

СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.0-2008

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2009-05-01

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 25 декабря 2008 года N Р-1674.

2. ВЗАМЕН СТО БР ИББС-1.0-2006.

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Банка России.

Введение

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

Особенности БС РФ таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов. В случаях наступления инцидентов ИБ значительно возрастает 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.

1. Область применения

Настоящий стандарт распространяется на организации банковской системы Российской Федерации (далее - организации БС РФ) и устанавливает положения по обеспечению ИБ в организациях БС РФ.

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

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

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

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО 9001-2001 Система менеджмента качества. Требования

3. Термины и определения

Термины, установленные настоящим стандартом, применяются во всех видах документации и во всех видах деятельности по обеспечению ИБ в рамках Комплекса БР ИББС <*>.

<*> См. п. 3.4.

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

3.2. Стандарт: Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.

[ГОСТ Р 1.12-2004]

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

[ГОСТ Р 1.12-2004]

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

3.5. Менеджмент: Скоординированная деятельность по руководству и управлению.

[ГОСТ Р ИСО 9000-2001]

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), т.е. свойством, 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 [3].

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

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

Примечание.

Информационная инфраструктура:

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

обеспечивает доступ потребителей к информационным ресурсам.

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

[ГОСТ Р 52069.0-2003]

Примечание.

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

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

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

3.13. Технологический процесс: Процесс, реализующий некоторую технологию.

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

[ГОСТ 34.003-90]

3.15. Авторизация: Предоставление прав доступа.

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

3.17. Аутентификация: 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 иницилируемые от их имени процессы по выполнению действий над объектами.

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

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

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

3.22. Актив: Все, что имеет ценность для организации банковской системы Российской Федерации и находится в ее распоряжении.

Примечание.

К активам организации банковской системы Российской Федерации могут относиться:

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

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

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

банковские продукты и услуги, предоставляемые клиентам.

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

3.24. Классификация информационных активов: Разделение существующих информационных активов организации банковской системы Российской Федерации по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

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

3.26. Ресурс: Актив организации банковской системы Российской Федерации, который используется или потребляется в процессе выполнения некоторой деятельности.

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

Примечания.

1. Операции над активами организации банковской системы Российской Федерации могут выполняться вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем.

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

3.28. Банковский платежный технологический процесс: Часть банковского технологического процесса, реализующая банковские операции над информационными активами организации банковской системы Российской Федерации, связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций.

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

Примечания.

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

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

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

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

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

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

Примечания.

1. Защищенность достигается обеспечением совокупности свойств ИБ - доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) организации банковской системы Российской Федерации.

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

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

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

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

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

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

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

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

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

Примечание.

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

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

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

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

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

3.46. Инцидент информационной безопасности; инцидент ИБ: Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, т.е. реализацию нарушения свойств ИБ информационных активов организации банковской системы Российской Федерации.

Примечание.

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

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

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

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

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

3.51. Оценка риска нарушения информационной безопасности: Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации банковской системы Российской Федерации на всех стадиях их жизненного цикла.

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

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

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

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

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

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

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

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

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

3.61. Аудит информационной безопасности; аудит ИБ: Систематический, независимый и документируемый процесс получения свидетельств деятельности

организации банковской системы Российской Федерации по обеспечению ИБ, установления степени выполнения в организации банковской системы Российской Федерации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ организации банковской системы Российской Федерации.

Примечание.

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

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

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

Примечание.

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

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

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

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

Примечание.

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

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

Примечание.

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

4. Обозначения и сокращения

АБС - автоматизированная банковская система;

БС - банковская система;

ЖЦ - жизненный цикл;

ИБ - информационная безопасность;

НСД - несанкционированный доступ;

НРД - нерегламентированные действия в рамках предоставленных полномочий;

РФ - Российская Федерация;

СКЗИ - средство криптографической защиты информации;
СМИБ - система менеджмента информационной безопасности;
СИБ - система информационной безопасности;
СОИБ - система обеспечения информационной безопасности;
ЭВМ - электронная вычислительная машина;
ЭЦП - электронная цифровая подпись.

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

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

Угрозы реализуются через их источники и имеют соответствующую вероятность реализации.

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

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

<*> 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.

<*> 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).

Если злоумышленнику удастся 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.

