банковских технологических процессов организации БС РФ;
- эскалация инцидента ИБ и привлечение дополнительной компетенции для его обработки. Необходимость эскалации определяет руководитель ГРИИБ и в случае необходимости обращается к куратору ГРИИБ. Эскалация может быть иерархической — если полномочий руководителя ГРИИБ недостаточно для выполнения действий в рамках реагирования на инциденты ИБ, которые, по его мнению, необходимо осуществить (например, прекратить выполнение определенных банковских технологических процессов), а также функциональной — если требуется привлечение специалистов, не входящих в состав ГРИИБ. К иерархической эскалации относится также обращение в ГРИИБ центрального уровня в случае невозможности закрытия инцидента ИБ силами ГРИИБ филиала организации БС РФ или при других обстоятельствах, например в случае невозможности закрытия инцидента ИБ силами ГРИИБ филиала организации БС РФ в установленный срок;
- в случае если инцидент ИБ может привести к судебному разбирательству против лица или организации, а также для проведения дисциплинарных процедур в организации БС РФ вся информация, относящаяся к данному инциденту ИБ, должна быть собрана, сохранена и представлена с целью проведения дальнейшего анализа и возможного принятия судом в качестве доказательства. В зависимости от характера инцидента ИБ желательно максимально полное дублирование журналов о событиях ИБ и об инцидентах ИБ с учетом возможности сохранения необходимости указанных действий и после закрытия инцидента ИБ;
- принятие решения о закрытии инцидента, утверждаемое руководителем ГРИИБ, осуществляемое только после полного восстановления нарушений в СОИБ организации БС РФ, выполнения банковских технологических процессов организации БС РФ, последствий реализации угрозы ИБ, выяснения причин всех проявлений нештатного выполнения бизнес-процессов организации БС РФ и нетипичного поведения работников организации БС РФ.

7.3.2. Управление процессом реагирования на инцидент ИБ, фиксация информации в рамках процесса реагирования на инцидент ИБ осуществляются путем использования классификатора инцидентов ИБ. Классификатор инцидентов ИБ используется для определения и фиксации работниками организации БС РФ, задействованными в деятельности по реагированию на инцидент ИБ, информации об инциденте ИБ (атрибутов инцидента ИБ), выявляемой в процессе реагирования на инцидент ИБ.

7.3.3. Классификатор инцидентов ИБ используется для формализации процесса формирования записи об инциденте ИБ централизованной базы данных об инцидентах ИБ (определения атрибутов инцидента ИБ) на этапах обнаружения инцидента ИБ и реагирования на инцидент ИБ, в том числе при выполнении следующих видов деятельности:

- первичная оценка события ИБ, которая проводится путем определения значений выделенных атрибутов (признаков) инцидента ИБ. Значения этих атрибутов заносятся в создаваемую запись об инциденте ИБ;
- управление процессом оповещения конкретных членов ГРИИБ и руководителя ГРИИБ в зависимости от определенных атрибутов инцидента ИБ;
- принятие решения об эскалации инцидента ИБ в зависимости от определенных атрибутов инцидента ИБ;
- определение значений атрибутов инцидента ИБ работниками организации БС РФ, осуществляющими реагирование на инцидент ИБ;
- определение значений атрибутов инцидента ИБ по результатам закрытия инцидента ИБ;
- фиксация фактов о некорректной (ложной) классификации события ИБ в качестве инцидента ИБ.

7.3.4. При регламентации действий членов ГРИИБ и других работников организации БС РФ, участвующих в реагировании на инциденты ИБ, рекомендуется увязывать эти действия со значениями отдельных атрибутов инцидента ИБ в записи о нем, а также предусматривать ведение записи об инциденте ИБ в соответствии с действующим классификатором инцидентов ИБ.

8. Рекомендации по анализу в рамках системы менеджмента инцидентов ИБ

8.1. В организации БС РФ рекомендуется установить и выполнять процедуры анализа процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ. Выполнение указанных процедур рекомендуется осуществлять под общим руководством куратора ГРИИБ работникам службы ИБ организации БС РФ.

