содержание

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

В целях выполнения в организациях банковской системы Российской Федерации требований Федерального закона "О персональных данных" и требований (рекомендаций) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю Банком России введены в действие с 21 июня 2010 года документы Комплекса документов в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации" (далее — документы Комплекса БР ИББС):

четвертая редакция стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения" (СТО БР ИББС-1.0-2010);

третья 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-1.0-2010" (СТО БР ИББС-1.2-2010);

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).

Проекты документов обсуждены банковским сообществом и рекомендованы к вводу в действие решением Подкомитета по стандартизации "Защита информации в кредитно-финансовой сфере" (ПК3) Технического комитета по стандартизации "Защита информации" (ТК362) Федерального агентства по техническому регулированию и метрологии.

Держателем контрольных экземпляров Комплекса БР ИББС определено Главное управление безопасности и защиты информации Банка России.

Ответственный представитель держателя контрольных экземпляров, а также контактное лицо по вопросам тиражирования и распространения официальных копий — заместитель начальника Главного управления безопасности и защиты информации Банка России **Курило Андрей Петрович.**

Почтовый адрес: 107016, г. Москва, ул. Неглинная, 12
Телефон (495) 771-91-61
E-mail: *kap1@cbr.ru*

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.0-2010

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2010-06-21

Издание официальное

Предисловие

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

2. ВЗАМЕН СТО БР ИББС-1.0-2008.

Содержание

Введение

Банковская система (БС) Российской Федерации (РФ) включает в себя Банк России, кредитные организации, а также филиалы и представительства иностранных банков [1]. Развитие и укрепление БС РФ, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ 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-1.0-2010

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2010-06-21

1. Область применения

Настоящий стандарт распространяется на организации банковской системы Российской Федерации (далее — 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 нормативных и методических 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. 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:
ГОСТ Р ИСО 9001-2008 Система менеджмента качества. Требования

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 и кредитные организации, а также филиалы и представительства иностранных банков [1].

3.2. **Стандарт:** Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Примечание.

Стандарт также может содержать 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”.

---

[1] См. п. 3.4.

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, которое 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 [3].

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 банковской системы Российской Федерации и находится в ее распоряжении.

Примечание.

К активам организации банковской системы Российской Федерации 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 банковской системы Российской Федерации; находящаяся в распоряжении организации банковской системы Российской Федерации 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 банковской системы Российской Федерации 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 банковской системы Российской Федерации, 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 банковской системы Российской Федерации, используемых при функционировании или необходимых для реализации банковских услуг.

Примечания.

1. Операции над активами организации банковской системы Российской Федерации 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 банковские операции над информационными активами организации банковской системы Российской Федерации, связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций.

3.29. **Банковский информационный технологический процесс:** Часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования организации банковской системы Российской Федерации и не являющихся платежной информацией.

Примечания.

1. Платежная информация — информация, содержащаяся в документах, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой.

2. Неплатежная информация, необходимая для функционирования организации банковской системы Российской Федерации, может включать в себя, например, данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.

3.30. **Автоматизированная банковская система:** Автоматизированная система, реализующая технологию выполнения функций организации банковской системы Российской Федерации.

3.31. **Комплекс средств автоматизации автоматизированной банковской системы:** Совокупность всех компонентов автоматизированной банковской системы организации банковской системы Российской Федерации, за исключением людей.

3.32. **Безопасность:** Состояние защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз.

3.33. **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 банковской системы Российской Федерации.

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.

3.34. **Доступность информационных активов:** Свойство ИБ организации банковской системы Российской Федерации, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

3.35. **Целостность информационных активов:** Свойство ИБ организации банковской системы Российской Федерации сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах.

3.36. **Конфиденциальность информационных активов:** Свойство ИБ организации банковской системы Российской Федерации, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

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

3.38. **Система менеджмента информационной безопасности; СМИБ:** Часть менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

3.39. **Система обеспечения информационной безопасности; СОИБ:** Совокупность СИБ и СМИБ организации банковской системы Российской Федерации.

3.40. **Область действия системы обеспечения информационной безопасности; область действия СОИБ:** Совокупность информационных активов и элементов информационной инфраструктуры организации банковской системы Российской Федерации.

3.41. **Осознание необходимости обеспечения информационной безопасности; осознание ИБ:** Понимание руководством организации банковской системы Российской Федерации 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 банковской системы Российской Федерации 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.

3.42. **Защитная мера:** Сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ организации банковской системы Российской Федерации.

3.43. **Угроза информационной безопасности; угроза ИБ:** Угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организации банковской системы Российской Федерации.

3.44. **Уязвимость информационной безопасности; уязвимость ИБ:** Слабое место в инфраструктуре организации банковской системы Российской Федерации, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.

3.45. **Ущерб:** Утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры организации или другой вред активам и (или) инфраструктуре организации банковской системы Российской Федерации, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

3.46. **Инцидент информационной безопасности; инцидент ИБ:** Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Примечания.

1. Реализация угрозы ИБ — реализация нарушения свойств ИБ информационных активов организации банковской системы Российской Федерации.

2. Нарушение может вызываться источниками угроз ИБ: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств, природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.

3.47. **Нарушитель информационной безопасности; нарушитель ИБ:** Субъект, реализующий угрозы ИБ организации банковской системы Российской Федерации, нарушая предоставленные ему полномочия по доступу к активам организации банковской системы Российской Федерации или по распоряжению ими.

3.48. **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.

3.49. **Модель угроз информационной безопасности; модель угроз ИБ:** Описание 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.

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

3.51. **Оценка риска нарушения информационной безопасности:** Систематический и документированный процесс выявления, сбора, использования и анализа информации, позво-

ляющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации банковской системы Российской Федерации на всех стадиях их жизненного цикла.

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

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

3.54. **Допустимый риск нарушения информационной безопасности:** Риск нарушения ИБ, предполагаемый ущерб от которого организация банковской системы Российской Федерации в данное время и в данной ситуации готова принять.

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

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

3.57. **Свидетельства выполнения деятельности по обеспечению информационной безопасности:** Документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ организации банковской системы Российской Федерации.

3.58. **Политика информационной безопасности; политика ИБ:** Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации банковской системы Российской Федерации в целом.

3.59. **Частная политика информационной безопасности; частная политика ИБ:** Документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации банковской системы Российской Федерации.

3.60. **Мониторинг:** Постоянное наблюдение за объектами и субъектами, влияющими на ИБ организации банковской системы Российской Федерации, а также сбор, анализ и обобщение результатов наблюдений.

3.61. **Аудит информационной безопасности; аудит ИБ:** Систематический, независимый и документируемый процесс получения свидетельств деятельности организации банковской системы Российской Федерации по обеспечению ИБ, установления степени выполнения в организации банковской системы Российской Федерации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ организации банковской системы Российской Федерации.

Примечание.

Аудит ИБ выполняется работниками организации, являющейся внешней по отношению к организации банковской системы Российской Федерации.

3.62. **Критерии оценки (аудита) информационной безопасности; критерии оценки (аудита) ИБ:** Совокупность требований в области ИБ, определенных стандартом Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” или его частью.

3.63. **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.

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

3.65. **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.

3.66. **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.

3.67. **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;
ЭЦП — электронная цифровая подпись.

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.

---

[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).

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

Незлоумышленные действия собственных работников создают либо уязвимости ИБ, либо инциденты, влияющие на свойства доступности, целостности и конфиденциальности 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 снижения рисков нарушения ИБ и управления ими 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, тем потенциально ниже риски нарушения ИБ организации БС РФ при минимальных ресурсных затратах. 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 минимизации рисков нарушения ИБ организации БС РФ — 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 Российской Федерации, 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 всемерно 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 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.

5.14. Любой целенаправленной деятельности (бизнесу) свойственны риски. Это объективная реальность, и понизить эти риски можно лишь до определенного остаточного уровня.

---

[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) используются имеющийся опыт и знания, поэтому чем выше знания, тем точнее прогноз.

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.

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. Анализ и оценка рисков нарушения ИБ должна 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, 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 и ИБ ISO/IEC IS 27001-2005 [4]. 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 Российской Федерации, 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 прояв-

ляется 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 принимается либо 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 нижние уровни, требующее специфических опыта, знаний и ресурсов (в т.ч. временных) и поэтому менее эффективное по соотношению “затраты / получаемый результат”.

Другими целями злоумышленника могут являться, например, нарушение функционирования бизнес-процессов организации БС РФ путем нарушения доступности или целостности информационных активов, 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 различна и определяется реальными потребностями для каждой организации в отдельности.

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 банковской системы Российской Федерации. 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.

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;

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

— 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:
— банковский платежный технологический процесс;
— платежную информацию.

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 и документально определены роли ее работников.

---

[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.

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

7.2.2. Роли следует персонифицировать с установлением ответственности за их выполнение. Ответственность должна быть документально зафиксирована в должностных инструкциях.

7.2.3. С целью снижения рисков нарушения ИБ не рекомендуется, чтобы в рамках одной роли совмещались следующие функции: разработки и сопровождения системы/ПО, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в системе и контроля их выполнения.

7.2.4. В организации БС РФ должны быть документально определены и выполняться процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации БС РФ.

7.2.5. В организации БС РФ должны быть документально определены 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 документальную фиксацию результатов проводимых проверок.

7.2.6. Рекомендуется документально определить процедуры регулярной проверки (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников, а также внеплановой проверки (с документальной фиксацией результатов) — 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. При формировании требований по обеспечению ИБ рекомендуется 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 разработки АБС в организации БС РФ рекомендуется рассматривать все стадии ЖЦ АБС, а в случае приобретения готовых АБС рекомендуется рассматривать стадии 4—7 ЖЦ АБС.

7.3.2. Разработка технических заданий и приемка АБС должны осуществляться по согласованию и при участии подразделения (лиц) в организации БС РФ, ответственного за обеспечение ИБ.

7.3.3. Ввод в действие, эксплуатация и сопровождение (модернизация), снятие с эксплуатации АБС должны осуществляться под контролем подразделения (лиц) в организации, ответственного за обеспечение ИБ.