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

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

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

С целью снижения рисков нарушения ИБ и управления ими собственник создает уполномоченный орган - свою службу ИБ (подразделение (лица) в организации БС РФ, ответственное 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) <*>.

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

Чем обоснованнее и точнее сделан прогноз, тем потенциально ниже риски нарушения ИБ организации БС РФ при минимальных ресурсных затратах. При этом следует учитывать, что со временем угрозы, их источники и риски могут изменяться. Поэтому модели следует периодически пересматривать.

5.8. Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации БС РФ - разработать политику ИБ организации БС РФ и в соответствии с ней реализовать, эксплуатировать и совершенствовать СОИБ организации БС РФ.

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

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

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

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

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

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

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

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

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

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

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

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

5.18. Анализ и оценка рисков нарушения ИБ должна основываться на идентификации активов организации БС РФ, на их ценности для целей и задач организации БС РФ, на моделях угроз и нарушителей ИБ организации БС РФ.

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

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

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

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

менеджмента отделены от основных и вспомогательных процессов, которые являются объектами менеджмента.

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

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

Совокупность СИБ и СМИБ составляет СОИБ организации БС РФ.

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

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

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

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

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

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

- планирование СОИБ организации БС РФ ("планирование");
- реализация СОИБ организации БС РФ ("реализация");
- мониторинг и анализ СОИБ организации БС РФ ("проверка");
- поддержка и улучшение СОИБ организации БС РФ ("совершенствование").

Указанные группы процессов составляют СМИБ организации БС РФ.

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

Группы процессов СМИБ организации БС РФ следует организовывать в виде циклической модели Деминга "... - планирование - реализация - проверка - совершенствование - планирование - ...", которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO/IEC IS 27001-2005 [4]. Организация и выполнение процессов СМИБ необходимы в том числе для обеспечения уверенности в том, что хороший практический опыт организации БС РФ документируется, становится обязательным к применению, а СОИБ совершенствуется.

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

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

Рисунок 1. СОИБ организации БС РФ (не приводится)

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

Другими целями злоумышленника могут являться, например, нарушение функционирования бизнес-процессов организации БС РФ путем нарушения доступности или целостности информационных активов, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

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

6.6. Основными источниками угроз ИБ являются:

- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;

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

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

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

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

- внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;
- комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре <*>.

<*> На данных уровнях и уровне бизнес-процессов реализация угроз внешними нарушителями ИБ, действующими самостоятельно, без соучастия внутренних, практически невозможна.

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

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

6.10. Источники угроз используют для реализации угрозы уязвимости ИБ.

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

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

7. Система информационной безопасности организаций банковской системы Российской Федерации

7.1. Общие положения

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

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

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

7.1.2. Положения подразделов 7.2 - 7.9 настоящего стандарта образуют базовый набор требований к СИБ, применимый к большинству организаций БС РФ. В соответствии с особенностями конкретной организации БС РФ данный базовый набор требований может быть расширен путем выполнения деятельности в рамках процессов СМИБ организации БС РФ, например, определения области действия СОИБ организации БС РФ, анализа и оценки рисков нарушения ИБ.

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

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

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" <*>;

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

- "знать своего служащего" <*>;

<*> "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.

- "необходимо знать" <*>;

<*> "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.

- а также рекомендуется использовать принцип "двойное управление" <*>.

<*> "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.

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

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

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

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

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

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

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

- банковский платежный технологический процесс;
- платежную информацию.

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

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

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

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

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

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

7.2.5. В организации БС РФ должны быть документально определены процедуры приема на работу, влияющую на обеспечение ИБ, включающие:

- проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов;
- проверку в части профессиональных навыков и оценку профессиональной пригодности.

Указанные процедуры должны предусматривать документальную фиксацию результатов проводимых проверок.

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

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

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

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

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

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

7.3.1. При формировании требований по обеспечению ИБ рекомендуется рассматривать следующие общие стадии модели ЖЦ АБС:

1. разработка технических заданий;
2. проектирование;
3. создание и тестирование;
4. приемка и ввод в действие;
5. эксплуатация;
6. сопровождение и модернизация;
7. снятие с эксплуатации.

В случае разработки АБС в организации БС РФ рекомендуется рассматривать все стадии ЖЦ АБС, а в случае приобретения готовых АБС рекомендуется рассматривать стадии 4 - 7 ЖЦ АБС.

