СТО БР ИББС-1.0-2004

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2004-12-01

Предисловие

1. РАЗРАБОТАН ООО НПФ “Кристалл” по заказу Центрального банка Российской Федерации (Банка России).

ДОРАБОТАН редакционной группой в следующем составе:

Банк России: Лахтиков А.И., Курило А.П., Гиленко В.Д., Поспелов А.Л., Гвоздев И.М., Харламов В.П.

ООО НПФ “Кристалл”: Андрианов В.В., Голованов В.Б., Каминский В.Г., Алексеев В.М., Зефиров С.Л.

РАССМОТРЕН И РЕКОМЕНДОВАН к применению Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” национального органа по стандартизации следующим составом членов подкомитета: Банк России, Ассоциация российских банков, Акционерный коммерческий Сберегательный банк Российской Федерации, Ассоциация региональных банков, Московская межбанковская валютная биржа, Национальная валютная ассоциация, ОАО “Альфа-банк”, ОАО Россельхозбанк, ГНИИИ ПТЗИ Федеральной службы по техническому и экспортному контролю, аудиторская компания KPMG, ОАО Банк “Петрокоммерц”, Институт Банковского Дела Ассоциации российских банков, Банк “Российский кредит”.

2. ВНЕСЕН Техническим комитетом 362 национального органа по стандартизации.

3. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 18 ноября 2004 года № Р-609.

4. ВВЕДЕН ВПЕРВЫЕ.

Содержание

1. Область применения 5
2. Нормативные ссылки 5
3. Термины и определения 6
4. Обозначения и сокращения 8
5. Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций БС РФ 8
6. Основные принципы обеспечения информационной безопасности организаций БС РФ 9
6.1. Общие принципы безопасного функционирования организации 9
6.2. Специальные принципы обеспечения информационной безопасности организации 10
7. Модели угроз и нарушителей информационной безопасности организаций БС РФ 10
8. Политика информационной безопасности организаций БС РФ 12
8.1. Состав и назначение политики информационной безопасности организаций БС РФ 12
8.2. Общие (основные) требования по обеспечению информационной безопасности, отображаемые в политиках информационной безопасности организации 12
8.2.1. Общие требования по обеспечению информационной безопасности для организации БС РФ 12
8.2.2. Общие требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу 12
8.2.3. Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла 13
8.2.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации 14
8.2.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты 15
8.2.6. Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет 16
8.2.7. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации 17
8.2.8. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов 17
8.2.9. Общие требования по обеспечению информационной безопасности банковских информационных технологических процессов 19
9. Управление информационной безопасностью организации БС РФ 20
10. Модель зрелости процессов управления информационной безопасностью организаций БС РФ 21
11. Аудит и мониторинг информационной безопасности организаций БС РФ 23
12. Направления развития стандарта 24
Библиография 24
Приложение А. Терминосистемы, используемые в стандарте 25

Введение

Банковская система Российской Федерации (БС 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 информационной безопасности банковских технологических процессов (платежных, информационных и пр.), автоматизированных банковских систем (АБС), эксплуатирующихся организациями БС РФ, и т.д.

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

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционные, кредитные 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, поэтому Банк России является сторонником регулярной оценки уровня ИБ в организациях БС РФ, оценки рисков и принятия мер, необходимых для управления этими рисками.

Исходя из этого разработан настоящий стандарт по обеспечению ИБ организаций БС РФ.

Основные цели стандартизации по обеспечению ИБ организаций БС РФ:

- повышение доверия к БС РФ;
- повышение стабильности функционирования организаций БС РФ и на этой основе — стабильности функционирования БС РФ в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение и/или снижение ущерба от инцидентов ИБ.

Основные задачи стандартизации по обеспечению ИБ организаций БС РФ:

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

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2004-12-01

1. Область применения

Настоящий стандарт распространяется на организации банковской системы Российской Федерации (далее по тексту — организации БС РФ) и устанавливает положения (политики, требования и т.п.) по обеспечению информационной безопасности в организациях БС РФ.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и 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 конкретных положений обязательность не установлена действующим законодательством Российской Федерации, нормативным правовым актом Банка России или условиями договора.

2. Нормативные ссылки

Настоящий стандарт разработан с учетом следующих стандартов и документов:

ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения.

ГОСТ 3.1109-82 Единая система технологической документации. Термины и определения основных понятий.

ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения.

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения.

ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты.

ГОСТ Р ИСО 9000-2001 Системы менеджмента качества. Основные положения и словарь.

ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия безопасности.

ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств.

ГОСТ Р ИСО/МЭК ТО 15271-2002 Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств).