7.3.4. Привлекаемые для разработки и (или) производства средств и систем защиты АБС на договорной основе специализированные организации должны иметь лицензии на данный вид деятельности в соответствии с законодательством РФ.

7.3.5. Разрабатываемые АБС и (или) их компоненты должны быть снабжены документацией, содержащей описание реализованных защитных мер, в том числе в отношении угроз ИБ (источников угроз), описанных в модели угроз организации БС РФ. Приобретаемые организацией БС РФ готовые АБС и (или) их компоненты рекомендуется снабжать указанной документацией.

Также документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты должна содержать описание реализованных защитных мер, предпринятых разработчиком относительно безопасности разработки и безопасности поставки.

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 рабочей конструкторской 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 документально оформить допустимость риска нарушения ИБ, возникающего при невозможности сопровождения АБС и их компонентов.

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

- попыток доступа к банковской информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования;
- возможности ошибок авторизованных пользователей систем;
- возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями.

7.3.7. На стадии тестирования должны обеспечиваться анонимность данных и проверка адекватности разграничения доступа.

7.3.8. На стадии эксплуатации АБС должны быть документально определены и выполняться процедуры контроля работоспособности (функционирования, эффективности) реализованных в АБС защитных мер. Результаты выполнения контроля должны документироваться.

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

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

Результаты выполнения контроля должны документироваться.

7.3.10. На стадии сопровождения (модернизации) при любом внесении изменения в АБС должны проводиться процедуры проверки функциональности, результаты которой должны документально фиксироваться.

7.3.11. На стадии снятия с эксплуатации должны быть документально определены и выполняться процедуры, обеспечивающие удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС и с внешних носителей, за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами. Результаты выполнения процедур должны документироваться.

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

7.4.1. Должен быть документально определен перечень информационных активов (их типов) организации БС РФ. Права доступа работников и клиентов организации БС РФ к данным активам должны быть документально зафиксированы.

7.4.2. В составе АБС должны применяться встроенные защитные меры, а также рекомендуются к использованию сертифицированные или разрешенные руководством организации БС РФ к применению средства защиты информации от НСД и НРД.

7.4.3. В организации БС РФ должны быть документально определены и утверждены руководством, выполняться и контролироваться процедуры идентификации, аутентификации, авторизации; управления доступом; контроля целостности; регистрации событий и действий.

Процедуры управления доступом должны исключать возможность “самосанкционирования”.

Результаты контроля процедур должны документироваться.

7.4.4. В организации БС РФ необходимо документально определить процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Для проведения процедур мониторинга и анализа данных регистрации, действий и операций рекомендуется использовать специализированные программные и (или) технические средства.

Процедуры мониторинга и анализа должны использовать документально определенные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга и анализа должны применяться на регулярной основе, например, ежедневно, ко всем выполненным операциям и транзакциям.

7.4.5. Порядок доступа работников организации БС РФ в помещения, в которых размещаются объекты среды информационных активов, должен быть регламентирован во внутренних документах организации БС РФ, а его выполнение должно контролироваться.

Результаты контроля выполнения порядка доступа должны оформляться документально.

7.4.6. 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.

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

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

7.4.8. При заключении договоров со сторонними организациями рекомендуется юридическое оформление договоренностей, предусматривающих 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 и анализа протоколов операций позволяют предположить, что выполнение данной транзакции является частью замысла злоумышленников.

7.4.9. Должны быть документально оформлены 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 документирование работниками и клиентами всех своих действий и их результатов.

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

7.4.11. В организации БС РФ должны применяться защитные меры, направленные на обеспечение защиты от НСД и НРД, повреждения или нарушения целостности информации, необходимой для регистрации, идентификации, аутентификации и (или) авторизации клиентов и работников организации БС РФ. Все попытки НСД и НРД к такой информации должны регистрироваться. При увольнении или изменении должностных обязанностей работников организации БС РФ, имевших доступ к указанной информации, необходимо выполнить документированные процедуры соответствующего пересмотра прав доступа.

7.4.12. Работа всех пользователей АБС должна осуществляться под уникальными 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, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты.

Процедуры установки и регулярного обновления средств антивирусной защиты (версий и баз данных) на автоматизированных рабочих местах и серверах АБС должны быть документированы и осуществляться администраторами АБС или иными официально уполномоченными лицами.

Рекомендуется организовать автоматический режим установки обновлений антивирусного программного обеспечения и его баз данных.

Установка и обновление антивирусных средств в организации должны контролироваться представителями подразделения (лицами) в организации, ответственными за обеспечение ИБ.

7.5.2. В организации БС РФ рекомендуется организовать функционирование постоянной антивирусной защиты в автоматическом режиме.

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

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

7.5.5. Рекомендуется организовать построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях, почтовых серверах и межсетевых экранах.

7.5.6. Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться.

7.5.7. Должны быть документально определены 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).

7.5.8. Должны быть документально определены и выполняться процедуры контроля за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах АБС. Результаты контроля должны документироваться.

7.5.9. 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 документально приниматься руководством организации БС РФ. При этом цели использования сети Интернет должны быть явно перечислены, 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, 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 оформляться документально и выполняться в соответствии с его должностными обязанностями, в частности, в соответствии с назначенными ему ролями.

7.6.2. В организации БС РФ должен быть документально определен порядок подключения и использования ресурсов сети Интернет, включающий в том числе положение о контроле со стороны подразделения (лиц) в организации, ответственного за обеспечение ИБ.

7.6.3. В организациях БС РФ, осуществляющих дистанционное банковское обслуживание клиентов, в связи с повышенными рисками нарушения ИБ при взаимодействии с сетью Интернет должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

7.6.4. Рекомендуется выполнить выделение и организовать физическую изоляцию от внутренних сетей тех ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line.

7.6.5. 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 образом.

7.6.6. Все операции клиентов в течение всего сеанса работы с системами дистанционного банковского обслуживания должны выполняться только после выполнения процедур идентификации, аутентификации и авторизации. В случаях нарушения или разрыва соединения необходимо обеспечить повторное выполнение указанных процедур.

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

7.6.7. Почтовый обмен через сеть Интернет должен осуществляться с использованием защитных мер. Перечень указанных защитных мер и порядок их использования должны быть определены документально.

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).

7.6.8. Электронная почта должна архивироваться. Архив должен быть доступен подразделению (лицу) в организации, ответственному за обеспечение ИБ. Изменения в архиве не допускаются. Порядок доступа к информации архива должен быть документально определен.

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

7.6.10. При взаимодействии с сетью Интернет должны быть документально определены и использоваться защитные меры противодействия атакам хакеров 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.

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.

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

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

7.7.2. 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;
- поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

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

---

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

7.7.4. При применении СКЗИ должны поддерживаться непрерывность процессов протоколирования работы 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.

7.7.5. ИБ процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

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

7.7.7. 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.

7.7.8. 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 документирован в организации БС РФ.

7.8.3. Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских платежных технологических процессов. Состав установленного и используемого в ЭВМ и АБС программного обеспечения должен соответствовать определенному перечню. Выполнение данных требований должно контролироваться с документированием результатов.

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

7.8.5. 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.

7.8.6. 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.

7.8.7. Обязанности по администрированию средств защиты платежной информации рекомендуется возлагать приказом или распоряжением по организации БС РФ на администраторов ИБ с отражением этих обязанностей в их должностных инструкциях.

7.8.8. Комплекс мер по обеспечению ИБ 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 (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);
— 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;
— 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”).

7.8.9. При проектировании, разработке и эксплуатации систем дистанционного банковского обслуживания должны быть документально определены и выполняться процедуры, реализующие в том числе механизмы:
— снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;
— доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

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

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

7.8.11. Должна осуществляться и быть регламентирована процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации БС РФ за обеспечение ИБ.

7.8.12. Должна осуществляться и быть регламентирована процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ платежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации БС РФ за обеспечение ИБ.

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 рекомендуется провести классификацию неплатежной информации.

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

7.9.3. Для каждого из типов неплатежных информационных активов (типов неплатежной информации), полученных в результате классификации, должен быть документально определен набор требований по их защите.

7.9.4. Обязанности по администрированию средств защиты неплатежной информации рекомендуется возлагать приказом или распоряжением по организации БС РФ на администраторов ИБ с отражением этих обязанностей в их должностных инструкциях.

7.9.5. Для каждой АБС должен быть документально определен порядок контроля ее функционирования со стороны лиц, отвечающих за ИБ.

7.9.6. Банковские информационные технологические процессы должны быть документированы в организации БС РФ. Указанные документы должны быть согласованы со службой ИБ. 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 либо лицом, отвечающим в организации за ИБ.

7.9.7. Должны быть документально определены перечни программного обеспечения, устанавливаемого и (или) используемого в ЭВМ и АБС и необходимого для выполнения конкретных банковских информационных технологических процессов. Состав установленного и используемого в ЭВМ и АБС программного обеспечения должен соответствовать определенному перечню. Выполнение данных требований должно контролироваться с документированием результатов.

7.9.8. Должна быть регламентирована и осуществляться процедура периодического контроля всех реализованных программно-техническими средствами и организационными мерами функций (требований) по обеспечению ИБ неплатежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации за ИБ.

7.9.9. Должна быть регламентирована и осуществляться процедура восстановления всех реализованных программно-техническими средствами и организационными мерами функций по обеспечению ИБ неплатежной информации. Регламентирующие документы должны быть согласованы со службой либо лицом, отвечающим в организации за ИБ.

7.10. Общие требования по обработке персональных данных в организации БС РФ

7.10.1. В организации БС РФ должны быть определены, документально зафиксированы и утверждены руководством организации БС РФ цели обработки персональных данных.

7.10.2. В организации БС РФ должна быть определена необходимость уведомления Уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных.