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

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

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

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

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

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

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

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

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

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

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

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

Результаты выполнения контроля должны документироваться.

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

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

срока предусмотрены соответствующими нормативными и (или) договорными документами. Результаты выполнения процедур должны документироваться.

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

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

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

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

Процедуры управления доступом должны исключать возможность "самосанционирования".

Результаты контроля процедур должны документироваться.

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

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

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

Результаты контроля выполнения порядка доступа должны оформляться документально.

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

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

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

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

7.4.8. При заключении договоров со сторонними организациями рекомендуется юридическое оформление договоренностей, предусматривающих необходимый уровень взаимодействия в случае выхода инцидента ИБ за рамки отдельной организации БС РФ. Примером такого взаимодействия может служить приостановка выполнения

распределенной между несколькими организациями транзакции в случае, если имеющиеся данные мониторинга и анализа протоколов операций позволяют предположить, что выполнение данной транзакции является частью замысла злоумышленников.

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

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

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

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

7.4.12. Работа всех пользователей АБС должна осуществляться под уникальными учетными записями.

7.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

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

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

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

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

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

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

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

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

7.5.6. Должны быть документально определены и выполняться процедуры предварительной проверки устанавливаемого или изменяемого программного обеспечения на отсутствие вирусов. После установки или изменения программного

обеспечения должна быть выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки должны документироваться.

7.5.7. Должны быть документально определены процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, должны быть зафиксированы:

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

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

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

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

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

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

Использование сети Интернет в неустановленных целях должно быть запрещено.

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

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

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

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

7.6.5. При осуществлении дистанционного банковского обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного

клиента злоумышленником в рамках сеанса работы. Все попытки таких подмен должны регистрироваться регламентированным образом.

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

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

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

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

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

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

7.6.10. При взаимодействии с сетью Интернет должны быть документально определены и использоваться защитные меры противодействия атакам хакеров и распространению спама <*>.

<*> Спам - общее наименование не запрошенных пользователями электронных посланий и рекламных писем, рассылаемых в Интернете по ставшим известными рассылающей стороне адресам пользователей.

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

7.7.1. СКЗИ предназначены для защиты информации при ее обработке, хранении и передаче по каналам связи. Применение СКЗИ в АБС должно проводиться в соответствии с моделью нарушителя, принятой организацией БС РФ. Рекомендуется утвердить политику (концепцию) применения СКЗИ в организации БС РФ.

7.7.2. СКЗИ:

- должны допускать встраивание в технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

- должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

- должны быть сертифицированы уполномоченным государственным органом, либо реализованы на основе рекомендованных уполномоченным государственным органом алгоритмов либо алгоритмов, определенных условиями договора с контрагентом (клиентом) организации БС РФ, либо соответствовать стандартам организации, взаимодействующей с организацией БС РФ.

7.7.3. При применении СКЗИ в АБС должна поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для всех звеньев АБС, взаимодействующих со СКЗИ.

7.7.4. ИБ процессов изготовления ключевых документов СКЗИ должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

7.7.5. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем в АБС рекомендуется реализовать процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена электронными сообщениями, и все инциденты ИБ.

7.7.6. Порядок применения СКЗИ в АБС определяется руководством организации БС РФ 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.

7.7.7. Ключи ЭЦП и (или) иных СКЗИ (например, кодов аутентификации <*>) должны изготавливаться в каждой организации и (или) физическим лицом самостоятельно. В случае изготовления ключей для одной организации БС РФ в другой организации правовые и организационные следствия таких действий должны быть отражены в соответствующем договоре.

<*> Код аутентификации - средство защиты информации, используемое для контроля целостности и подтверждения подлинности электронных документов. Код аутентификации позволяет подтвердить его принадлежность зарегистрированному владельцу.

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

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

7.8.2. Банковский платежный технологический процесс должен быть документирован в организации БС РФ.

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

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

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

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

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

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

7.8.8. Комплекс мер по обеспечению ИБ банковского платежного технологического процесса должен предусматривать в том числе:

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

- доступ работника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения должностных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;

- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;

- аутентификацию входящих электронных платежных сообщений;

- двустороннюю аутентификацию автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;

- возможность ввода платежной информации в АБС только для авторизованных пользователей;

- контроль, направленный на исключение возможности совершения злоумышленных действий (двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций и т.д.);

- восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

- сверку выходных электронных платежных сообщений с соответствующими входными и обработанными электронными платежными сообщениями при осуществлении межбанковских расчетов;

- доставку электронных платежных сообщений участникам обмена.