ISO/IEC IS 17799-2000 Information Technology. Code of practice for information security management.

BS 7799-2-2002 Information security management systems. Specification with guidance for use.

ISO/IEC TR 13335 Information Technology. Security techniques. Guidelines for the management of IT security.

ISO TR 13569 Banking and related financial services. Information security guidelines.

ISO/IEC TR 18044 Information Technology. Security techniques. Information security incident management.

ISO/IEC IS 15288-2002 Information Technology. Life Cycle Management. System Life Cycle Processes.

ISO/IEC TR 15504-98 Information Technology. Software Process Assessment.

COBIT Control Objectives for Information and related Technology, 3rd Edition, July 2000.

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation.

CRAMM UK Government's Risk Analysis and Management Method.

3. Термины и определения

Для целей настоящего стандарта используются следующие термины.

3.1. **Автоматизированная банковская система:** Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая банковскую информационную технологию.

3.2. **Активы организации банковской системы Российской Федерации:** Все, представляющее ценность для организации БС РФ с точки зрения достижения ее целей.

Примечание.

К активам организации БС РФ могут относиться:

- банковские ресурсы (финансовые, людские, вычислительные, телекоммуникационные и пр.);
- информационные активы, в т.ч. различные виды банковской информации (платежной, финансово-аналитической, служебной, управляющей и пр.) на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;
- банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем и др.);
- банковские продукты и услуги, предоставляемые клиентам.

3.3. **Аудит информационной безопасности организации банковской системы Российской Федерации:** Периодический, независимый от объекта аудита и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организациях БС РФ установленных требований по обеспечению информационной безопасности.

Примечания.

1. Внутренние аудиты ("аудиты первой стороной") проводятся самой организацией или от ее имени для анализа менеджмента или других внутренних целей и могут служить основанием для самодеклараций организации о соответствии требованиям по ИБ.

2. Внешние аудиты включают "аудиты второй стороной" и "аудиты третьей стороной". Аудиты второй стороной проводятся сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами от их имени. Аудиты третьей стороной проводятся внешними независимыми организациями.

3.4. **Аутентификация электронного сообщения:** Процесс проверки сообщения, позволяющий установить, что сообщение исходит из указанного источника и не было изменено при передаче.

3.5. **Банковская информационная технология:** Приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования финансовой или другой связанной с функционированием организаций БС РФ, информации.

3.6. **Банковская технология:** Совокупность методов деятельности и процессов в банковской отрасли, а также описание способов деятельности.

Примечание.

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

3.7. **Банковский информационный технологический процесс:** Часть банковского технологического процесса, содержащая операции над неплатежной информацией, необходимой для функционирования организации БС РФ.

Примечание.

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

3.8. **Банковский платежный технологический процесс:** Часть банковского технологического процесса, содержащая расчетные, учетные, кассовые и иные банковские операции над

платежной информацией, связанные с перемещением денежных средств с одного счета на другой, открытием (закрытием) счетов или контролем за данными операциями.

Примечание.

Платежная информация может включать в себя платежные (расчетные) сообщения и информацию, связанную с проведением расчетных, учетных, кассовых и иных операций.

3.9. **Банковский технологический процесс:** Технологический процесс, содержащий операции по изменению и(или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг.

Примечания.

1. Операции над банковской информацией могут выполняться вручную или быть автоматизированными, например, с помощью комплексов средств автоматизации автоматизированных банковских систем.

2. Операции над банковской информацией требуют указания ролей их участников (исполнителей и лиц, принимающих решения или имеющих полномочия по изменению технологических процессов, в том числе персонала автоматизированных банковских систем).

3.10. **Информационная безопасность организации банковской системы Российской Федерации:** Состояние защищенности интересов (целей) организации БС РФ в условиях угроз в информационной сфере.

Примечания.

1. Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

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.

3.11. **Информационные активы организации банковской системы Российской Федерации:** Активы организации БС РФ, представляющие ценность для нее с точки зрения достижения целей и имеющие отношение к ее информационной сфере.

3.12. **Инцидент информационной безопасности:** Действительное, предпринимаемое или вероятное нарушение информационной безопасности.

Примечание.

Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности, учетности или неотказуемости.

3.13. **Ключ кода аутентификации электронного сообщения:** Данные, используемые при создании и проверке кода аутентификации электронного сообщения.

3.14. **Код аутентификации электронного сообщения:** Данные, используемые для установления подлинности и контроля целостности электронного сообщения.

3.15. **Модель зрелости процессов управления информационной безопасностью организации банковской системы Российской Федерации:** Схема для измерения проработанности процессов управления информационной безопасностью организации БС РФ.