7.10.3. Для каждой цели обработки персональных данных должны быть определены, документально зафиксированы и утверждены руководством организации БС РФ:

- объем и содержание персональных данных;
- сроки обработки, в том числе сроки хранения персональных данных;
- необходимость получения согласия субъектов персональных данных.

7.10.4. В организации БС РФ рекомендуется проводить классификацию персональных данных в соответствии со степенью тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных.

Рекомендуется выделять следующие категории персональных данных:

- персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” [5] к специальным категориям персональных данных;
- персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” [5] к биометрическим персональным данным;
- персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным;
- персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” [5] к общедоступным или обезличенным персональным данным.

7.10.5. Передача персональных данных организацией БС РФ третьему лицу должна осуществляться с согласия субъекта персональных данных. В том случае, если организация БС РФ поручает обработку персональных данных третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

7.10.6. Организация БС РФ должна прекратить обработку персональных данных и уничтожить собранные персональные данные, если иное не установлено законодательством РФ, в следующих случаях и в сроки, установленные законодательством РФ:

- по достижении целей обработки или при утрате необходимости в их достижении;
- по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных — если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ;
- при невозможности устранения оператором допущенных нарушений при обработке персональных данных.

В организации БС РФ должен быть определен и документально зафиксирован порядок уничтожения персональных данных (в том числе и материальных носителей персональных данных).

7.10.7. В организации БС РФ должен быть определен и документально зафиксирован порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных.

7.10.8. В организации БС РФ должен быть определен и документально зафиксирован порядок действий в случае запросов Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных.

7.10.9. В организации БС РФ должен быть определен и документально зафиксирован подход к отнесению АБС к информационным системам персональных данных (ИСПДн).

В организации БС РФ должен быть определен и документально зафиксирован перечень ИСПДн. В перечень ИСПДн должны быть включены как минимум АБС, целью создания и использования которых является обработка персональных данных.

АБС, реализующие банковские платежные технологические процессы, не относятся к ИСПДн.

7.10.10. Для каждой ИСПДн организации БС РФ должны быть определены и документально зафиксированы:

— цель обработки персональных данных;
— объем и содержание обрабатываемых персональных данных;
— перечень действий с персональными данными и способы их обработки.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать целям обработки. В том случае, если для выполнения банковского информационного технологического процесса, реализацию которого поддерживает ИСПДн, нет необходимости в обработке определенных персональных данных, эти персональные данные должны быть удалены.

7.10.11. Банковские информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, должны быть документированы в организации БС РФ.

При этом рекомендуется исключать фиксацию на одном материальном носителе и персональных данных, и иных видов информационных активов, а также персональных данных, цели обработки которых заведомо несовместимы.

При обработке различных категорий персональных данных для каждой категории персональных данных рекомендуется использовать отдельный материальный носитель.

7.10.12. В организации БС РФ должен быть определен и документально зафиксирован перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн либо имеющих доступ к персональным данным.

Допускается указание работников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью на основании требований раздела 7.2 настоящего стандарта.

Возможно существование перечня (списка) в электронном виде при условии предоставления работникам прав доступа в ИСПДн только на основании распорядительного документа в документально зафиксированном в организации БС РФ порядке.

Доступ работников организации БС РФ к персональным данным и обработка персональных данных работниками организации БС РФ должны осуществляться только для выполнения их должностных обязанностей.

7.10.13. Работники организации БС РФ, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

7.10.14. В организации БС РФ должен быть определен и документально зафиксирован порядок доступа работников организации БС РФ и иных лиц в помещения, в которых ведется обработка персональных данных.

7.10.15. В организации БС РФ должен быть определен и документально зафиксирован порядок хранения материальных носителей персональных данных, устанавливающий:

— места хранения материальных носителей персональных данных;
— требования по обеспечению безопасности персональных данных при хранении их носителей;
— работников, ответственных за реализацию требований по обеспечению безопасности персональных данных;
— порядок контроля выполнения требований по обеспечению безопасности персональных данных при хранении материальных носителей персональных данных.

7.10.16. При обработке в организации БС РФ персональных данных на бумажных носителях, в частности, при использовании в организации БС РФ типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных,

должны соблюдаться требования, установленные “Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации”, утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. № 687 [6].

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 вне ИСПДн, должна соответствовать требованиям пункта 7.9 настоящего стандарта.

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

7.11.2. Все ИСПДн организаций БС РФ относятся к специальным в соответствии с пунктом 8 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 “Об утверждении Порядка проведения классификации информационных систем персональных данных” [7].

7.11.3. В организации БС РФ должны быть определены и документально зафиксированы критерии классификации ИСПДн и порядок проведения классификации ИСПДн.

Классификация ИСПДн должна проводиться в том числе на основе категорий обрабатываемых в ИСПДн персональных данных.

Результаты классификации ИСПДн должны быть документально определены и утверждены руководством организации БС РФ.

7.11.4. Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн определяются для каждого класса ИСПДн на основе:

— требований 7-го и 8-го разделов настоящего стандарта с учетом положений рекомендаций в области стандартизации Банка России РС БР ИББС-2.3 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации”, детализирующих указанные требования;

Требования 7-го и 8-го разделов настоящего стандарта направлены на нейтрализацию актуальных[1] (применительно к большинству организаций БС РФ) угроз безопасности персональных данных при обработке в ИСПДн организаций БС РФ и образуют базовый набор требований, применимый к большинству организаций БС РФ. С учетом специфики обработки и обеспечения безопасности персональных данных в организациях БС РФ угрозы утечки персональных данных по техническим каналам являются для организаций БС РФ неактуальными.

— оценки рисков нарушения безопасности персональных данных.

Результатом оценки рисков нарушения безопасности персональных данных является Модель угроз безопасности персональных данных, содержащая актуальные для организации БС РФ угрозы ИБ, на основе которой вырабатываются требования, учитывающие особенности обработки персональных данных в конкретной организации БС РФ, и расширяющие требования 7-го и 8-го разделов настоящего стандарта и (или) положения рекомендаций в области стандартизации Банка России РС БР ИББС-2.3 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации”.

---

[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 и контроль используемых защитных мер, периодически выполнять деятельность по самооценке соответствия ИБ организации БС РФ требованиям настоящего стандарта (далее — самооценка ИБ) 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 последующие обновления 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 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 (назначить уполномоченное лицо), 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 (уполномоченное лицо) 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;
- 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. Должна быть документально определена/скорректирована опись структурированных по классам защищаемых информационных активов (типов информационных активов — типов информации). 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 случае наличия в организации БС РФ классификации информационных активов опись информационных активов должна содержать информацию о принадлежности конкретного информационного актива к выделенным типам информационных активов.

8.3.3. Опись информационных активов (типов информационных активов) должна содержать перечень их объектов среды. Перечень объектов среды должен покрывать все уровни информационной инфраструктуры организации БС РФ, определенной в разделе 6 настоящего стандарта.

8.3.4. Должны быть документально определены процедуры анализа и пересмотра области действия СОИБ, в частности, процедуры пересмотра при изменении перечня информационных активов организации (типов информационных активов).

8.3.5. В организации БС РФ должны быть документально определены роли по определению/коррекции области действия СОИБ, по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ. В организации БС РФ должны быть 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. В организации БС РФ рекомендуется создать и поддерживать в актуальном состоянии единый информационный ресурс (базу данных), содержащий информацию об инцидентах ИБ.

8.4.6. 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 документально оформленный перечень недопустимых рисков нарушения ИБ.

8.4.7. В организации БС РФ должны быть документально 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.

8.4.8. В организации БС РФ должны быть документально 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 документально определен план, определяющий 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 формирования 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 защитных мер.

8.5.4. В организации БС РФ должны быть документально 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, должны быть определены 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 Российской Федерации;
— комплекса БР ИББС, в частности, требований 7 и 8 разделов 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 (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 (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 документально определены процедуры выделения и распределения ролей в области обеспечения ИБ.

8.6.10. Должен быть документально 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 документально 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 документально оформить решения руководства:

— об анализе и принятии остаточных рисков нарушения ИБ;
— о планировании этапов внедрения СОИБ, в частности, требований по обеспечению ИБ, изложенных в 7-м и 8-м разделах 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 7-го и 8-го разделов 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 7-го и 8-го разделов настоящего стандарта, планы обработки рисков нарушения ИБ и внедрения защитных мер должны быть утверждены руководством. Указанные планы должны документально фиксировать:

— 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 документально определен порядок разработки, пересмотра и контроля исполнения планов по обеспечению ИБ организации БС РФ.

8.7.4. В организации БС РФ должны быть документально оформлены 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 документально определены и выполняться проектирование/приобретение/развертывание, внедрение, эксплуатация, контроль и сопровождение 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 документально 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 документально оформленная и утвержденная руководством работа с персоналом организации БС РФ в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов.

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

8.9.3. Программы обучения и повышения осведомленности должны 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.

8.9.4. В организации БС РФ должен быть определен перечень документов, являющихся свидетельством выполнения программ обучения и повышения осведомленности в области ИБ. В частности, такими документами 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.

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

8.9.6. В организации БС РФ должны быть документально 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. В организации БС РФ должны быть документы, регламентирующие процедуры обработки инцидентов, включающие:

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

8.10.2. В организации БС РФ рекомендуется сформировать и поддерживать в актуальном состоянии централизованную базу данных инцидентов ИБ. Должны быть документально определены процедуры по хранению информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

8.10.3. Должны быть документально определены порядки действий 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 действующее законодательство Российской Федерации, положения нормативных актов Банка России, а также внутренних документов организации БС РФ в области ИБ.

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

8.10.6. В организации БС РФ должны быть документально 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. В описи защищаемых информационных активов должны быть выделены информационные активы, существенные для обеспечения непрерывности бизнеса организации БС РФ.

8.11.2. В организации БС РФ должны быть документально определены требования по обеспечению ИБ, регламентирующие вопросы обеспечения непрерывности бизнеса и его восстановления после прерывания.

8.11.3. Должен быть документально 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 активизации 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 документально оформленных 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 быть документально определены, реализованы и использоваться защитные меры обеспечения непрерывности бизнеса применительно к информационным активам, существенным для обеспечения непрерывности бизнеса и его восстановления после прерывания.

Реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания должны 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. Должно быть документально определено и выполняться периодическое тестирование 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. Должны быть документально определены и выполняться процедуры регулярного пересмотра и обновления плана обеспечения непрерывности бизнеса и его восстановления после прерывания для обеспечения уверенности в их эффективности. Процедуры пересмотра и обновления плана должны учитывать изменения в приоритетах, целях и интересах бизнеса организации БС РФ; пересмотр моделей угроз; оценку рисков нарушения ИБ.

8.11.10. В организации БС РФ должны быть документально 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 и контролю защитных мер

8.12.1. Должны быть документально определены процедуры мониторинга СОИБ и контроля защитных мер, включая контроль параметров конфигурации и настроек средств и механизмов защиты. Указанные процедуры должны проводиться персоналом организации БС РФ, ответственным за обеспечение ИБ, и охватывать все реализованные и эксплуатируемые защитные меры, входящие в СИБ.

8.12.2. Результаты выполнения процедур мониторинга СОИБ и контроля защитных мер должны документально фиксироваться.

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

8.12.4. Информация обо всех инцидентах, выявленных в процессе мониторинга СОИБ и контроля защитных мер, должна включаться в базу данных инцидентов ИБ.

8.12.5. Процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе

и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра должен быть документально определен.

8.12.6. В организации БС РФ должны быть документально определены роли, связанные с выполнением процедур мониторинга СОИБ 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 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".

8.13.2. Должна быть документально определена 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.

8.13.3. В организации БС РФ должны быть документально определены:

— порядок формирования, сбора и хранения свидетельств самооценки ИБ;
— периодичность проведения самооценки ИБ;
— порядок хранения и использования результатов самооценки ИБ.

8.13.4. Для каждой проводимой в организации БС РФ самооценки ИБ необходимо документально оформить 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.

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

8.13.6. В организации БС РФ должны быть документально 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 документально определена и реализовываться 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 документально оформить 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 документально определены:

- порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;
- порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ;
- порядок взаимодействия аудиторской группы и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству;
- порядок организации опроса работников;
- порядок организации наблюдения за деятельностью работников организации 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. Должен быть документально определен порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности, отчетов аудитов.

8.14.7. В организации БС РФ должны быть документально 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. В организации БС РФ должен проводиться анализ функционирования СОИБ, использующий в том числе:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов ИБ, самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри организации 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 Российской Федерации, 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 Российской Федерации, 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 адекватности модели угроз организации БС РФ существующим угрозам ИБ;
- оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска;
- проверку адекватности используемых защитных мер требованиям внутренних документов организации БС РФ и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

8.15.3. Результаты анализа функционирования СОИБ должны документироваться.

8.15.4. В организации БС РФ должны быть документально 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 утвержден 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 СОИБ 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 Российской Федерации 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 определен и утвержден руководством 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 производятся поиск и анализ проблем ИБ, влияющих на бизнес организации БС РФ.

8.16.3. В организации БС РФ должны быть документально 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[1] улучшениям системы обеспечения информационной безопасности

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

8.17.2. Решения по тактическим улучшениям СОИБ должны быть документально 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 СОИБ и контроля защитных мер;
— пересмотр программ аудитов;

---

[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.

— 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. Вся деятельность по реализации тактических улучшений должна документально регистрироваться. Должны быть определены документы, содержащие планы реализации тактических улучшений СОИБ, и документы, в которых фиксируются результаты выполнения указанных планов.

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 документально определены и выполняться 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, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

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

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

8.18.1. Для принятия решений, связанных со стратегическими улучшениями СОИБ, необходимо рассмотреть среди прочего документально оформленные результаты:
— аудитов ИБ;
— самооценок ИБ;
— мониторинга СОИБ 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 Российской Федерации;
— 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 документально 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;
— уточнение описи типов информационных активов;
— 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 документально регистрироваться. Должны быть определены документы, содержащие 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 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 защитных мер и соответствующих внутренних документов. В частности, необходимо выполнить:

---

[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.

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

8.18.6. Должны быть документально определены и выполняться 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, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

8.18.7. В случаях принятия решений по стратегическим улучшениям СОИБ должны быть 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 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 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. Самооценка ИБ проводится собственными силами и по инициативе руководства организации.

Порядок проведения самооценки ИБ в организации БС РФ определен в рекомендациях 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 стандарта СТО БР ИББС-1.0”.

В процессе самооценки ИБ проводятся оценка степени выполнения требований настоящего стандарта и на ее основе — вычисление итогового уровня ИБ организации БС РФ. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется 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”.

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.

Аудит ИБ проводится в соответствии с требованиями подраздела 8.14 настоящего стандарта, а также в соответствии с требованиями стандартов Банка России СТО БР ИББС-1.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности”.

В процессе аудита ИБ проводятся оценка степени выполнения требований настоящего стандарта и на ее основе — вычисление итогового уровня ИБ организации БС РФ. Поря-

док проведения указанной деятельности (оценка и вычисление) регламентируется 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”.

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

Порядок проведения работ по контролю и надзору, включающий, в частности, вопросы:

проведения ведомственного контроля (с участием Банка России, предприятий лицензиатов, самооценки);

государственного контроля, предусмотренного Федеральным законом “О персональных данных” [5], со стороны ФСБ России и ФСТЭК России;

взаимодействия сторон при проведении указанных видов контроля;

согласования планов, информационного взаимодействия, форм предоставления отчетности и т.д.;

а также регламентация обеспечения безопасности персональных данных при использовании средств криптографической защиты информации будут изложены в отдельных документах.

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 Российской Федерации 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.

Требования к проведению анализа функционирования СОИБ определены в подразделах 8.15 и 8.16 настоящего стандарта.

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 специальных 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 специальных ИСПДн организаций БС РФ.

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

Библиография

[1] Федеральный закон “О банках и банковской деятельности” от 01.12.1990 № 395-1 в редакции Федерального закона от 03.02.1996 № 17-ФЗ, от 31.07.1998 № 151-ФЗ, от 05.07.1999 № 126-ФЗ, от 08.07.1999 № 136-ФЗ, от 19.06.2001 № 82-ФЗ, от 07.08.2001 № 121-ФЗ, от 21.03.2002 № 31-ФЗ с изменениями, внесенными постановлением Конституционного суда РФ от 23.02.1999 № 4-П.

[2] Федеральный закон “О Центральном банке Российской Федерации (Банке России)” от 10 июля 2002 г. № 86-ФЗ.

[3] Федеральный закон “Об информации, информационных технологиях и о защите информации” от 27 июля 2006 г. № 149-ФЗ.

[4] ISO/IEC IS 27001-2005 Information technology. Security techniques. Information security management systems. Requirements.

[5] Федеральный закон “О персональных данных” от 27 июля 2006 г. № 152-ФЗ.

[6] Постановление Правительства РФ от 15 сентября 2008 г. № 687 “Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации”.

[7] Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 “Об утверждении Порядка проведения классификации информационных систем персональных данных”.

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

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.2-2010

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Дата введения: 2010-06-21

Издание официальное

Предисловие

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

2. ВЗАМЕН СТО БР ИББС-1.2-2009.

Содержание

Введение

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

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

СТО БР ИББС-1.2-2010

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Дата введения: 2010-06-21

1. Область применения

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

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

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

2. Нормативные ссылки

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

3. Термины и определения

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

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

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

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

4. Обозначения и сокращения

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

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

5. Общие положения

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

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

6. Показатели информационной безопасности. Способы оценивания показателей

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

При формировании коэффициентов значимости учитывалось следующее условие нормировки:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$EV_{ООПД} = EV_{M9}.$$

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

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

8. Оценка менеджмента информационной безопасности организации банковской системы Российской Федерации

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

При проведении оценивания частных показателей следует использовать следующий общий подход:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Нулевому уровню соответствует круг до окружности радиусом 0,25.

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

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

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

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

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

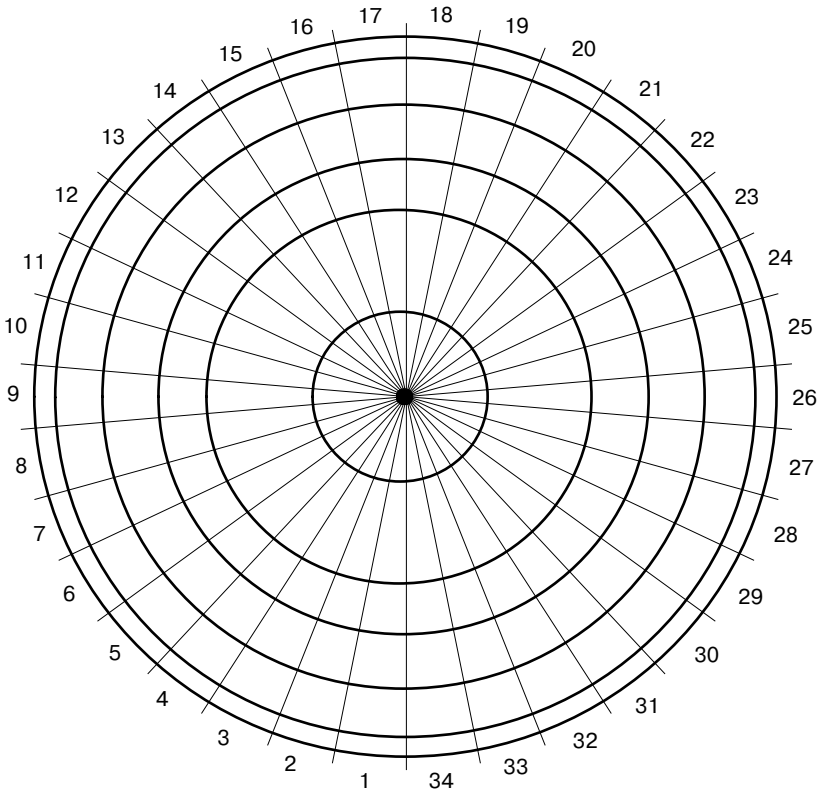
$EV^{I}_{ОЗПД}$ — оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической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

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

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

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

Рисунок 1 — Круговая диаграмма для отображения результатов оценивания



Приложение А
(обязательное)

Показатели информационной безопасности

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

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

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

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

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

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

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

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

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

Групповой показатель М4 “Обеспечение информационной безопасности средствами антивирусной защиты”

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[1] Графа не заполняется.