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

7.8.9. При проектировании, разработке и эксплуатации систем дистанционного банковского обслуживания должны быть документально определены и выполняться процедуры, реализующие в том числе механизмы:

- снижения вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами;

- доведения информации о возможных рисках, связанных с выполнением операций или транзакций до клиентов.

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

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

7.8.11. Должна осуществляться и быть регламентирована процедура периодического контроля всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ платежной информации. Регламентирующие документы

должны быть согласованы со службой либо лицом, отвечающим в организации БС РФ за обеспечение ИБ.

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

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

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

7.9.2. В организации БС РФ рекомендуется провести классификацию неплатежной информации.

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

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

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

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

7.9.6. Банковские информационные технологические процессы должны быть документированы в организации БС РФ. Указанные документы должны быть согласованы со службой ИБ. Указанные технологические процессы должны быть реализованы в рамках созданных для этих целей АБС. Не входящие в состав данных АБС серверы, офисные ЭВМ и другое оборудование рекомендуется изолировать от АБС на уровне локальных вычислительных сетей способом, согласованным со службой либо лицом, отвечающим в организации за ИБ.

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

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

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

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 (см. п. 5.25).

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 - руководством).

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

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

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

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

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

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

обеспечения непрерывности бизнеса, поскольку на стадии "проверка" определена необходимость в этом. Пример второй ситуации - идентификация новой угрозы и 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 и контролю защитных мер;
- требования к проведению самооценки ИБ;
- требования к проведению аудита ИБ;
- требования к анализу функционирования СОИБ;
- требования к анализу СОИБ со стороны руководства организации БС РФ;
- требования к принятию решений по тактическим улучшениям СОИБ;
- требования к принятию решений по стратегическим улучшениям СОИБ.

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

8.2.1. Для реализации, эксплуатации, контроля и поддержания на должном уровне СОИБ руководству следует сформировать службу ИБ (назначить уполномоченное лицо), а также утвердить цели и задачи ее деятельности.

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

Рекомендуется наделить службу ИБ собственным бюджетом.

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

8.2.2. Служба ИБ (уполномоченное лицо) должна быть наделена следующими минимальными полномочиями:

- организовывать составление и контролировать выполнение всех планов по обеспечению ИБ организации БС РФ;
- разрабатывать и вносить предложения по изменению политик ИБ организации;

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

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

8.3.1. Должна быть документально определена/скорректирована опись структурированных по классам защищаемых информационных активов (типов информационных активов - типов информации). Классификацию информационных активов рекомендуется проводить на основании оценок ценности информационных активов для интересов (целей) организации БС РФ, например, в соответствии с тяжестью последствий потери свойств ИБ информационных активов.

8.3.2. В случае наличия в организации БС РФ классификации информационных активов опись информационных активов должна содержать информацию о принадлежности конкретного информационного актива к выделенным типам информационных активов.

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

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

8.3.5. В организации БС РФ должны быть документально определены роли по определению/коррекции области действия СОИБ, по составлению и пересмотру описи информационных активов (типов информационных активов), находящихся в области действия СОИБ. В организации БС РФ должны быть назначены ответственные за выполнение указанных ролей.

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

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

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

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

- степени возможности реализации угроз ИБ выявленными и (или) предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя, в результате их воздействия на объекты среды информационных активов организации БС РФ (типов информационных активов);

- степени тяжести последствий от потери свойств ИБ, в частности, свойств доступности, целостности и конфиденциальности, для рассматриваемых информационных активов (типов информационных активов).

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

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

8.4.5. В организации БС РФ рекомендуется создать и поддерживать в актуальном состоянии единый информационный ресурс (базу данных), содержащий информацию об инцидентах ИБ.

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

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

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

8.5. Требования к разработке планов обработки рисков нарушения информационной безопасности

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

- перенос риска на сторонние организации (например, путем страхования указанного риска);

- уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска);

- осознанное принятие риска;

- формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и 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 реализации требований по обеспечению ИБ должны содержать последовательность и сроки реализации и внедрения организационных, технических и иных защитных мер.

