СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.0-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2014-06-01

Издание официальное

Москва
2014

Предисловие

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

2. ВЗАМЕН СТО БР ИББС-1.0-2010.

Содержание

Введение

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

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

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

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

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

Основные цели стандартизации по обеспечению ИБ организаций БС РФ:

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

Основные задачи стандартизации по обеспечению ИБ организаций БС РФ:

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

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения 2014-06-01

1. Область применения

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

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

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

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

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0”;

Рекомендации в области стандартизации Банка России РС БР ИББС-2.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”.

3. Термины и определения

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

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

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

[1] См. п. 3.4.

Примечание.

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

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

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

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

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

Примечание.

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

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

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

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

Примечание.

Информационная инфраструктура:

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

обеспечивает доступ потребителей к информационным ресурсам.

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

[ГОСТ Р 52069.0-2003]

Примечание.

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

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

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

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

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

[ГОСТ 34.003-90]

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

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

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

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

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

Примечания.

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

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

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

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

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

Примечание.

К активам организации БС РФ могут относиться:

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

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

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

банковские продукты и услуги, предоставляемые клиентам.

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

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

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

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

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

Примечания.

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

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

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

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

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

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

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

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

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

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

Примечания.

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

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

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

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

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

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

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

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

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

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

Примечание.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Примечание.

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

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

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

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

Примечание.

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

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

Примечание.

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

4. Обозначения и сокращения

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

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

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

Угрозы реализуются через их источники и имеют соответствующую вероятность реализации.

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Совокупность СИБ и СМИБ составляет СОИБ организации БС РФ.

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

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

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

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

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

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

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

Указанные группы процессов составляют СМИБ организации БС РФ.

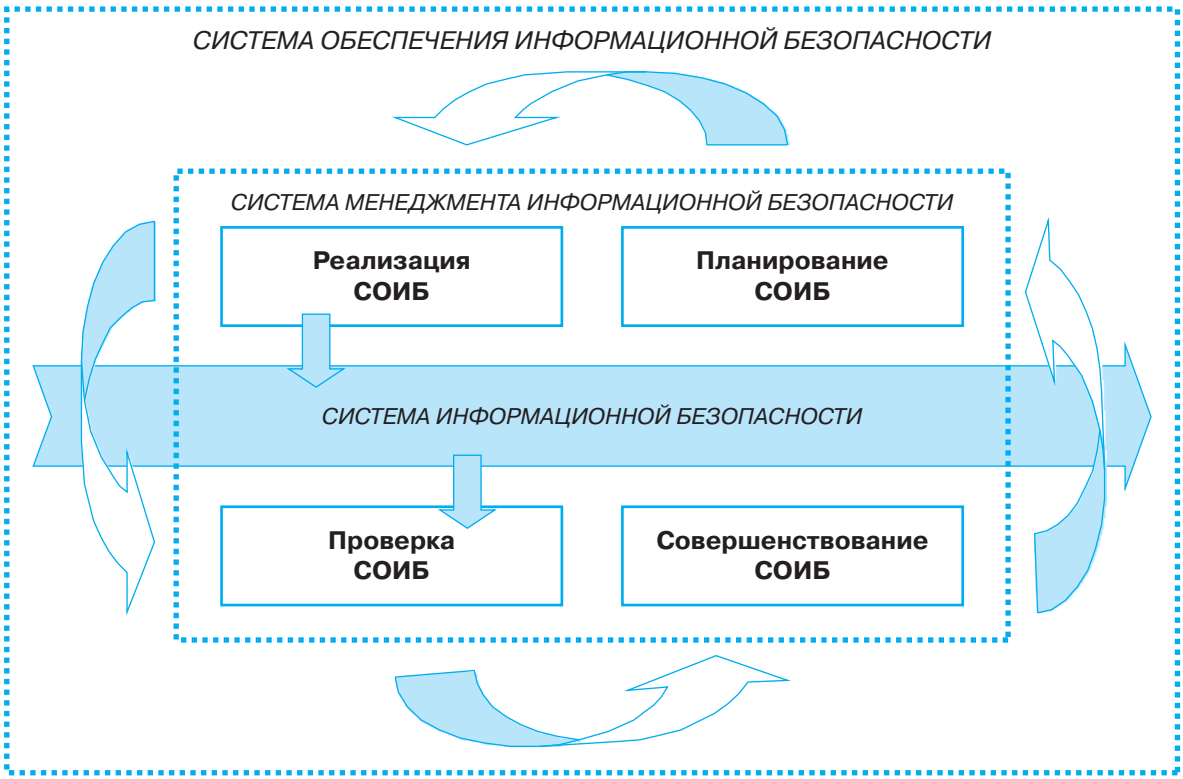
5.25. Менеджмент ИБ есть часть общего корпоративного менеджмента организации БС РФ, которая ориентирована на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы.

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

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

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

Рисунок 1. СОИБ организации БС РФ



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

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

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

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

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

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

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

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

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

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

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

6.6. Основными источниками угроз ИБ являются:

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

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

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

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

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

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

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

6.10. Источники угроз используют для реализации угрозы уязвимости ИБ.

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

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

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

7. Система информационной безопасности организаций банковской системы Российской Федерации

7.1. Общие положения

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

Указанные процедуры должны предусматривать фиксацию результатов проводимых проверок.

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

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

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

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

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

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

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

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

5. эксплуатация;

6. сопровождение и модернизация;

7. снятие с эксплуатации.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Процедуры управления доступом должны исключать возможность "самосанкционирования".