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

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

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

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

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

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

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

Групповой показатель М12 “Определение/коррекция области действия СОИБ”

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

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

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

Групповой показатель М14 “Разработка планов обработки рисков нарушения ИБ”

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

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

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

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

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

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

Групповой показатель М17 “Организация реализации планов внедрения СОИБ”

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

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

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

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

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

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

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

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

Групповой показатель М21 "Мониторинг и контроль защитных мер"

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

Групповой показатель М22 “Проведение самооценки ИБ”

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	Оценка частного показателя ИБ						Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
			0	0,25	0,5	0,75	1	н/о		
М22.1	Проводится ли самооценка ИБ в соответствии с настоящим стандартом?	обязательный							0,1340	
М22.2	Организован ли порядок проведения самооценки ИБ в соответствии с рекомендациями по стандартизации Банка России РС БР ИББС-2.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”?	рекомендуемый							0,1118	
М22.3	Определена ли в документах организации и реализована ли программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки?	обязательный							0,1026	
М22.4	Определены ли в документах организации: — порядок формирования, сбора и хранения свидетельств самооценки ИБ; — периодичность проведения самооценки ИБ; — порядок хранения и использования результатов самооценки ИБ?	обязательный							0,1098	
М22.5	Оформлен ли в документах организации для каждой проводимой в организации самооценки ИБ план ее проведения, определяющий: — цель самооценки ИБ; — объекты и деятельность, подвергающиеся самооценке ИБ; — порядок и сроки выполнения мероприятий самооценки ИБ; — распределение ролей среди работников организации, связанных с проведением самооценки ИБ?	обязательный							0,0978	
М22.6	Подготавливаются ли по результатам самооценок ИБ отчеты?	обязательный							0,1150	
М22.7	Доводятся ли результаты самооценок ИБ и соответствующие отчеты до руководства организации?	обязательный							0,1262	
М22.8	Определены ли в документах организации роли, связанные с выполнением программы самооценок ИБ?	обязательный							0,1014	
М22.9	Назначены ли ответственные за выполнение ролей, связанных с выполнением программы самооценок ИБ?	обязательный							0,1014	
Итоговая оценка группового показателя М22										

Групповой показатель М23 "Проведение аудита ИБ"

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

Групповой показатель М24 “Анализ функционирования СОИБ”

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

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

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

Групповой показатель М26 “Принятие решений по тактическим улучшениям СОИБ”

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

Групповой показатель М27 “Принятие решений по стратегическим улучшениям СОИБ”

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Приложение Б
(обязательное)

Форма листов для сбора свидетельств аудита ИБ

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

_____
(подпись)

_____
(подпись)

_____
(подпись)

Приложение В
(обязательное)

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

Таблица 1. Уточняющие вопросы частных показателей ИБ

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

[1] Классы ИСПДн:

ИСПДн-С – ИСПДн обработки специальных категорий персональных данных;

ИСПДн-Б – ИСПДн обработки биометрических персональных данных;

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

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

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

СТО БР ИББС-1.2-2010

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

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

СТО БР ИББС-1.2-2010

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

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

СТО БР ИББС-1.2-2010

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

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

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

СТО БР ИББС-1.2-2010

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

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

РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.3-2010

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата введения: 2010-06-21

Издание официальное

Предисловие

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

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) важнейшим условием реализации целей деятельности Банка России является обеспечение необходимого и достаточного уровня информационной безопасности организаций банковской системы Российской Федерации (БС РФ), их активов, к которым в том числе относятся персональные данные и банковские технологические процессы, в рамках которых они обрабатываются.

Стандартом СТО БР ИББС-1.0 с целью выполнения в организациях БС РФ требований законодательства Российской Федерации в области персональных данных определены требования по обработке персональных данных и по обеспечению информационной безопасности (ИБ) банковских технологических процессов, в рамках которых обрабатываются персональные данные (далее — требования СТО БР ИББС-1.0 в области персональных данных).

Настоящий документ содержит детализирующие требования по обеспечению безопасности персональных данных, выполнение которых способствует реализации в организациях БС РФ требований СТО БР ИББС-1.0 в области персональных данных и обеспечивает нейтрализацию актуальных для организаций БС РФ угроз безопасности персональных данных, содержащихся в рекомендациях в области стандартизации Банка России РС БР ИББС-2.x-20xx “Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ”.

РС БР ИББС-2.3-2010

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

Дата введения: 2010-06-21

1. Область применения

Настоящие рекомендации распространяются на организации БС РФ, реализующие требования стандарта СТО БР ИББС-1.0 в области персональных данных, в рамках построения/совершенствования системы обеспечения информационной безопасности организации БС РФ.

Настоящий документ применяется в организации БС РФ путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних нормативных и методических документах организаций БС РФ.

Рекомендательный статус документа допускает, что его отдельные требования по решению организации БС РФ могут быть заменены иными требованиями, обеспечивающими эквивалентный (аналогичный) уровень безопасности персональных данных.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на следующие документы в области стандартизации Банка России:

СТО БР ИББС-1.0;

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” (далее — СТО БР ИББС-1.2).

3. Термины и определения

В настоящих рекомендациях применены термины в соответствии со СТО БР ИББС-1.0.

4. Обозначения и сокращения

АРМ — автоматизированное рабочее место;
БС — банковская система;
ИБ — информационная безопасность;
ИСПДн — информационная система персональных данных;
ЛВС — локальная вычислительная сеть;
ОС — операционная система;
ПО — программное обеспечение;

РФ — Российская Федерация;
СКЗИ — средства криптографической защиты информации;
СУБД — система управления базы данных.

5. Общий подход к определению требований по обеспечению безопасности персональных данных в информационных системах персональных данных

5.1. Выбор требований по обеспечению безопасности персональных данных в информационных системах персональных данных (ИСПДн) осуществляется в зависимости от результатов классификации ИСПДн.

5.2. В соответствии с действующим стандартом СТО БР ИББС-1.0 все ИСПДн организаций БС РФ относятся к специальным. ИСПДн организации БС РФ классифицируются на основе категорий обрабатываемых в ИСПДн персональных данных. Выделяются следующие основные классы ИСПДн:

ИСПДн обработки специальных категорий персональных данных (далее — ИСПДн-С);

Примечание.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] к специальным категориям персональных данных относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

ИСПДн обработки биометрических персональных данных (далее — ИСПДн-Б);

Примечание.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] к биометрическим персональным данным относятся сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.

ИСПДн обработки персональных данных, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным (далее — ИСПДн-И);

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

Примечание.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] к общедоступным персональным данным относятся персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

5.3. Для обеспечения выполнения требований СТО БР ИББС-1.0 в ИСПДн организации БС РФ для каждой ИСПДн должны быть реализованы:

— общие требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн любого класса (раздел 6.1 настоящих рекомендаций);
— требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн соответствующего класса (разделы 6.2—6.5 настоящих рекомендаций).

5.4. Связь положений СТО БР ИББС-1.0 и требований настоящего документа, необходимых для реализации этих положений, приведена в Приложении.

5.5. При проведении оценок соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 (самооценок и внешних оценок соответствия) вопросы частных показателей СТО БР ИББС-1.2 в части банковских технологических процессов, в рамках которых обрабатываются персональные данные, детализируются и конкретизируются вопросами, составленными на основе требований настоящего документа. Перечень указанных детализирующих и конкретизирующих вопросов, а также подход к проведению оценок соответствия ИБ содержатся в СТО БР ИББС-1.2.

6. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных

6.1. Общие требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных любого класса

6.1.1. Требования по обеспечению безопасности персональных данных в ИСПДн в общем случае реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

Организация выполнения и (или) реализация требований по обеспечению безопасности персональных данных должна осуществляться структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, либо на договорной основе организацией — контрагентом организации БС РФ, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Допускается возложение ответственности за организацию работы по обеспечению безопасности персональных данных на существующее в организации БС РФ подразделение (например, на службу ИБ).

Реализация требований по обеспечению безопасности персональных данных должна осуществляться по согласованию и под контролем службы ИБ организации БС РФ.

6.1.2. Создание ИСПДн организации БС РФ должно включать разработку и согласование (утверждение) предусмотренной техническим заданием организационно-распорядительной, проектной и эксплуатационной документации на создаваемую систему. В документации должны быть отражены вопросы обеспечения безопасности обрабатываемых персональных данных.

Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн должны осуществляться по согласованию и под контролем структурного подразделения или должностного лица (работника) организации БС РФ, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации БС РФ.

6.1.3. Все информационные активы, принадлежащие ИСПДн организаций БС РФ, должны быть защищены от воздействий вредоносного кода. В организации БС РФ должны быть определены и документально зафиксированы требования по обеспечению безопасности персональных данных средствами антивирусной защиты и порядок проведения контроля реализации этих требований в соответствии с требованиями пункта 7.5 СТО БР ИББС-1.0.

6.1.4. В организации БС РФ должна быть определена система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн.

6.1.5. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений организации БС РФ обеспечивают безопасность персональных данных при их обработке в ИСПДн.

Работники, осуществляющие обработку персональных данных в ИСПДн, должны действовать в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдать требования документов организации БС РФ по обеспечению ИБ.

6.1.6. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению ИБ ИСПДн организации БС РФ, возлагаются приказами (распоряжениями) на администраторов информационной безопасности ИСПДн.

6.1.7. Порядок действий администратора информационной безопасности ИСПДн и персонала, занятых в процессе обработки персональных данных, должен быть определен инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн.