3.16. **Мониторинг информационной безопасности организации банковской системы Российской Федерации:** Постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности в организации БС РФ, сбор, анализ и обобщение результатов наблюдения под заданные цели.

Примечания.

1. Объектом мониторинга в зависимости от целей может быть автоматизированная банковская система или ее часть, банковские информационные технологические процессы, информационные банковские услуги и пр.

2. Цели мониторинга информационной безопасности определяются службой безопасности организации БС РФ.

3.17. **Оценка соответствия информационной безопасности организации банковской системы Российской Федерации установленным требованиям:** Любая деятельность, связанная с прямым или косвенным определением того, что выполняются или не выполняются соответствующие требования информационной безопасности в организации БС РФ.

3.18. **Политика информационной безопасности организации:** Одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

3.19. **Процесс:** Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

3.20. **Роль в организации банковской системы Российской Федерации:** Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом в организации БС РФ.

Примечания.

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

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

3.21. **Свидетельство аудита:** Записи, изложение фактов или другой информации, связанной с критериями аудита, которые могут быть перепроверены.

Примечание.

Свидетельство аудита может быть качественным или количественным.

3.22. **Требование:** Положение нормативного документа, содержащее критерии, которые должны быть соблюдены.

3.23. **Управление информационной безопасностью организации банковской системы Российской Федерации:** Совокупность целенаправленных действий, осуществляемых для достижения заявленных целей организации БС РФ в условиях угроз в информационной сфере.

Примечание.

Совокупность действий включает оценку ситуации и состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер (средств управления информационной безопасностью).

3.24. **Уязвимость:** Недостатки или слабые места активов, которые могут быть использованы угрозой.

4. Обозначения и сокращения

БС — банковская система;
РФ — Российская Федерация;
АБС — автоматизированная банковская система;
ИБ — информационная безопасность;
ОС — операционная система;
СУБД — система управления базами данных;
НСД — несанкционированный доступ;
ЖЦ — жизненный цикл;
ЭВМ — электронная вычислительная машина;
ЛВС — локальная вычислительная сеть;
СКЗИ — средство криптографической защиты информации;
ЭЦП — электронная цифровая подпись;
КА — код аутентификации.

5. Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций БС РФ

5.1. В основе исходной концептуальной схемы информационной безопасности организаций БС РФ лежит противоборство собственника[1] и злоумышленника[2] за контроль над информационными активами. Однако другие, незлоумышленные действия, также лежат в сфере рассмотрения данного стандарта.

В случае если злоумышленник устанавливает контроль над информационными активами, как самой организации БС РФ, так и клиентам, которые доверили ей свои собственные активы, наносится ущерб.

5.2. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. Внешний злоумышленник, скорее да, чем нет, может иметь сообщника(ов) внутри организации.

---

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

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

5.3. Собственник практически никогда не знает о готовящемся нападении, оно всегда бывает неожиданным. Нападения, как правило, носят локальный и конкретный по месту, цели и времени характер.

5.4. Злоумышленник изучает объект нападения, как правило, не только теоретически, никак не проявляя себя, но и практически, путем эксперимента, подбора "отмычек" к системе обеспечения ИБ организации. Таким образом, он отрабатывает наиболее эффективный метод нападения. Поэтому собственник должен постоянно стремиться к выявлению следов такой активности. В том числе и для этой цели собственник создает уполномоченный орган — свою службу обеспечения ИБ (подразделения (лица) в организации, ответственные за обеспечение ИБ).

5.5. Сложно и ресурсоемко, а значит, малоэффективно искать следы такой активности и по факту настраивать свою систему обеспечения ИБ. Поэтому главный инструмент собственника — основанный на опыте прогноз (составление модели угроз и модели нарушителя)[1].

Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ в организации БС РФ при минимальных ресурсных затратах.

5.6. Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ для собственника — разработать на основе точного прогноза политику ИБ и в соответствии с ней построить систему управления ИБ.

5.7. Политика ИБ организаций БС РФ разрабатывается на основе принципов обеспечения ИБ организаций БС РФ, моделей угроз и нарушителей, идентификации активов, подлежащих защите, оценки рисков и с учетом особенностей и интересов конкретного собственника.

Собственник должен знать, что он должен защищать. Собственник должен знать и уметь выделять (идентифицировать) наиболее важный для его бизнеса информационный актив (ресурс).

5.8. Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ в финансовой организации оказывают серьезное влияние отношения как в коллективе, так и между коллективом и собственником или менеджментом организации, представляющим интересы собственника. Поэтому этими отношениями необходимо управлять.