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

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

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

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

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

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

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

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

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

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

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

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

— операций с данными о клиентских счетах, включая операции открытия, модификации и закрытия клиентских счетов;
— проводимых транзакций, имеющих финансовые последствия;
— операций, связанных с назначением и распределением прав пользователей.

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

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

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

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

7.4.11. Должны быть определены и доведены до сведения работников и клиентов организации БС РФ процедуры, определяющие действия в случае компрометации информации, необходимой для их идентификации, аутентификации и (или) авторизации, в том числе произошедшей по их вине, включая информацию о способах распознавания таких случаев.

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

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

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

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

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

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

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

7.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Использование сети Интернет в неустановленных целях должно быть запрещено.

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

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

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

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

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

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

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

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

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

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

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

Рекомендуется организовать почтовый обмен с сетью Интернет через ограниченное количество точек, состоящих из внешнего (подключенного к сети Интернет) и внутреннего (подключенного к внутренним сетям организации) почтовых серверов с безопасной системой репликации почтовых сообщений между ними (интернет-киоски).

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

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

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

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

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

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

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

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

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

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

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

---

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

7.7.5. Для обеспечения безопасности необходимо использовать СКЗИ, которые:

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

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

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

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

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

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

— порядок ввода в действие, включая процедуры встраивания СКЗИ в АБС;
— порядок эксплуатации;
— порядок восстановления работоспособности в аварийных случаях;
— порядок внесения изменений;
— порядок снятия с эксплуатации;
— порядок управления ключевой системой;
— порядок обращения с носителями ключевой информации, включая действия при смене и компрометации ключей.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7.10.4.1. Для каждого ресурса ПДн должно быть обеспечено:

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

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

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

---

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

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

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

7.10.5.1. Указанные документы:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

в части обеспечения ИБ АБС на стадиях жизненного цикла:

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

в части обеспечения ИБ при управлении доступом и регистрации:

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

в части обеспечения ИБ банковских информационных технологических процессов:

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

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

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

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

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

---

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

8. Система менеджмента информационной безопасности организаций банковской системы Российской Федерации

8.1. Общие положения

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Рекомендуется наделить службу ИБ собственным бюджетом.

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

8.2.2. Служба ИБ должна быть наделена следующими минимальными полномочиями:

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

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

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

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

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

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

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

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

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

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

8.4.3. Методика оценки рисков нарушения ИБ/подход к оценке рисков нарушения ИБ организации БС РФ должна определять способ и порядок качественного или количественного оценивания риска нарушения ИБ на основании оценивания:

— степени возможности реализации угроз ИБ выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов организации БС РФ (типов информационных активов);
— степени тяжести последствий от потери свойств ИБ, в частности свойств доступности, целостности и конфиденциальности, для рассматриваемых информационных активов (типов информационных активов).

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

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

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

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

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

8.5. Требования к разработке планов обработки рисков нарушения информационной безопасности

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

— перенос риска на сторонние организации (например, путем страхования указанного риска);
— уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);

— осознанное принятие риска;
— формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирование планов по их реализации.

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

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

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

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

8.6.1. Разработку/коррекцию внутренних документов, регламентирующих деятельность в области обеспечения ИБ в организации БС РФ, рекомендуется проводить с учетом рекомендаций по стандартизации Банка России РС БР ИББС-2.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0”.

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

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

Политика ИБ организации БС РФ должна быть утверждена руководством.

8.6.3. В политике (в частных политиках) ИБ должны определяться/корректироваться:
— цели и задачи обеспечения ИБ;
— основные области обеспечения ИБ;
— типы основных защищаемых информационных активов;
— модели угроз и нарушителей;
— совокупность правил, требований и руководящих принципов в области ИБ;
— основные требования по обеспечению ИБ;
— принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов;
— основные принципы повышения уровня осознания и осведомленности в области ИБ;
— принципы реализации и контроля выполнения требований политики ИБ.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.12. Требования к мониторингу информационной безопасности и контролю защитных мер

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

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

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

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

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

8.13. Требования к проведению самооценки информационной безопасности

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

8.13.2. Самооценка ИБ должна проводиться в соответствии со стандартом Банка России СТО БР ИББС-1.2 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”. Порядок проведения самооценки ИБ рекомендуется организовывать в соответствии с рекомендациями по стандартизации Банка России РС БР ИББС-2.1 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0”.

8.13.3. Должна быть установлена и реализована программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки.

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

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

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

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

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

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

8.14. Требования к проведению аудита информационной безопасности

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

8.14.2. Должна быть установлена и реализована программа аудитов ИБ, содержащая информацию, необходимую для планирования и организации аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения указанных аудитов ИБ в заданные сроки.

8.14.3. Для каждого проводимого в организации БС РФ аудита ИБ необходимо установить план аудита, определяющий:

— цель аудита ИБ;
— критерии аудита ИБ;
— область аудита ИБ;
— дату и продолжительность проведения аудита ИБ;
— состав аудиторской группы;
— описание деятельности и мероприятий по проведению аудита;
— распределение ресурсов при проведении аудита.

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

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

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

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

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

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

8.15. Требования к анализу функционирования системы обеспечения информационной безопасности

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

8.17.5. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ.

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

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

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

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

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

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

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

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

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

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

8.18.6. Должны быть определены, выполняться, регистрироваться и контролироваться процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ.

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Основными целями проведения анализа функционирования СОИБ являются:

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

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

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

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

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

Библиография

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

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