8.2. Выполнение процедур анализа следует осуществлять на основе:

- результатов проведения контроля за выполнением процессов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- анализа статистической отчетности по обнаружению инцидентов ИБ и реагированию на инциденты ИБ;
- анализа записей об инцидентах ИБ, содержащих информацию о нарушениях ИБ, затронутых инцидентом ИБ информационных активах, АБС, степени тяжести последствий от обнаруженных инцидентов ИБ.

8.3. В результате анализа рекомендуется определять наиболее проблемные с точки зрения подверженности инцидентам ИБ сегменты и компоненты информационной инфраструктуры организации БС РФ, наиболее существенные уязвимости и недостатки в обеспечении ИБ, оценивать достаточность принятых мер и выделенных ресурсов для реагирования на инциденты ИБ.

Кроме того, рекомендуется анализировать наличие тенденций, которые могут указывать на потребности в совершенствовании СОИБ организации БС РФ.

8.4. Дополнительному анализу подлежат действия работников организации БС РФ, осуществляемые при реагировании на инциденты ИБ. Целью проведения анализа является формирование (инициирование) совершенствований в части:

- корректировки установленных регламентов обнаружения инцидентов ИБ и реагирования на инциденты ИБ;
- изменения состава ГРИИБ и корректировка состава лиц, привлекаемых к реагированию на инциденты ИБ;
- изменения требований к квалификации членов ГРИИБ;
- корректировки порядка взаимодействия лиц, осуществляющих реагирование на инциденты ИБ;
- корректировки порядка эксплуатации технических средств.

8.5. Результаты анализа обнаружения инцидентов ИБ и реагирования на инциденты ИБ целесообразно использовать в качестве основы для инициирования и реализации процесса проведения тактических и стратегических улучшений СОИБ организации БС РФ, требования к выполнению которого установлены СТО БР ИИБС-1.0.

8.6. Для определения направлений и способов улучшения процессов менеджмента инцидентов ИБ рекомендуется на основе анализа документов и отчетов по инцидентам ИБ провести анализ эффективности применяемых процедур обнаружения инцидентов ИБ и реагирования на инциденты ИБ, в частности:

— оценить адекватность применяемого состава регистрируемых событий ИБ и потребность в его корректировке;
— оценить адекватность используемого классификатора инцидентов ИБ и потребность в его корректировке;
— оценить эффективность используемых процедур мониторинга ИБ;
— оценить адекватность регламентов реагирования на инциденты ИБ.

8.7. При выработке предложений по совершенствованию процессов менеджмента инцидентов ИБ рекомендуется учитывать:

— доступные сведения о соответствующем опыте сторонних организаций;
— изменения в законодательстве РФ, требованиях нормативных актов Банка России, правил платежной системы, внутренних документов организации БС РФ.

8.8. В организации БС РФ рекомендуется установить процедуры информирования руководства организации БС РФ о результатах анализа процессов менеджмента инцидентов ИБ, а также о значимых инцидентах ИБ, оказывающих существенное негативное влияние на выполнение бизнес-процессов организации БС РФ.

9. Рекомендации к классификации инцидентов ИБ и использованию классификатора инцидентов ИБ в процессе их обработки

9.1. Основной целью проведения классификации инцидентов ИБ является повышение степени системности и минимизация субъективности при реализации процессов реагирования на инциденты ИБ, осуществляемые путем определения и фиксации атрибутов инцидента ИБ для дальнейшего их использования в ходе реагирования на инцидент ИБ, а также при анализе системы менеджмента инцидентов ИБ.

9.2. При проведении классификации ИБ рекомендуется осуществлять описание инцидентов ИБ с помощью предварительно установленного набора признаков (атрибутов), при этом значения атрибутов должны задаваться максимально конкретно по определенным правилам.