5.9. Любые защитные меры в силу ряда объективных причин со временем имеют тенденцию к ослаблению своей эффективности, в результате чего общий уровень ИБ может снижаться. Это неминуемо ведет к возрастанию рисков ИБ.

Для того чтобы этого не допустить, необходимо проводить регулярный мониторинг и аудит системы обеспечения ИБ организаций БС РФ и своевременно принимать меры по поддержанию эффективности системы управления ИБ на необходимом уровне за счет руководства и управления ИБ организации на основе циклической модели: "планирование — реализация — проверка — совершенствование — планирование — ...".

5.10. Далеко не каждый собственник располагает потенциалом для составления точного прогноза (модели угроз и модели нарушителя). Такой прогноз может и должен составляться с учетом опыта ведущих специалистов банковской системы, а также с учетом международного опыта в этой сфере. Аналогично должны разрабатываться и основные требования ИБ организаций БС РФ.

5.11. Стратегия обеспечения ИБ организаций БС РФ, таким образом, заключается в использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников. В случае реализации не предусмотренных планом угроз должен быть использован дополнительный (специально разработанный) план действий, позволяющий свести к минимуму возможные потери.

6. Основные принципы обеспечения информационной безопасности организаций БС РФ

6.1. Общие принципы безопасного функционирования организации

6.1.1. **Своевременность обнаружения проблем.** Организация должна своевременно обнаруживать проблемы[2], потенциально способные повлиять на ее бизнес-цели.

6.1.2. **Прогнозируемость развития проблем.** Организация должна выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.

---

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

[2] Здесь и далее по тексту стандарта рассматриваются проблемы, прямо или косвенно относящиеся к ИБ.

6.1.3. **Оценка влияния проблем на бизнес-цели.** Организация должна адекватно оценивать степень влияния выявленных проблем на ее бизнес-цели.

6.1.4. **Адекватность защитных мер.** Организация должна выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.

6.1.5. **Эффективность защитных мер.** Организация должна эффективно реализовывать принятые защитные меры.

6.1.6. **Использование опыта при принятии и реализации решений.** Организация должна накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

6.1.7. **Непрерывность принципов безопасного функционирования.** Организация должна обеспечивать непрерывность реализации принципов безопасного функционирования.

6.1.8. **Контролируемость защитных мер.** Организация должна применять только те защитные меры, правильность работы которых может быть проверена, при этом организация должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели организации.

6.2. Специальные принципы обеспечения информационной безопасности организации

Реализация специальных принципов обеспечения ИБ направлена на повышение уровня зрелости процессов управления ИБ в организации.

6.2.1. **Определенность целей.** Функциональные цели и цели ИБ организации должны быть явно определены во внутрибанковском документе. Неопределенность приводит к “расплывчатости” организационной структуры, ролей персонала, политик ИБ и невозможности оценки адекватности принятых защитных мер.

6.2.2. **Знание своих клиентов и служащих.** Организация должна обладать информацией о своих клиентах, тщательно подбирать персонал (служащих), вырабатывать и поддерживать корпоративную этику, что создает благоприятную доверительную среду для деятельности организации по управлению активами.

6.2.3. **Персонификация и адекватное разделение ролей и ответственности.** Ответственность должностных лиц организации за решения, связанные с ее активами, должна персонифицироваться и осуществляться преимущественно в форме поручительства. Она должна быть адекватной степени влияния на цели организации, фиксироваться в политиках, контролироваться и совершенствоваться.

6.2.4. **Адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки.** Роли должны адекватно отражать исполняемые функции и процедуры их реализации, принятые в организации. При назначении взаимосвязанных ролей должна учитываться необходимая последовательность их выполнения. Роль должна быть согласована с критериями оценки эффективности ее выполнения. Основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки.

6.2.5. **Доступность услуг и сервисов.** Организация должна обеспечить доступность для своих клиентов и контрагентов услуг и сервисов в установленные сроки, определенные соответствующими договорами (соглашениями) и/или иными документами.

6.2.6. **Наблюдаемость и оцениваемость обеспечения ИБ.** Любые предлагаемые защитные меры должны быть устроены так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен подразделением организации, имеющим соответствующие полномочия.

7. Модели угроз и нарушителей информационной безопасности организаций БС РФ

7.1. Модели угроз и нарушителей (прогноз ИБ) должны быть основным инструментом менеджмента организации при развертывании, поддержании и совершенствовании системы обеспечения ИБ организации.

7.2. 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 (сетевые аппаратные средства: 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.

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

7.4. Главной целью злоумышленника является получение контроля над 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".