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

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

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

8.6.2. В организации БС РФ должны разрабатываться/корректироваться следующие внутренние документы:

- политика ИБ организации БС РФ;
- частные политики ИБ организации БС РФ;
- документы, регламентирующие процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ организации БС РФ.

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

Политика ИБ организации БС РФ должна быть утверждена руководством.

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

- цели и задачи обеспечения ИБ;
- основные области обеспечения ИБ;
- типы основных защищаемых информационных активов;
- модели угроз и нарушителей;
- совокупность правил, требований и руководящих принципов в области ИБ;
- основные требования по обеспечению ИБ;
- принципы противодействия угрозам ИБ по отношению к типам основных защищаемых информационных активов;
- основные принципы повышения уровня осознания и осведомленности в области ИБ;
- принципы реализации и контроля выполнения требований политики ИБ.

8.6.4. Разработка/корректировка внутренних документов, регламентирующих деятельность в области обеспечения ИБ, должна проводиться на основе:

- законодательства Российской Федерации;
- комплекса БР ИББС, в частности, требований 7-го и 8-го разделов настоящего стандарта;
- нормативных актов и предписаний регулирующих и надзорных органов;
- договорных требований организации БС РФ со сторонними организациями;
- результатов оценки рисков, выполненной с соответствующей уровню разрабатываемого документа детализацией рассматриваемых информационных активов (типов информационных активов).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8.8.1. Должны быть документально определены и выполняться проектирование/приобретение/развертывание, внедрение, эксплуатация, контроль и сопровождение эксплуатации защитных мер (СИБ), предусмотренных планами реализации требований по обеспечению ИБ.

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

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

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

8.9.1. Должна быть организована документально оформленная и утвержденная руководством работа с персоналом организации БС РФ в направлении повышения осведомленности и обучения в области ИБ, включая разработку и реализацию планов и программ обучения и повышения осведомленности в области ИБ и контроля результатов выполнения указанных планов.

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

8.9.3. Программы обучения и повышения осведомленности должны включать информацию:

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

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

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

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

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

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

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

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

8.10.2. В организации БС РФ рекомендуется сформировать и поддерживать в актуальном состоянии централизованную базу данных инцидентов ИБ. Должны быть

документально определены процедуры по хранению информации об инцидентах ИБ, практиках анализа инцидентов ИБ и результатах реагирования на инциденты ИБ.

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

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

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

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

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

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

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

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

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

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

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

Реализация и использование защитных мер обеспечения непрерывности бизнеса и его восстановления после прерывания должна основываться на соответствующих требованиях по обеспечению ИБ.

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

8.11.7. Должно быть документально определено и выполняться периодическое тестирование плана обеспечения непрерывности бизнеса и его восстановления после прерывания. По результатам тестирования при необходимости проводится

соответствующая корректировка плана. Сценарий тестирования должен быть составлен с учетом существующей в организации БС РФ модели угроз и нарушителей, а также результатов оценки рисков.

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

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

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

8.12. Требования к мониторингу и контролю защитных мер

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

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

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

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

8.12.5. Процедуры мониторинга СОИБ и контроля защитных мер должны подвергаться регулярным и документально зафиксированным пересмотрам в связи с изменениями в составе и способах использования защитных мер, выявлением новых угроз и уязвимостей ИБ, а также на основе данных об инцидентах ИБ. Порядок выполнения процедур пересмотра должен быть документально определен.

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

8.13. Требования к проведению самооценки информационной безопасности

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

8.13.2. Должна быть документально определена и реализована программа самооценок ИБ, содержащая информацию, необходимую для планирования и организации самооценок ИБ, их контроля, анализа и совершенствования, а также обеспечения их

ресурсами, необходимыми для эффективного и результативного проведения указанных самооценок ИБ в заданные сроки.

8.13.3. В организации БС РФ должны быть документально определены:

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

8.13.4. Для каждой проводимой в организации БС РФ самооценки ИБ необходимо документально оформить план проведения самооценки, определяющий:

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

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

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

8.14. Требования к проведению аудита информационной безопасности

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

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

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

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

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

- порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудита ИБ;

- порядок взаимодействия с аудиторской организацией в процессе проведения аудита ИБ;

- порядок взаимодействия аудиторской группы и руководства, позволяющий представителям аудиторской группы при необходимости непосредственно обращаться к руководству;

- порядок организации опроса работников;

- порядок организации наблюдения за деятельностью работников организации БС РФ со стороны представителей аудиторской организации.