9.3. Используемый организацией БС РФ классификатор инцидентов ИБ должен давать возможность его адаптации, дополнения, расширения, для чего структура классификатора инцидентов ИБ должна позволять:

— введение дополнительных атрибутов или значений атрибутов;
— проведение классификации вновь обнаруженных инцидентов ИБ без нарушения целостности и изменения установленных процессов классификации.

9.4. Для классификации инцидентов ИБ необходимо определить набор атрибутов, характеризующих инцидент ИБ, для каждого атрибута — значения, которые он может принимать.

Процедура классификации инцидента ИБ состоит в присвоении для конкретного инцидента ИБ соответствующих значений классификационным атрибутам. При этом для конкретного инцидента ИБ могут быть использованы не все атрибуты или значения некоторых атрибутов инцидента ИБ могут определяться постепенно по мере выполнения деятельности по реагированию на него.

9.5. Набор значений атрибутов для конкретного инцидента ИБ представляет собой запись об инциденте ИБ, которая вносится в централизованную базу инцидентов ИБ. Рекомендуется сформировать и поддерживать в актуальном состоянии централизованную базу данных инцидентов ИБ, структуру записей которой рекомендуется задавать на основе классификатора инцидентов ИБ.

9.6. Роли по классификации инцидентов ИБ назначаются членам ГРИИБ и работникам, привлекаемым к реагированию на инциденты ИБ.

9.7. Инциденты ИБ рекомендуется классифицировать по следующим признакам:

— по степени тяжести последствий для деятельности организации БС РФ (в денежном выражении, в балльной шкале);

— по степени вероятности повторного возникновения инцидента ИБ;
— по видам источников угроз ИБ, вызывающих инциденты ИБ;
— по преднамеренности возникновения инцидента ИБ (случайный, намеренный, ошибочный);
— по видам объектов информационной инфраструктуры, задействованных (пораженных) при реализации инцидента ИБ;
— по уровню информационной инфраструктуры, на котором происходит инцидент ИБ;
— по нарушенным свойствам информационной безопасности (конфиденциальность, целостность, доступность);
— по типу инцидента ИБ (свершившийся инцидент ИБ, попытка осуществления инцидента ИБ, подозрение на инцидент ИБ);
— по области распространения и действия инцидента ИБ (в пределах одной АБС, в пределах отдельного структурного подразделения организации БС РФ, в организации БС РФ в целом, выходящий за пределы организации БС РФ);
— по сложности обнаружения инцидента ИБ;
— по сложности закрытия инцидента ИБ;
— по другим признакам, устанавливаемым организацией БС РФ.

9.8. Признаки классификации инцидентов ИБ рекомендуется определять с учетом формирования на основе результатов классификации инцидентов ИБ отчетных форм, представляемых организацией БС РФ в соответствии с требованиями законодательства РФ, нормативных актов Банка России и правилами платежных систем.

9.9. Классификатор инцидентов ИБ рекомендуется использовать на всех этапах обнаружения инцидента ИБ и реагирования на инцидент ИБ. Рекомендуется установить состав атрибутов инцидентов ИБ, возможных для заполнения на каждом из этапов реагирования на инцидент ИБ.

9.10. В Приложении 2 к настоящему документу содержится примерный классификатор инцидентов ИБ.

РС БР ИББС-2.5-2014

Приложение 1. Примерный перечень типов событий ИБ

Физический уровень информационной инфраструктуры:

— физический доступ работников организации БС РФ и иных лиц в здания и помещения организации БС РФ;
— физический доступ работников организации БС РФ и иных лиц к средствам вычислительной техники и использование указанными субъектами средств вычислительной техники;
— использование работниками организации БС РФ и иными лицами устройств копирования и многофункциональных устройств;
— использование работниками организации БС РФ и иными лица аппаратов факсимильной связи;
— изменение параметров настроек средств вычислительной техники, телекоммуникационного оборудования;
— изменение параметров настроек оборудования, обеспечивающего функционирование средств вычислительной техники;
— сбои и отказы в работе средств вычислительной техники, телекоммуникационного оборудования;
— сбои и отказы в работе оборудования, обеспечивающего функционирование средств вычислительной техники;
— сбои и отказы в работе средств защиты информации;
— сбои и отказы в работе сети телефонной связи;
— отказы в работе сетей передачи данных;
— физическое воздействие на средства вычислительной техники, телекоммуникационное оборудование, средства защиты информации и сети передачи данных;
— изменения климатических режимов помещений, в которых расположены средства вычислительной техники, телекоммуникационное оборудование;
— изменения параметров функционирования сетей передачи данных;
— замена и (или) модификация программных и (или) аппаратных частей средств вычислительной техники, телекоммуникационного оборудования;
— осуществление действий с носителями информации, в том числе вынос за пределы территории объектов организации БС РФ носителей информации;
— вынос за пределы организации БС РФ переносных средств вычислительной техники;
— использование переносных средств вычислительной техники на территории объектов организации БС РФ;
— передача средств вычислительной техники между подразделениями организации БС РФ;
— передача средств вычислительной техники во внешние организации;
— проведение работниками организации БС РФ и иными лицами фото- и (или) видеосъемки в зданиях или помещениях организации БС РФ;
— проведение мероприятий по доступу к телевизионным системам охранного наблюдения, охранной сигнализации, системам контроля и управления доступом;
— события, формируемые телевизионными системами охранного наблюдения, охранной сигнализации, системами контроля и управления доступом;
— осуществление действий с носителями информации и системами, позволяющими осуществить физический доступ в здания и помещения организации БС РФ.

Уровень сетевого оборудования:

— изменение параметров настроек сетевого оборудования и программного обеспечения сетевого оборудования;
— изменение состава и версий программного обеспечения сетевого оборудования;
— обнаружение аномальной сетевой активности;
— аутентификация и завершение сеанса работы на сетевом оборудовании;
— обнаружение вредоносного кода и его проявлений;
— изменение топологии вычислительных сетей;
— подключение оборудования к вычислительным сетям;
— сбои в работе программного обеспечения сетевого оборудования;
— обновление программного обеспечения сетевого оборудования;
— выполнение операций по техническому обслуживанию сетевого оборудования;
— использование средств анализа уязвимостей сетевого оборудования;
— отключение/перезагрузка сетевого оборудования;
— обнаружение атак типа “отказ в обслуживании”;

— смена и (или) компрометация аутентификационных данных, используемых для доступа к сетевому оборудованию;
— сбои в работе средств защиты информации;
— изменение параметров работы средств защиты информации;
— запуск средств анализа топологии вычислительной сети.

Уровень сетевых приложений и сервисов:

— идентификация, аутентификация, авторизация и завершение сеанса работников организации БС РФ и иных лиц;
— изменение параметров настроек, состава и версий программного обеспечения;
— обнаружение вредоносного кода и его проявлений;
— установление соединений и обработка запросов, в том числе удаленных, на уровне сетевых приложений и сервисов;
— сбои и отказы в работе сетевых приложений и сервисов;
— выполнение операций, связанных с эксплуатацией и администрированием сетевых приложений и сервисов;
— обнаружение нетипичных (аномальных) запросов на уровне сетевых приложений и сервисов;
— отключение/перезагрузка или приостановление работы сетевых приложений и сервисов;
— выполнение операций по предоставлению доступа к использованию сетевых приложений и сервисов, в том числе использованию электронной почты и сети Интернет;
— выполнение операции по архивированию данных сетевых приложений и сервисов, в том числе данных электронной почты;
— осуществление операций по обмену сообщениями, в том числе обмену платежными сообщениями;
— сбои в осуществлении обменом сообщениями, в том числе в обмене платежными сообщениями;
— искажение, модификация сообщений, в том числе платежных сообщений;
— аутентификация сообщений, в том числе платежных сообщений;
— аутентификация автоматизированных рабочих мест — участников обмена сообщениями, в том числе платежными сообщениями;
— завершение/приостановка выполнения сетевых приложений и сервисов по ошибке;
— распространение и (или) сбор информации с использованием сетевых приложений и сервисов;
— выполнение операций со списками рассылки и адресными книгами;
— наделение работников организации БС РФ и (или) иных лиц правами пользователя конкретного пакета сервисов, в том числе сервисов и ресурсов сети Интернет;
— использование средств анализа уязвимостей сетевых приложений и сервисов;
— смена и (или) компрометация аутентификационных данных, используемых для осуществления доступа к сетевым приложениям и сервисам;
— сбои в работе средств защиты информации;
— переадресация сообщений, в том числе платежных сообщений;
— распространение информации, побуждающей клиента сообщать информацию, необходимую для осуществления действий от его имени;
— внешние воздействия из сети Интернет, в том числе сетевые атаки;
— выполнение операций со средствами криптографической защиты информации и ключевой информацией.