7.5. Организация должна определить конкретные объекты защиты на каждом из уровней информационной инфраструктуры.

7.6. Наиболее актуальные источники угроз на физическом, сетевом уровнях и уровне сетевых приложений:
— внешние источники угроз: лица, распространяющие вирусы и другие вредоносные программы, хакеры, фрикеры[1]; и иные лица, осуществляющие несанкционированный доступ (НСД);
— внутренние источники угроз, реализующие угрозы в рамках своих полномочий и за их пределами (персонал, имеющий права доступа к аппаратному оборудованию, в том числе, сетевому, администраторы сетевых приложений и т.п.);
— комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно.

7.7. Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:
— внутренние, реализующие угрозы в рамках своих полномочий и за их пределами (администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.);
— комбинированные источники угроз: внешние и внутренние, действующие в сговоре[2].

7.8. Наиболее актуальные источники угроз на уровне бизнес-процессов:
— внутренние источники, реализующие угрозы в рамках своих полномочий и за их пределами (авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.);
— комбинированные источники угроз: внешние (например, конкуренты) и внутренние, действующие в сговоре.

7.9. Также необходимо учитывать угрозы, связанные с природными и техногенными катастрофами и террористической деятельностью.

7.10. Источники угроз для реализации угрозы используют уязвимости объектов и системы защиты.

7.11. Хорошей практикой является разработка моделей угроз и нарушителей ИБ для данной организации.

Модель угроз ИБ включает описание источников угрозы, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба.

Для источников угроз — людей может быть разработана модель нарушителя ИБ, включающая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, и возможной мотивации их действий.

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

7.12. При анализе угроз ИБ необходимо исходить из того, что эти угрозы непосредственно влияют на операционные риски деятельности организации. Операционные риски сказываются на бизнес-процессах организации.

7.13. Операционные риски порождаются следующими эксплуатационными факторами: технические неполадки, ошибочные (случайные) и/или преднамеренные злоумышленные действия персонала организации, ее клиентов при их непосредственном доступе к АБС организаций и другими факторами.

---

[1] **Фрикер** — злоумышленник, скрытно подключающийся с помощью различных устройств и приемов к телефонным сетям, обеспечивая себе связь с любой точкой мира, с указанием номера законного абонента, который и оплачивает телефонные услуги.

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

7.14. Наиболее эффективным способом минимизации рисков нарушения ИБ для собственника является разработка совокупности мероприятий, методов и средств, создаваемых и поддерживаемых для обеспечения требуемого уровня безопасности информационных активов (системы обеспечения ИБ) в соответствии с политикой ИБ организации БС РФ, разрабатываемой в том числе и на основе моделей угроз и нарушителей ИБ.

8. Политика информационной безопасности организаций БС РФ

8.1. Состав и назначение политики информационной безопасности организаций БС РФ

8.1.1. Собственник (и/или менеджмент) организации должен обеспечить разработку, принятие и внедрение политики ИБ организации БС РФ, включая выделение требуемых для реализации этой политики ресурсов.

8.1.2. Политика ИБ должна описывать цели и задачи системы обеспечения ИБ и определять совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется организация в своей деятельности.

8.1.3. Должны быть назначены лица, ответственные за реализацию политики ИБ и поддержание ее в актуальном состоянии.

8.2. Общие (основные) требования по обеспечению информационной безопасности, отображаемые в политиках информационной безопасности организации

8.2.1. Общие требования по обеспечению информационной безопасности для организации БС РФ

8.2.1.1. Требования ИБ должны быть взаимоувязаны в непрерывный по задачам, подсистемам, уровням и стадиям жизненного цикла комплекс.

8.2.1.2. Требования ИБ должны определять содержание и цели деятельности организации БС РФ в рамках процессов управления ИБ.

8.2.1.3. Эти требования должны быть сформулированы как минимум для следующих областей:

- назначения и распределения ролей и доверия к персоналу;
- стадий жизненного цикла АБС;
- защиты от НСД, управления доступом и регистрацией в АБС, в телекоммуникационном оборудовании и автоматических телефонных станциях и т.д.;
- антивирусной защиты;
- использования ресурсов Интернет;
- использования средств криптографической защиты информации;
- защиты банковских платежных и информационных технологических процессов.

Политика ИБ организации БС РФ может учитывать и другие области, такие, как обеспечение непрерывности, физическая защита и т.д., отвечающие ее бизнес-целям.

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

8.2.2.1. Роль — это заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом, например, сотрудником организации, и неким объектом, например, программно-аппаратным средством.