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

8.14.6. Должен быть документально определен порядок хранения, доступа и использования материалов, получаемых в процессе проведения аудитов, в частности, отчетов аудитов.

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

8.15. Требования к анализу функционирования системы обеспечения информационной безопасности

8.15.1. В организации БС РФ должен проводиться анализ функционирования СОИБ, использующий в том числе:

- результаты мониторинга СОИБ и контроля защитных мер;
- сведения об инцидентах ИБ;
- результаты проведения аудитов ИБ, самооценок ИБ;
- данные об угрозах, возможных нарушителях и уязвимостях ИБ;
- данные об изменениях внутри организации БС РФ, например, данные об изменениях в процессах и технологиях, реализуемых в рамках основного процессного потока, изменениях во внутренних документах организации БС РФ;
- данные об изменениях вне организации БС РФ, например, данные об изменениях в законодательстве Российской Федерации, изменениях в требованиях комплекса БР ИББС, изменениях в договорных обязательствах организации.

8.15.2. Анализ функционирования СОИБ должен включать в том числе:

- анализ соответствия комплекса внутренних документов, регламентирующих деятельность по обеспечению ИБ в организации БС РФ, требованиям законодательства Российской Федерации, требованиям стандартов Банка России, в частности, требованиям настоящего стандарта, контрактным требованиям организации;
- анализ соответствия внутренних документов нижних уровней иерархии, регламентирующих деятельность по обеспечению ИБ в организации БС РФ, требованиям политик ИБ организации БС РФ;
- оценку адекватности модели угроз организации БС РФ существующим угрозам ИБ;
- оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска;
- проверку адекватности используемых защитных мер требованиям внутренних документов организации БС РФ и результатам оценки рисков;
- анализ отсутствия разрывов в технологических процессах обеспечения ИБ, а также несогласованности в использовании защитных мер.

8.15.3. Результаты анализа функционирования СОИБ должны документироваться.

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

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

8.16.1. В организации БС РФ должен быть утвержден перечень документов (данных), необходимых для формирования информации, предоставляемой руководству с целью проведения анализа СОИБ. В частности, в указанный перечень документов должны входить:

- отчеты с результатами мониторинга СОИБ и контроля защитных мер;
- отчеты с результатами анализа функционирования СОИБ;
- отчеты с результатами аудитов ИБ;
- отчеты с результатами самооценок ИБ;
- документы, содержащие информацию о способах и методах защиты, защитных мерах или процедурах их использования, которые могли бы использоваться для улучшения функционирования СОИБ;
- документы, содержащие информацию о новых, выявленных уязвимостях и угрозах ИБ;
- документы, содержащие информацию о действиях, предпринятых по итогам предыдущих анализов СОИБ, осуществленных руководством;
- документы, содержащие информацию об изменениях, которые могли бы повлиять на организацию СОИБ, например, изменения в законодательстве Российской Федерации и (или) в положениях стандартов Банка России;
- документы, содержащие информацию по выявленным инцидентам ИБ;
- документы, подтверждающие выполнение требуемой деятельности по обеспечению ИБ, например, выполнение планов обработки рисков;
- документы, подтверждающие выполнение требований непрерывности бизнеса и его восстановления после прерывания.

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

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

8.17. Требования к принятию решений по тактическим <*> улучшениям системы обеспечения информационной безопасности

<*> 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.

8.17.1. Для принятия решений, связанных с тактическими улучшениями СОИБ, необходимо рассмотреть среди прочего документально оформленные результаты:

- аудитов ИБ;
- самооценок ИБ;
- мониторинга СОИБ и контроля защитных мер;
- анализа функционирования СОИБ;
- обработки инцидентов ИБ;
- выявления новых угроз и уязвимостей ИБ;
- оценки рисков;
- анализа перечня защитных мер, возможных для применения;
- стратегических улучшений СОИБ;
- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций).