Указанные инструкции (руководства):

устанавливают требования к квалификации администратора информационной безопасности и персонала в области защиты информации, а также актуальный перечень защищаемых объектов и правила его обновления;

содержат в полном объеме актуальные (по времени) данные о полномочиях пользователей;

содержат данные о технологии обработки информации в объеме, необходимом для администратора информационной безопасности;

устанавливают порядок и периодичность анализа журналов регистрации событий (архивов журналов);

регламентируют другие действия администратора информационной безопасности и персонала, предусмотренные настоящими рекомендациями.

Параметры конфигурации средств защиты и механизмов защиты информации от НСД, используемых в зоне ответственности администратора информационной безопасности, определяются в эксплуатационной документации на ИСПДн. Порядок и периодичность проверок установленных параметров конфигурации устанавливаются в эксплуатационной документации или регламентируются внутренним документом организации БС РФ, при этом проверки должны проводиться не реже чем раз в год.

6.1.8. В организации БС РФ должен быть определен и документально зафиксирован порядок доступа в помещения, в которых размещаются технические средства ИСПДн и хранятся носители персональных данных, предусматривающий контроль доступа в помещения посторонних лиц и наличие препятствий для несанкционированного проникновения в помещения.

Указанный порядок должен быть разработан структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение режима физической безопасности организации БС РФ и согласован структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и службой ИБ организации БС РФ.

6.1.9. Пользователи и обслуживающий персонал ИСПДн не должны осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных. С этой целью организационно-техническими мерами должно быть запрещено несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки.

6.2. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки общедоступных и (или) обезличенных персональных данных

6.2.1. Процессы обработки персональных данных, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются разработчиком ИСПДн в проектной и эксплуатационной документации.

6.2.2 Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечиваются по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов.

При наличии технической возможности количество последовательных неудачных попыток ввода пароля должно быть ограничено — от 3 до 5 попыток. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности.

Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком ИСПДн в эксплуатационной документации в инструкциях (руководствах) администраторов информационной безопасности.

6.2.3. Передача персональных данных должна осуществляться только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию со структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных.

6.3. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным

6.3.1. Для информационных систем обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным, применяются все требования по обеспечению безопасности, определенные в разделе 6.2, а также следующие требования.

6.3.2. Выполнение функций обеспечения безопасности персональных данных в ИСПДн должно обеспечиваться средствами защиты информации, прошедшими в установленном по-

рядке процедуру оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО).

6.3.3. На стадии ввода в действие разработчиком ИСПДн должны быть выполнены настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий. Разработчиком ИСПДн должен быть определен порядок постоянного контроля фактического состояния указанных настроек на предмет их соответствия установленным правилам.

Указанный порядок должен быть согласован структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и согласован службой ИБ организации БС РФ.

6.3.4. Регистрация входа в ИСПДн (выхода из ИСПДн) субъекта доступа является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время входа в систему (выхода из системы) субъекта доступа;
— идентификатор субъекта, предъявленный при запросе доступа;
— результат попытки входа: успешная или неуспешная (несанкционированная);
— идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

6.3.5. В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журнале регистрации событий, указанном в пункте 6.3.4.

Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив.

Операция по архивированию журнала регистрации событий должна, в свою очередь, регистрироваться с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

6.3.6. В организации БС РФ должен быть определен и документально зафиксирован порядок постановки на учет и снятия с учета машинных носителей, предназначенных для размещения персональных данных.

Снятие с учета машинных носителей, на которых были размещены персональные данные, производится по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения.

Процедура стирания информации регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн в зависимости от применяемого средства гарантированного стирания.

При наличии технической возможности осуществляется очистка освобождаемых областей памяти на носителях, ранее использованных для хранения персональных данных.

6.3.7. Состав и назначение ПО ИСПДн должны быть определены и зафиксированы документально в соответствии с требованиями пункта 7.9.7 СТО БР ИББС-1.0.

6.3.8. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован. Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован. Соответствующие регламенты в виде инструкций, руководств готовятся разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

6.3.9. Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий, регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

6.3.10. Восстановление функций обеспечения безопасности персональных данных в ИСПДн в случае нештатной ситуации должно осуществляться администратором ИСПДн с обязательным привлечением администратора информационной безопасности ИСПДн (при необходимости — с привлечением специалистов структурного подразделения или должностного лица (работника) организации БС РФ, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации БС РФ). Процедура восстановления должна быть регламентирована разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

6.3.11. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые обеспечивают выполнение следующих функций:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

возможность проверки (контроля) целостности программной и информационной частей средства межсетевого экранирования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);

возможность проведения регламентного тестирования реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования).

6.4. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки биометрических персональных данных

6.4.1. Для информационных систем обработки биометрических персональных данных применяются все требования по обеспечению безопасности, определенные в разделе 6.3, а также требования, установленные Постановлением Правительства от 6 июля 2008 г. № 512 “Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных” [2].

6.5. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки специальных категорий персональных данных

6.5.1. Для информационных систем обработки специальных категорий персональных данных применяются все требования по обеспечению безопасности, определенные в разделе 6.3, а также следующие требования.

6.5.2. Идентификация информационных ресурсов (например, информационных массивов, баз данных, файлов, обрабатывающих их программ), содержащих персональные данные, должна осуществляться по логическим именам.

6.5.3. Контроль доступа субъектов к защищаемым информационным ресурсам в соответствии с правами доступа указанных субъектов является обязательным.

6.5.4. Регистрация печати материалов, содержащих персональные данные, является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время печати;
— спецификация устройства печати (логическое имя (номер) внешнего устройства);
— полное наименование (вид, шифр, код) материала;
— идентификатор субъекта доступа, запросившего печать материала;

— объем фактически отпечатанного материала (количество страниц, листов, копий) и результат печати: успешная (весь объем) или неуспешная.

6.5.5. Регистрация запуска программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам, является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время запуска;
— имя (идентификатор) программы (процесса, задания);
— идентификатор субъекта доступа, запросившего программу (процесс, задание);
— результат попытки запуска: успешная или неуспешная (несанкционированная);
— дата и время попытки доступа к защищаемому информационному ресурсу;
— имя (идентификатор) защищаемого информационного ресурса;
— вид запрашиваемой операции (например, чтение, запись, модификация, удаление);
— результат попытки доступа: успешная или неуспешная (несанкционированная).

6.5.6. Регистрация изменений полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов) является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время изменения;
— содержание изменения с указанием идентификатора субъекта доступа, чьи полномочия подверглись изменению, или логического имени защищаемого информационного ресурса, чей статус изменился;
— идентификатор администратора информационной безопасности, осуществившего изменение.

6.5.7. В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журналах регистрации событий, указанных в пунктах 6.5.4—6.5.6.

Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив.

Операция по архивированию журнала регистрации событий должна, в свою очередь, регистрироваться с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

6.5.8. С целью недопущения изменения состава ПО ИСПДн, комплекс средств автоматизации которой представляет собой автономное, изолированное на физическом уровне в соответствии с эталонной моделью взаимодействия открытых систем — моделью OSI, автоматизированное рабочее место (АРМ) работника или работников, из ПО должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения). Если стандартные программные средства общего назначения (например, MS Office) не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО, допускается использование этих программных средств при условии, что документально введен запрет использования отдельных их компонент (средств разработки и отладки ПО).

6.5.9. В ИСПДн, комплекс средств автоматизации которой включает одно или несколько сетевых АРМ, сетевого оборудования и серверов, технические и программные средства, предназначенные для разработки и отладки ПО либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения, должны располагаться в сегментах локальной вычислительной сети (ЛВС), изолированных (на уровне не выше сетевого в соответствии с эталонной моделью взаимодействия открытых систем — моделью OSI) от сегментов, задействованных в обработке персональных данных.

Параметры настроек технических и программных средств, обеспечивающих указанное разделение, а также процедура контроля этих параметров настроек регламентируются разработчиком в эксплуатационной документации на ИСПДн.

Стандартные программные средства общего назначения (например, MS Office), которые не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО, могут быть использованы в сегментах, задействованных в обработке персональных данных, при условии, что документально введен запрет использования отдельных их компонент (средств разработки и отладки ПО).

6.5.10. Передача персональных данных между подразделениями организации БС РФ по телекоммуникационным каналам и линиям связи, не принадлежащим организации БС РФ или не пролегающим только по территории организации БС РФ, должна осуществляться только при обеспечении их защиты с помощью организации виртуальных частных сетей (Virtual Private Network — VPN) или иных защитных мер, механизмов и средств, применение которых определяется структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и согласовывается со службой ИБ организации БС РФ.

6.5.11. Передача персональных данных по телекоммуникационным каналам и линиям связи между подразделениями организации БС РФ, с одной стороны, и внешними организациями, с другой стороны, должна осуществляться с использованием сертифицированных средств криптографической защиты или иных защитных механизмов, применение которых определяется структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и согласовывается со службой ИБ организации БС РФ.

В случае использования СКЗИ должны быть выполнены требования нормативных правовых актов ФСБ России.

В случае обмена информацией с другой организацией правила использования СКЗИ должны быть определены соглашением сторон, в частности, условиями договора.

При отсутствии указанной технической возможности передача персональных данных в электронном виде осуществляется на магнитных и других съемных носителях. Порядок такой передачи должен быть согласован со структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и со службой ИБ организации БС РФ.

6.5.12. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые должны иметь подтвержденный сертификатом класс защиты не ниже четвертого при возможности информационного обмена между всеми компонентами защищаемой ИСПДн без использования компонентов других автоматизированных банковских систем организации БС РФ (в иных случаях — не ниже третьего класса). Указанные классы защиты устанавливаются в соответствии с руководящим документом “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”, утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 года.