Для эффективного выполнения целей организации и задач по управлению активами должны быть выделены и определены соответствующие роли персонала организации. Роли следует персонифицировать с установлением ответственности за их исполнение. Формирование ролей, как правило, должно осуществляться на основании бизнес-процессов. Ответственность должна быть зафиксирована в должностных инструкциях.

8.2.2.2. При определении ролей для сотрудников организации БС РФ необходимо учитывать цели организации, имеющиеся ресурсы, функциональные и процедурные требования, критерии оценки эффективности выполнения правил для данной роли.

8.2.2.3. Не рекомендуется, чтобы одна персональная роль целиком отражала цель, например, включала все правила, требуемые для реализации бизнес-процесса. Совокупность правил, составляющих роли, не должна быть критичной для организации с точки зрения последствий успешного нападения на ее исполнителя. Не следует совмещать в одном лице (в любой комбинации) роли разработки, сопровождения, исполнения, администрирования или контроля, например, исполнителя и администратора, администратора и контролера или других комбинаций.

8.2.2.4. Роль должна быть обеспечена ресурсами, необходимыми и достаточными для ее выполнения.

8.2.2.5. Роли должны группироваться и взаимодействовать так, чтобы организационная структура соответствовала целям организации. Роль одного из руководителей организации (уполномоченного менеджера, высшего менеджера и т.п.) должна включать задачу координации своевременности и качества выполнения ролей сотрудников для достижения целей организации.

8.2.2.6. Ненадлежащее выполнение правил назначения и распределения ролей создает уязвимости.

8.2.2.7. Для контроля за качеством выполнения требований ИБ в организации должны быть выделены и определены роли по обеспечению ИБ.

8.2.2.8. При приеме на работу должны быть проверены идентичность личности, заявляемая квалификация, точность и полнота биографических фактов, наличие рекомендаций.

8.2.2.9. Лиц, которых предполагается принять на работу, связанную с защищаемыми активами или операциями, следует подвергать проверке в части профессиональных навыков и оценки профессиональной пригодности. Рекомендуется выполнять контрольные проверки уже работающих сотрудников регулярно, а также внепланово при выявлении фактов их нештатного поведения, или участия в инцидентах ИБ, или подозрений в таком поведении или участии.

8.2.2.10. Весь персонал организации БС РФ должен давать письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов. При этом условие о соблюдении конфиденциальности должно распространяться на всю защищаемую информацию, доверенную сотруднику или ставшую ему известной в процессе выполнения им своих служебных обязанностей.

Для внешних организаций требования по ИБ регламентируются положениями, включаемыми в договора (соглашения).

8.2.2.11. Персонал организации должен быть компетентным для выполнения своих функций в области обеспечения ИБ. Компетентность персонала следует обеспечивать с помощью процессов обучения в области ИБ, осведомленности персонала и периодической проверки уровня компетентности.

8.2.2.12. Обязанности персонала по выполнению требований ИБ в соответствии с положениями ISO TR 13569 и ISO/IEC IS 17799-2000 следует включать в трудовые контракты (соглашения, договора).

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

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

8.2.3.2. При заказе АБС модель ЖЦ (стадии ЖЦ, этапы работ и процессы ЖЦ, выполняемые на этих стадиях) рекомендуется определять в соответствии с ГОСТ 34.601 и документом ISO/IEC IS 15288.

8.2.3.3. Разработка технических заданий, проектирование, создание и тестирование и приемка средств и систем защиты АБС должны осуществляться по согласованию с подразделениями (лицами) в организации БС РФ, ответственными за обеспечение ИБ.

8.2.3.4. Ввод в действие, эксплуатация, снятие с эксплуатации АБС в части вопросов ИБ должны осуществляться при участии подразделения (лиц) в организации, ответственного за обеспечение ИБ.

8.2.3.5. На стадиях, связанных с разработкой АБС (определение требований заинтересованных сторон, анализ требований, архитектурное проектирование, реализация, интеграция и верификация, поставка, ввод в действие), разработчиком должна быть обеспечена защита от угроз:

- неверной формулировки требований к АБС;
- выбора неадекватной модели ЖЦ АБС, в том числе неадекватного выбора процессов ЖЦ и вовлеченных в них участников;
- принятия неверных проектных решений;
- внесения разработчиком дефектов на уровне архитектурных решений;
- внесения разработчиком недокументированных возможностей в АБС;
- неадекватной (неполной, противоречивой, некорректной и пр.) реализации требований к АБС;
- разработки некачественной документации;
- сборки АБС разработчиком/производителем с нарушением требований, что приводит к появлению недокументированных возможностей в АБС либо к неадекватной реализации требований;

— неверного конфигурирования АБС;
— приемки АБС, не отвечающей требованиям заказчика;
— внесения недокументированных возможностей в АБС в процессе проведения приемочных испытаний посредством недокументированных возможностей функциональных тестов и тестов ИБ.