Уровень операционных систем:

— аутентификация и завершение работы работников организации БС РФ и иных лиц, в том числе на уровне системного программного обеспечения, систем управления базами данных и прикладного программного обеспечения, программного обеспечения АБС (далее — программное обеспечение уровня операционных систем);
— изменение параметров конфигурации, состава и версий программного обеспечения уровня операционных систем;
— запуск, остановка и (или) отключение/перезагрузка программного обеспечения уровня операционных систем;
— обнаружение вредоносного кода и его проявлений;
— установление соединений и обработка запросов с использованием программного обеспечения уровня операционных систем;

— сбои в работе программного обеспечения уровня операционных систем;
— выполнение операций, связанных с эксплуатацией и администрированием программного обеспечения уровня операционных систем;
— обнаружение нетипичных запросов с использованием программного обеспечения уровня операционных систем;
— сбои и отказы в работе средств защиты информации;
— изменение параметров конфигурации средств защиты информации;
— выполнение операций по предоставлению доступа к программному обеспечению уровня операционных систем и информационным ресурсам, обрабатываемым с использованием программного обеспечения уровня операционных систем;
— выполнение операций по архивированию, резервированию и восстановлению информации;
— завершение/приостановка работы программного обеспечения уровня операционных систем по ошибке;
— использование средств анализа уязвимостей программного обеспечения уровня операционных систем;
— смена и (или) компрометация аутентификационных данных, используемых для доступа к программному обеспечению уровня операционных систем, и информационным ресурсам, обрабатываемым с использованием программного обеспечения уровня операционных систем;
— изменение параметров конфигурации средств защиты информации;
— внешние воздействие из сети Интернет на программное обеспечение уровня операционных систем;
— создание, авторизация, уничтожение или изменение платежной информации;
— создание, уничтожение или изменение информационных ресурсов, баз данных и (или) иных массивов информации;
— компрометация аутентификационных данных и ключевой информации;
— выполнение операций со средствами криптографической защиты информации и ключевой информацией.

Уровень технологических процессов и приложений и уровень бизнес-процессов организации БС РФ:

— выполнение отдельных операций или процедур в рамках банковских платежных и информационных технологических процессов;
— контроль выполнения операций или процедур в рамках банковских платежных и информационных технологических процессов;
— осуществление операций или процедур в рамках банковских платежных и информационных технологических процессов с использованием средств криптографической защиты информации;
— выполнение отдельных этапов жизненного цикла АБС;
— контроль выполнения отдельных этапов жизненного цикла АБС;
— выделение и назначение ролей, в том числе ролей, связанных с обеспечением ИБ.