Приложение

Таблица соответствия положений СТО БР ИББС-1.0, частных показателей СТО БР ИББС-1.2, положений РС БР ИББС-2.3, положений Приказа ФСТЭК от 5.02.2010 № 58 [3], положений ISO/IEC 17799-2005 [4]

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.2.1	М1.1	6.1.5			6.1.1, 6.1.3, 8.1.1, 8.2.1, 8.2.3
		6.1.6			
		6.1.7			
		6.3.10			
7.2.2	М1.3	6.1.5			6.1.3, 8.2.3
		6.1.6			
		6.1.7			
		6.3.10			
	М1.4	6.1.5			
		6.1.6			
		6.1.7			
		6.3.10			
7.2.3	М1.9	6.3.5	2.1		6.1.3, 10.1.3
		6.5.7	2.1		
7.2.6	М1.13	6.1.7			8.1.2, 8.2
	М1.14	6.1.7			
7.2.8	М1.19	6.1.5			8.1.3, 8.2.3
7.3.1	М2.1	6.1.1	1.3		10.1.4, 10.3.2, 12
		6.1.2			
		6.2.1			
		6.3.2	2.1		
		6.3.8			
		6.5.8		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.3.2	М2.2	6.1.1	1.3		6.1.2, 6.1.3, 10.3.2, 12.1.1, 12.5
		6.1.2			
7.3.3	М2.3	6.1.1	1.3		6.1.2, 6.1.3, 12
		6.1.2			
7.3.4	М2.4	6.1.1	1.3		10.2
7.3.5	М2.5	6.1.2			10.1.1, 10.2, 10.3.2, 10.7.4, 12.5.1
		6.1.7			
		6.3.10			
		6.4.1			
	М2.6	6.1.2			
		6.1.7			
		6.3.10			
		6.4.1			
	М2.7	6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.3.7	М2.10	6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.1.4, 10.3.2, 12.4.2, 15.2.2
7.3.8	М2.11	6.1.7			15.2
	М2.12	6.1.7			

РС БР ИББС-2.3-2010

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.3.9	М2.13	6.3.7			10.2.1, 10.2.3
		6.3.8			10.4.1, 10.5
		6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.10.1, 12.4.1, 12.5.1, 12.5.2, 12.5.3
		6.3.10			
		6.5.8		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
	М2.14	6.3.7			
		6.3.8			
		6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.3.11	М2.16	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	10.5, 10.7.2, 10.10.3, 12.4.1
	М2.17	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
7.4.1	М3.1	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	7.1.1, 7.1.3, 10.7, 11.1
		6.4.1	2.1		11.6
	М3.2	6.1.7			
		6.5.3	2.1	4.3а	
7.4.2	М3.3	6.4.1			11
	М3.4	6.3.2	2.1		12.1
		6.3.3			
		6.4.1			
		6.5.2	2.1	4.2а, 4.3а	
		6.5.3	2.1	4.3а	
		6.5.10	2.1		
		6.5.11	2.1		
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	
7.4.3	М3.5	6.1.4	2.1		10.4, 10.5, 10.7
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	11, 12.2, 12.5.1
		6.5.2	2.1	4.2а, 4.3а	
		6.5.3	2.1	4.3а	
	М3.6	6.1.4	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.5.3	2.1	4.3а	
	М3.7	6.1.4	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.4.1	2.1		
		6.5.3	2.1	4.3а	
	М3.8	6.1.4	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.4.1	2.1		
		6.5.3	2.1	4.3а	
	М3.9	6.2.3	2.1, 2.4, 2.10		
		6.4.1	2.1		
	М3.10	6.4.1	2.1		

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
	М3.11	6.1.7			
		6.3.4	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.3.5	2.1		
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
		6.5.4	2.1	4.1б, 4.2б, 4.3б	
		6.5.5	2.1	4.1б, 4.2б, 4.3б	
		6.5.6	2.1	4.1б, 4.2б, 4.3б	
		6.5.7	2.1		
	М3.12	6.1.7			
		6.3.4	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.3.5	2.1		
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
		6.5.4	2.1	4.1б, 4.2б, 4.3б	
		6.5.5	2.1	4.1б, 4.2б, 4.3б	
		6.5.6	2.1	4.1б, 4.2б, 4.3б	
		6.5.7	2.1		
7.4.4	М3.14	6.1.7			10.10
	М3.15	6.1.7			
	М3.16	6.1.7			
	М3.17	6.1.7			
7.4.5	М3.18	6.1.8	2.1		9.1.2
	М3.19	6.1.8	2.1		9.1.5
	М3.20	6.1.8	2.1		
7.5.1	М4.1	6.1.3	2.1, 2.3		10.4.1
	М4.5	6.1.3	2.1, 2.3		
7.6.1	М5.1	6.2.3	2.1, 2.4, 2.10		10.6, 10.8, 10.9.2
		6.3.11	2.1, 2.4, 2.6–2.10	2.4	11.4, 11.7.2
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	
7.6.7	М5.15	6.2.3	2.1, 2.4, 2.10		10.4.1
		6.3.11	2.1, 2.4, 2.6–2.10	2.4	10.8.1, 10.8.4
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	11.4.6
7.6.10	М5.23	6.2.3	2.1, 2.4, 2.10		10.6
		6.3.11	2.1, 2.4, 2.6–2.10	2.4	11.4
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	
7.7.1	М6.1	6.5.10	2.1		10.8.1, 10.9.1
		6.5.11	2.1		11.5.2, 11.7.1
7.7.2	М6.3	6.4.1			12.2.3, 12.3
	М6.4	6.4.1			15.1.6
7.9.2	М8.1	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	7.2, 10.7
		6.4.1	2.1		
7.9.3	М8.3	6.1.2			7.1.1, 7.1.3, 7.2

РС БР ИББС-2.3-2010

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.9.4	М8.4	6.1.6			6.1.1, 6.1.3, 8.1.1
		6.3.5	2.1		
		6.3.10			
		6.5.7	2.1		
7.9.5	М8.5	6.1.2			10.10.2
		6.1.6			12.1
		6.1.7			15.2
		6.3.5	2.1		
		6.3.10			
		6.5.7	2.1		
7.9.6	М8.6	6.2.1			10.1.1, 10.2,
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	10.3.2, 10.7.4, 12.5.1
	М8.7	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
	М8.8	6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.9.7	М8.9	6.3.7			10.1.1, 10.3.2,
	М8.10	6.3.7			10.10.2, 12, 15.2
7.9.8	М8.12	6.1.7			15.2
		6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.9.9	М8.13	6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.1.1, 10.5, 13.2.1, 14.1.1, 14.1.3
		6.3.10			
7.11.3	М10.2	5.2	1.4		7.1, 7.2
	М10.3	5.2	1.4		
8.2.2	М11.9	6.1.8	2.1		6.1.1, 6.1.3
		6.2.3	2.1, 2.4, 2.10		8.1.1
		6.3.3			
		6.4.1			
		6.5.11	2.1		
	М28.9	6.1.8	2.1		
		6.2.3	2.1, 2.4, 2.10		
		6.3.3			
		6.4.1			
		6.5.11	2.1		
		6.1.8	2.1		
8.3.1	М12.2	5.2	1.4		7.1, 7.2
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	10.7
		6.4.1	2.1		
8.3.2	М12.3	5.2	1.4		7.1, 7.2
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	10.7
		6.4.1	2.1		
8.3.3	М12.4	5.2	1.4		7.1, 7.2, 10.7

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
8.6.2	M15.6	6.1.2			5, 6.1.5
		6.1.6			10.1.1, 10.7.4
		6.1.7			15.2
		6.1.9	2.1		
		6.2.1			
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.3.5	2.1		
		6.3.8			
		6.5.7	2.1		
	M15.7	6.1.2			
		6.1.6			
		6.1.7			
		6.2.1			
		6.3.8			
	M15.8	6.1.6			
		6.1.7			
		6.1.9	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.3.5	2.1		
		6.3.8			
		6.5.7	2.1		
8.7.1	M16.1	6.1.5			4.2,
	M29.1	6.1.5			6.1.1, 6.1.2, 10.1
8.8.2	M17.2	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	5, 6.1, 10, 11, 12
		6.4.1	2.1		
8.11.2	M20.2	6.3.10			14
8.11.3	M20.3	6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	14
8.11.5	M20.5	6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.1.4, 10.3.1, 10.5, 12.2, 12.5, 12.6, 13.4, 14
8.12.1	M21.1	6.1.7			10.10
		6.1.9	2.1		
		6.3.3			
8.12.6	M21.7	6.1.7			6.1.1, 6.1.3,
		6.1.9	2.1		8.1.1, 8.2.1,
	M21.8	6.1.7			10.10
	M32.1	6.1.7			
		6.1.9	2.1		
	M32.2	6.1.7			

Библиография

[1] Федеральный закон “О персональных данных” от 27 июля 2006 г. № 152-ФЗ.
[2] Постановление Правительства от 6 июля 2008 г. № 512 “Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных”.
[3] Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58 “Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных”.
[4] ISO/IEC 17799-2005 Information technology — Security techniques — Code of practice for information security management.

Ключевые слова: банковская система Российской Федерации, персональные данные, безопасность, информационная система персональных данных.

РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.4-2010

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

Дата введения: 2010-06-21

Издание официальное

Предисловие

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

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) модели угроз и нарушителей должны быть основным инструментом организации банковской системы Российской Федерации (БС РФ) при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности.

Настоящая Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ (далее — Отраслевая модель угроз) содержит актуальные для большинства организаций БС РФ угрозы безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн). Актуальные угрозы определены в результате проведения оценки рисков в соответствии с рекомендациями в области стандартизации Банка России РС БР ИББС-2.2-2009 “Обеспечение информационной безопасности организаций БС РФ. Методика оценки рисков нарушения информационной безопасности”.

РС БР ИББС-2.4-2010

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

Дата введения: 2010-06-21

1. Область применения

Настоящий документ распространяется на организации БС РФ и содержит актуальные для большинства организаций БС РФ угрозы безопасности персональных данных при их обработке в ИСПДн.

Настоящий документ рекомендован для применения путем включения ссылок и (или) прямого использования устанавливаемых в нем положений во внутренних документах организаций БС РФ.