8.2.3.6. 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.

8.2.3.7. При приобретении организациями БС РФ готовых АБС и их компонентов разработчиком должна быть предоставлена документация, содержащая в том числе описание защитных мер, предпринятых разработчиком в отношении угроз, перечисленных в п. 8.2.3.5.

Также разработчиком должна быть представлена документация, содержащая описание защитных мер, предпринятых разработчиком АБС и их компонентов относительно безопасности разработки, безопасности поставки и эксплуатации, поддержки жизненного цикла, включая описание модели жизненного цикла, оценки уязвимости. Данная документация может быть представлена в рамках декларации о соответствии или быть результатом оценки соответствия изделия, проведенной в рамках соответствующей системы оценки.

В договор (контракт) о поставке АБС и их компонентов организациям БС РФ рекомендуется включать положения по сопровождению поставляемых изделий на весь срок их службы. В случае невозможности включения в договор (контракт) указанных требований к разработчику должна быть рассмотрена возможность приобретения полного комплекта рабочей конструкторской документации на изделие, обеспечивающего возможность сопровождения АБС и их компонентов без участия разработчика. Если оба указанных варианта неприемлемы, например, вследствие высокой стоимости, руководство организации БС РФ должно обеспечить анализ влияния угрозы невозможности сопровождения АБС и их компонентов на обеспечение непрерывности бизнеса.

8.2.3.8. На стадии эксплуатации в соответствии с документом ISO TR 13569 должна быть обеспечена защита от следующих угроз:
— умышленное несанкционированное раскрытие, модификация или уничтожение информации;
— неумышленная модификация или уничтожение информации;
— недоставка или ошибочная доставка информации;
— отказ в обслуживании или ухудшение обслуживания.

Кроме этого, актуальной является угроза отказа от авторства сообщения.

8.2.3.9. На стадии сопровождения должна быть обеспечена защита от угроз:
— внесения изменений в АБС, приводящих к нарушению ее функциональности либо к появлению недокументированных возможностей;
— невнесения разработчиком/поставщиком изменений, необходимых для поддержки правильного функционирования и правильного состояния АБС.

8.2.3.10. На стадии снятия с эксплуатации должно быть обеспечено удаление информации, несанкционированное использование которой может нанести ущерб бизнес-деятельности организации, и информации, используемой средствами обеспечения ИБ, из постоянной памяти АБС или с внешних носителей.

8.2.3.11. Требования ИБ должны включаться во все договора и контракты на проведение работ или оказание услуг на всех стадиях ЖЦ АБС.

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

8.2.4.1. При распределении прав доступа персонала и клиентов к активам организации БС РФ следует руководствоваться специальным принципом “знание своих клиентов и служащих” (см. п. 6.2.2), выражаемым следующим образом:
— “знать своего клиента”[1];
— “знать своего служащего”[2];

---

[1] **“Знать своего клиента”** *(Know your Customer):* принцип, используемый регулирующими органами для выражения отношения к финансовым организациям с точки зрения знания деятельности их клиентов [ISO TR 13569].

[2] **“Знать своего служащего”** *(Know your Employee):* принцип, демонстрирующий озабоченность организации по поводу отношения служащих к своим обязанностям и возможных проблем, таких, как злоупотребление имуществом, аферы или финансовые трудности, которые могут приводить к проблемам с безопасностью [ISO TR 13569].

— “необходимо знать”[1],

а также руководствоваться принципом “двойное управление”[2].

8.2.4.2. В составе АБС должны использоваться сертифицированные или разрешенные к применению средства защиты информации от НСД.

8.2.4.3. В организации должны обеспечиваться: идентификация, аутентификация, авторизация; управление доступом; контроль целостности; регистрация, включая:

— функционирование системы парольной защиты электронных вычислительных машин (ЭВМ) и локальных вычислительных сетей (ЛВС). Рекомендуется организовать службу централизованной парольной защиты для генерации, распространения, смены, удаления паролей, разработки необходимых инструкций, контроля за действиями персонала по работе с паролями;
— непротиворечивая и прозрачная административно-техническая поддержка задач управления доступом к ресурсам ЭВМ и/или ЛВС. Назначение/лишение полномочий по доступу сотрудников к ресурсам ЭВМ и/или ЛВС санкционируется руководителем функционального подразделения организации, несущего персональную ответственность за обеспечение ИБ в данном подразделении;
— контроль доступа пользователей к ресурсам ЭВМ и/или ЛВС. Оперативный контроль доступа пользователей осуществляется подразделениями (лицами) в организации, ответственными за обеспечение ИБ;
— формирование уникальных идентификаторов сообщений и идентификаторов пользователей (виды идентификаторов определяются особенностями конкретного технологического процесса);
— регистрация действий персонала и пользователей в специальном электронном журнале. Данный электронный журнал должен быть доступным для чтения, просмотра, анализа, хранения и резервного копирования только администратору ИБ. При невозможности поддержки данного режима эксплуатирующимися в организации БС РФ аппаратно-программными средствами, реализация данного требования должна быть обеспечена организационными и/или административными мерами.