Приложение 2. Примерный классификатор инцидентов ИБ

Атрибут инцидента ИБ	Описание значений атрибута инцидента ИБ
Группа 1. Атрибуты регистрации	
1.1. Уникальный идентификатор инцидента ИБ	номер или иной идентификатор, позволяющий ссылаться на инцидент ИБ
1.2. Дата и время обнаружения инцидента ИБ	
1.3. Источник информации об инциденте ИБ	работник организации БС РФ или техническое средство
1.4. Фамилия, имя, отчество работника организации БС РФ, выявившего инцидент ИБ	
1.5. Подразделение работника организации БС РФ, выявившего инцидент ИБ	
1.6. Должность работника организации БС РФ, выявившего инцидент ИБ	
1.7. Роль работника организации БС РФ, выявившего инцидент ИБ	(пользователь, администратор АБС, администратор ИБ, работник службы ИБ)
1.8. Контактная информация работника организации БС РФ, выявившего инцидент ИБ	данные, позволяющие связаться с работником
1.9. Наименование технического средства, с использованием которого обнаружен инцидент ИБ	
1.10. Описание инцидента ИБ	сообщение работника или информация, выданная ТС
Группа 2. Атрибуты, описывающие содержание инцидента ИБ	
2.1. Факт нарушения требований к обеспечению ИБ	– “нет”; – “реквизиты документа, пункт документа”
2.2. Данные о нарушителе требований к обеспечению ИБ	– “нет”; – “Фамилия И.О., должность нарушителя”
2.3. Факт нарушения работы средств защиты информации (далее – СЗИ)	– “нет”; – “выход из строя СЗИ”; – “сбой СЗИ”; – “недоступность критичной для выполнения функций СЗИ информации (например, выход из строя носителей ключевой информации)”; – “нарушение целостности программного обеспечения СЗИ”; – “отклонение параметров настроек СЗИ”; – “снижение функциональных характеристик (параметров) СЗИ”
2.4. Факт реализации угрозы ИБ	– “нет”; – “идентификатор источника угрозы согласно модели угроз или действующему перечню актуальных угроз ИБ”
2.5. Факт нарушения свойств безопасности	– “нет”; – “Конфиденциальность”; – “Целостность”; – “Доступность”; – “Иные свойства”
2.6. Факт нестандартного (несанкционированного) поведения	– “нет”; – “нарушение установленного порядка и режима дня”; – “отклонение от сложившегося порядка и режима использования информационных ресурсов”
2.7. Факт преднамеренности возникновения инцидента ИБ	– “случайный”; – “намеренный”; – “ошибочный”
2.8. Тип инцидента ИБ	– “свершившийся”; – “попытка осуществления инцидента ИБ”; – “подозрение на инцидент ИБ”
2.9. Степень сложности обнаружения инцидента ИБ	– “Обычная”; – “Высокая”

Атрибут инцидента ИБ	Описание значений атрибута инцидента ИБ
Группа 3. Атрибуты, описывающие воздействие объекты информационной инфраструктуры	
3.1. Тип информационных активов, затронутых инцидентом ИБ	– “нет” (информационные активы не затронуты); – “платежная информация”; – “финансово-аналитическая информация”; – “служебная информация”; – “управляющая информация общего и специального назначения”; – “справочная информация”; – “информация операционной и телекоммуникационной среды”
3.2. Затронутые объекты информационной инфраструктуры	– “нет”; – “линии и сети передачи данных”; – “сетевые программные и аппаратные средства”; – “прочие технические средства”; – “файлы данных, базы данных”; – “носители информации (в том числе бумажные носители)”; – “прикладные и общесистемные программные средства”; – “программно-технические компоненты автоматизированных систем”; – “помещения, здания, сооружения, инженерные сети и коммуникации”; – “автоматизированные рабочие места”
3.3. Характеристика банковских технологических процессов	– “нет” (нет информационно-технологических процессов, затронутых инцидентом ИБ); – “платежные технологические процессы”; – “информационные технологические процессы”
3.4. Уровень инцидента ИБ	– “физический”; – “сетевой”; – “операционных систем”; – “систем управления базами данных”; – “банковских технологических процессов и приложений”; –”бизнес-процессов организации”
3.5. Степень тяжести последствий	– “нет”; – “минимальная”; – “средняя”; – “высокая”; – “критическая”
3.6. Степень вероятности повторного возникновения инцидента ИБ	– “нет”; – “минимальная”; – “средняя”; – “высокая”; – “критическая”
3.7. Область распространения и действия инцидента ИБ	– “пределы одной АБС”; – “пределы отдельного структурного подразделения организации БС РФ”; – “организации БС РФ в целом”; – “выходящий за пределы организации БС РФ”
Группа 4. Атрибуты, отражающие значимость инцидента ИБ	
4.1. Приоритет инцидента ИБ	– “0 (Наивысший)”; – “1 (Высокий)”; – “2 (Повышенный)”; – “3 (Средний)”; – “4 (Низкий)”; – “5 (Минимальный)”
4.2. Срочность реагирования на инцидент ИБ	– “Обычная”; – “Высокая”
Группа 5. Атрибуты, связанные с реагированием на инцидент ИБ	
5.1. Доклад о возникновении инцидента ИБ	– “нет”; – “время доклада и кому доложено”
5.2. Доклад об устранении инцидента ИБ	– “нет”; – “время доклада и кому доложено”
5.3. Эскалация инцидента ИБ	– “нет”; – “да”
5.4. Функциональная группа	– “нет”; – “наименование функциональной группы специалистов, которой поручено реагирование на инцидент ИБ”