8.17.2. Решения по тактическим улучшениям СОИБ должны быть документально зафиксированы и должны либо содержать выводы об отсутствии необходимости

тактических улучшений СОИБ, либо указывать направления тактических улучшений СОИБ в виде корректирующих или превентивных действий, например:

- пересмотр процедур выполнения отдельных видов деятельности по обеспечению ИБ;

- пересмотр процедур эксплуатации отдельных видов защитных мер;

- пересмотр процедур обнаружения и обработки инцидентов;

- уточнение описи информационных активов;

- пересмотр программы обучения и повышения осведомленности персонала;

- пересмотр плана обеспечения непрерывности бизнеса и его восстановления после прерывания;

- пересмотр планов обработки рисков;

- вынесение санкций в отношении персонала;

- пересмотр процедур мониторинга СОИБ и контроля защитных мер;

- пересмотр программ аудитов;

- корректировка соответствующих внутренних документов, регламентирующих процедуры выполнения деятельности по обеспечению ИБ и эксплуатации защитных мер;

- ввод новых или замена используемых защитных мер.

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

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

8.17.5. Должны быть документально определены и выполняться процедуры согласования и информирования заинтересованных сторон о тактических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

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

8.18. Требования к принятию решений по стратегическим <*> улучшениям системы обеспечения информационной безопасности

<*> 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.

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

- аудитов ИБ;

- самооценок ИБ;

- мониторинга СОИБ и контроля защитных мер;

- анализа функционирования СОИБ;

- обработки инцидентов ИБ;

- выявления новых информационных активов организации БС РФ или их типов;

- выявления новых угроз и уязвимостей ИБ;

- оценки рисков;

- пересмотра основных рисков ИБ;

- анализа СОИБ со стороны руководства;
- анализа успешных практик в области ИБ (собственных или других организаций), а также изменения:
- в законодательстве Российской Федерации;
- в нормативных актах Банка России, в частности, требованиях настоящего стандарта;
- интересов, целей и задач бизнеса организации БС РФ;
- контрактных обязательств организации БС РФ.

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

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

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

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

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

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

8.18.6. Должны быть документально определены и выполняться процедуры согласования и информирования заинтересованных сторон о стратегических улучшениях СОИБ, в частности, об изменениях, относящихся к обеспечению ИБ, к ответственности в области ИБ, к требованиям по обеспечению ИБ, а также должны быть документально зафиксированы результаты выполнения указанных процедур.

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

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

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

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

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

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

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

Мониторинг и контроль защитных мер проводятся 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. Аудит ИБ проводится внешними, независимыми проверяющими организациями как для собственных целей самой организации БС РФ, так и с целью повышения доверия к ней со стороны других организаций.

Требования к проведению аудита ИБ организации БС РФ определены в подразделе 8.13 настоящего стандарта, а также в стандарте Банка России СТО БР ИББС-1.1 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности".

9.4. При подготовке к аудиту ИБ рекомендуется проведение самооценки ИБ. Самооценка ИБ проводится собственными силами и по инициативе руководства организации.

Порядок проведения самооценки ИБ в организации БС РФ определен в рекомендациях в области стандартизации Банка России РС БР ИББС-2.1 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям стандарта СТО БР ИББС-1.0".

9.5. В процессе аудита ИБ и (или) самооценки ИБ проводится оценка степени выполнения требований настоящего стандарта и на ее основе вычисление итогового уровня ИБ организации БС РФ. Порядок проведения указанной деятельности (оценка и вычисление) регламентируется стандартом Банка России СТО БР ИББС-1.2 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0".

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

Основными целями проведения анализа функционирования СОИБ являются:

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

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

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

Библиография

[1] Федеральный закон "О банках и банковской деятельности" от 01.12.1990 N 395-1 в редакции ФЗ от 03.02.1996 N 17-ФЗ, от 31.07.1998 N 151-ФЗ, от 05.07.1999 N 126-ФЗ, от 08.07.1999 N 136-ФЗ, от 19.06.2001 N 82-ФЗ, от 07.08.2001 N 121-ФЗ, от 21.03.2002 N 31-ФЗ, с изменениями, внесенными Постановлением Конституционного суда РФ от 23.02.1999 N 4-П

[2] Федеральный закон "О Центральном банке Российской Федерации (Банке России)" от 10 июля 2002 года N 86-ФЗ

[3] Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. N 149-ФЗ

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