В случае необходимости в организации БС РФ может быть составлена частная модель актуальных угроз безопасности персональных данных при их обработке в ИСПДн организации БС РФ (далее — частная модель угроз), учитывающая особенности обработки персональных данных в конкретной организации БС РФ. При этом:

— в случае сокращения набора угроз частной модели угроз (по сравнению с Отраслевой моделью угроз) рекомендуется проводить согласование частной модели угроз с Банком России и Федеральной службой по техническому и экспортному контролю (далее — ФСТЭК России);

— в случае расширения набора угроз частной модели угроз (по сравнению с Отраслевой моделью угроз) дополнительное согласование с Банком России и ФСТЭК России не требуется.

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

В качестве методики выбора актуальных для организации БС РФ угроз и последующего составления частной модели угроз рекомендуется использовать рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 “Обеспечение информационной безопасности организаций БС РФ. Методика оценки рисков нарушения информационной безопасности”.

2. Нормативные ссылки

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

3. Термины и определения

В настоящем документе применены термины в соответствии с СТО БР ИББС-1.0, а также следующие термины с соответствующими определениями:

3.1. **Источник угрозы безопасности персональных данных:** Объект или субъект, реализующий угрозы безопасности персональных данных путем воздействия на объекты среды обработки персональных данных организации БС РФ.

3.2. **Объект среды обработки персональных данных:** Материальный объект среды хранения, передачи, обработки, уничтожения и т.д. персональных данных.

3.3. **Оценка риска нарушения безопасности персональных данных:** Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения безопасности персональных данных, обрабатываемых в организации БС РФ.

3.4. **Риск нарушения безопасности персональных данных[1]:** Риск, связанный с угрозой безопасности персональных данных.

3.5. **Угроза безопасности персональных данных:** Угроза нарушения свойств безопасности персональных данных — доступности, целостности или конфиденциальности персональных данных организации БС РФ.

4. Обозначения и сокращения

БС — банковская система;
ИСПДн — информационная система персональных данных;
НСД — несанкционированный доступ;
ПДн — персональные данные;
РФ — Российская Федерация.

5. Общий подход к составлению Отраслевой модели угроз

5.1. Угрозы безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) организаций БС РФ — это:

- угроза нарушения доступности ПДн;
- угроза нарушения целостности ПДн;
- угроза нарушения конфиденциальности[2] (неправомерное использование) ПДн, в том числе за счет хищения отчуждаемых машинных носителей с несанкционированно копированной информацией.

5.2. Отраслевая модель угроз содержит систематизированный перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн, источников актуальных угроз безопасности ПДн, уровней реализации угроз безопасности ПДн, типов материальных объектов среды обработки ПДн (далее — актуальные угрозы безопасности ПДн).

Актуальная угроза безопасности ПДн — угроза безопасности ПДн, риск реализации которой не является допустимым для организации БС РФ по результатам проведения оценки рисков нарушения безопасности персональных данных, обрабатываемых в ИСПДн.

5.3. Отраслевая модель угроз содержит единые исходные данные по актуальным для организации БС РФ угрозам безопасности ПДн, связанным с несанкционированным, в том числе случайным, доступом в ИСПДн с целью ознакомления, изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с целью уничтожения или блокирования ПДн.

В рамках настоящей Отраслевой модели угроз под доступом к ПДн понимаются ознакомление с ПДн, их обработка, в частности, копирование, модификация или уничтожение ПДн (в со-

---

[1] Риски нарушения безопасности персональных данных заключаются в возможности утраты свойств безопасности персональных данных в результате реализации угроз безопасности персональных данных, вследствие чего субъекту персональных данных и (или) организации БС РФ может быть нанесен ущерб.

[2] Конфиденциальность ПДн – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или иного законного основания (пункт 10 статьи 3 Федерального закона “О персональных данных”). Обеспечение конфиденциальности ПДн не требуется в случае обезличивания ПДн и в отношении общедоступных ПДн (пункт 2 статьи 7 Федерального закона “О персональных данных”).

ответствии с Руководящим документом “Защита от несанкционированного доступа к информации. Термины и определения”, Гостехкомиссия России. М.: Воениздат, 1992).

К несанкционированному доступу (НСД) к ПДн при их обработке в ИСПДн, в частности, относятся:

доступ к ПДн или действия с ПДн, нарушающие установленные права и (или) правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн;

несанкционированное воздействие на ресурсы ИСПДн, осуществляемое с использованием вредоносных программ (вредоносного кода).

6. Исходные данные Отраслевой модели угроз

6.1. Категории ПДн:

категория 1 — персональные данные, отнесенные в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ “О персональных данных” (далее — Федеральный закон “О персональных данных”) [3] к специальным категориям персональных данных;

категория 2 — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к биометрическим персональным данным;

категория 3 — персональные данные, которые не могут быть отнесены к категории 1, категории 2 или категории 4;

категория 4 — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к общедоступным или обезличенным персональным данным.

6.2. Перечень основных источников угроз безопасности ПДн:

- неблагоприятные события природного и техногенного характера;
- террористы, криминальные элементы;
- компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак;
- поставщики программно-технических средств, расходных материалов, услуг и т.п.;
- подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт;
- сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие вне рамок предоставленных полномочий;
- сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие в рамках предоставленных полномочий.

6.3. Уровни информационной инфраструктуры, на которых возможна реализация угроз безопасности ПДн:

- физический уровень;
- сетевой уровень;
- уровень сетевых приложений и сервисов;
- уровень операционных систем;
- уровень систем управления базами данных;
- уровень банковских технологических процессов и приложений.

7. Отраслевая модель угроз

Отраслевая модель угроз безопасности ПДн (Таблица) содержит обобщенное описание угроз безопасности ПДн для каждой категории ПДн, включающее:

- источник угрозы безопасности ПДн;
- угроза безопасности ПДн;
- уровень реализации угрозы безопасности ПДн;
- типы материальных объектов среды обработки ПДн (далее — типы объектов среды).

Таблица. Отраслевая модель угроз безопасности ПДн

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
	ПДн категории 1, ПДн категории 2			
1	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение целостности
2				Нарушение доступности
3		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение целостности
4				Нарушение доступности
5		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
6				Нарушение целостности
7				Нарушение доступности
8		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
9				Нарушение целостности
10				Нарушение доступности
11		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
12				Нарушение целостности
13	Поставщики программно-технических средств, расходных материалов, услуг и т.п. и подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
14				Нарушение целостности
15		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
16				Нарушение целостности
17		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
18				Нарушение целостности
19	Сотрудники, действующие в рамках предоставленных полномочий	Физический уровень	Линии связи, аппаратные и технические средства, серверы, физические носители информации	Нарушение конфиденциальности
20				Нарушение целостности
21		Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение конфиденциальности
22				Нарушение целостности
23				Нарушение доступности
24		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение конфиденциальности
25				Нарушение целостности
26				Нарушение доступности
27		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
28				Нарушение целостности
29				Нарушение доступности
30		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
31				Нарушение целостности
32				Нарушение доступности
33		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
34				Нарушение целостности
35				Нарушение доступности

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
36	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
37				Нарушение целостности
38		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
39				Нарушение целостности
40		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
41				Нарушение целостности
	ПДн категории 3			
42	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение целостности
43				Нарушение доступности
44		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение целостности
45				Нарушение доступности
46		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
47				Нарушение целостности
48				Нарушение доступности
49		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
50				Нарушение целостности
51				Нарушение доступности
52	Сотрудники, действующие в рамках предоставленных полномочий	Физический уровень	Линии связи, аппаратные и технические средства, серверы, физические носители информации	Нарушение конфиденциальности
53				Нарушение целостности
54		Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение конфиденциальности
55				Нарушение целостности
56				Нарушение доступности
57		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение конфиденциальности
58				Нарушение целостности
59				Нарушение доступности
60		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
61				Нарушение целостности
62				Нарушение доступности
63		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
64				Нарушение целостности
65				Нарушение доступности
66		Уровень банковских технологических приложений и сервисов		Нарушение конфиденциальности
67				Нарушение целостности
68				Нарушение доступности

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
69	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
70				Нарушение целостности
71				Нарушение доступности
72		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
73				Нарушение целостности
74		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
75				Нарушение целостности
	ПДн категории 4			
76	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Уровень операционных систем	Файлы данных с ПДн	Нарушение целостности
77				Нарушение доступности
78		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение целостности
79				Нарушение доступности
80	Сотрудники, действующие в рамках предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение целостности
81				Нарушение доступности
82		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение целостности
83				Нарушение доступности
84		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение целостности
85				Нарушение доступности
86	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение целостности
87		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение целостности
88		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение целостности

Библиография

[1] Постановление Правительства РФ от 17 ноября 2007 г. № 781 “Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных”.

[2] Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 “Об утверждении Порядка проведения классификации информационных систем персональных данных”.

[3] Федеральный закон “О персональных данных” от 27 июля 2006 г. № 152-ФЗ.

Ключевые слова: банковская система Российской Федерации, персональные данные, модель угроз, информационная система персональных данных.

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЕСТНИК БАНКА РОССИИ

Нормативные акты и оперативная информация
Центрального банка Российской Федерации

№ 36–37 (1205–1206)

29 ИЮНЯ 2010

МОСКВА

Учредитель – Центральный банк Российской Федерации
107016, Москва, ул. Неглинная, 12
Адрес представительства Центрального банка Российской Федерации в Internet: *http://www.cbr.ru*
Тел. 771-43-73, факс 623-83-77, e-mail: *mvg@cbr.ru*

Издание зарегистрировано Комитетом Российской Федерации по печати. Регистрационный № 012253

Издатель и распространитель: ЗАО "АЭИ "ПРАЙМ-ТАСС"
125009, Москва, Тверской б-р, 2
Тел. 974-76-64, факс 692-36-90, *www.prime-tass.ru,* e-mail: *sales01@prime-tass.ru*

Отпечатано в типографии "ЛБЛ. Полиграф Сервис"
105066, г. Москва, ул. Нижняя Красносельская, 40/12

Москва, 2010