Атрибут инцидента ИБ	Описание значений атрибута инцидента ИБ
5.5. Время назначения функциональной группы	– “нет”; – “время, когда была назначена функциональная группа, ответственная за реагирование на инцидент ИБ”
5.6. Назначение специалиста – члена ГРИИБ	– “нет”; – “фамилия специалиста, ответственного за реагирование на инцидент ИБ”
5.7. Статус инцидента ИБ	– “Зарегистрирован; – “Назначен”; – “В работе”; – “Закрыт”
5.8. Этап реагирования на инцидент ИБ	
5.9. Установленный срок закрытия инцидента ИБ	– “нет”; – “установленный срок закрытия инцидента ИБ”
5.10. Применение иных мероприятий:	– “нет”; – “описание мероприятий по закрытию инцидента ИБ”
5.11. Необходимость информирования об инциденте ИБ структурных подразделений организации БС РФ.	– “нет”; – “перечень подразделений”.
Группа 6. Атрибуты, связанные с закрытием инцидента ИБ	
6.1. Дата и время закрытия инцидента ИБ	– “нет”; – дата и время.
6.2. Последствия (ущерб) для организации БС РФ от воздействия инцидента ИБ	– “нет”; – “описание ущерба (последствий) в текстовой форме”
6.3. Степень сложности закрытия инцидента ИБ	– “Обычная”; – “Высокая”
6.4. Необходимость информирования о закрытии инцидента ИБ структурных подразделений организации БС РФ	– “нет”; – “перечень подразделений”

Библиография

1. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности”.
2. ГОСТ Р ИСО/МЭК ТО 18044-2007 “Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности”.

Ключевые слова: банковская система Российской Федерации, система менеджмента информационной безопасности, политика информационной безопасности, инциденты информационной безопасности, менеджмент инцидентов информационной безопасности.

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЕСТНИК БАНКА РОССИИ

Нормативные акты и оперативная информация
Центрального банка Российской Федерации

№ 48—49 (1526—1527)

30 МАЯ 2014

МОСКВА

Учредитель — Центральный банк Российской Федерации
107016, Москва, ул. Неглинная, 12
Адрес официального сайта Банка России: *http://www.cbr.ru*
Тел. 8 (495) 771-43-73, факс 8 (495) 623-83-77, e-mail: *mvg@cbr.ru*

Издание зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Регистрационный номер ПИ № ФС77-47238

Издатель и распространитель: ЗАО "АЭИ "ПРАЙМ"
119021, Москва, Зубовский б-р, 4
Тел. 8 (495) 974-76-64, факс 8 (495) 637-45-60, *www.1prime.ru,* e-mail*: sales01@1prime.ru*

Отпечатано в ООО "Типография "Возрождение"
117105, Москва, Варшавское ш., 37а, стр. 2

Москва, 2014