8.2.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты

8.2.5.1. В организации должны применяться только официально приобретенные средства антивирусной защиты. Установка и регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах АБС должны осуществляться администраторами АБС.

Лучшей практикой является автоматическая установка обновлений антивирусного программного обеспечения.

8.2.5.2. При обеспечении антивирусной защиты в организации должны быть разработаны и введены в действие инструкции по антивирусной защите, учитывающие особенности банковских технологических процессов. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена.

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

8.2.5.3. В ЭВМ и АБС не допускается присутствие и использование программного обеспечения и данных, не связанных с выполнением конкретных функций в банковских технологических процессах организации.

8.2.5.4. Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка.

8.2.5.5. При обнаружении компьютерного вируса необходимо принять меры по устранению последствий вирусной атаки, проинформировать руководство и приостановить при необходимости работу (на период устранения последствий вирусной атаки).

---

[1] **“Необходимо знать”** *(Need to Know):* принцип безопасности, который ограничивает доступ к информации и ресурсам по обработке информации тем, кому требуется выполнять определенные обязанности [ISO TR 13569].

[2] **“Двойное управление”** *(Dual Control):* принцип сохранения целостности процесса и борьбы с искажением функций системы, требующий того, чтобы два лица независимо предпринимали некое действие до завершения определенных транзакций [ISO TR 13569].

8.2.5.6. Отключение или необновление антивирусных средств не допускается. Установка и обновление антивирусных средств в организации должны контролироваться представителями подразделений (лицами) в организации, ответственными за обеспечение ИБ.

8.2.5.7. Ответственность за выполнение требований инструкции по антивирусной защите должна быть возложена на руководителя функционального подразделения организации, а обязанности по выполнению мер антивирусной защиты должны быть возложены на каждого сотрудника организации, имеющего доступ к ЭВМ и/или АБС.

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

8.2.6.1. Ресурсы сети Интернет в организации БС РФ могут использоваться для ведения дистанционного банковского обслуживания (например, Internet-banking), получения и распространения информации, связанной с банковской деятельностью (путем создания информационных web-сайтов), информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями исключительно с внешними организациями, а также ведения собственной хозяйственной деятельности.

Иное использование ресурсов сети Интернет, решение о котором не принято руководством организации в установленном порядке, должно рассматриваться как нарушение ИБ.

При принятии руководством организации решений об использовании сети Интернет для производственной и/или собственной хозяйственной деятельности 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;
— гарантии по обеспечению ИБ при использовании сети Интернет никаким органом не предоставляются.

8.2.6.2. В организациях БС РФ, осуществляющих дистанционное банковское обслуживание клиентов, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет обязательно должны применяться соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации (СКЗИ) и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии. Хорошей практикой является выделение и неподключение к внутренним сетям ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет.

8.2.6.3. Почтовый обмен через сеть Интернет должен осуществляться с использованием защитных мер.

Хорошей практикой является наличие в организации ограниченного количества точек почтового обмена с сетью Интернет, 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).

8.2.6.4. Электронная почта должна архивироваться. Архив должен быть доступен только подразделению (лицу) в организации, ответственному за обеспечение ИБ. Изменения в архиве не допускаются. Доступ к информации архива должен быть ограничен.

8.2.6.5. В организациях БС РФ наличие банковской информации на ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, определяется бизнес-целями организации. При этом необходимо учитывать высокую вероятность несанкционированного доступа, потери и искажения данной информации. Хорошей практикой является практика, когда ЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, не содержат никакой банковской информации (в т.ч. открытой).

8.2.6.6. При взаимодействии с сетью Интернет должно обеспечиваться противодействие атакам хакеров и распространению спама[1].

8.2.6.7. Порядок подключения и использования ресурсов сети Интернет в организации БС РФ должен контролироваться подразделениями (лицами) в организации, ответственными за обеспечение ИБ. Любое подключение и использование сети Интернет должно быть санкционировано руководством функционального подразделения организации.

---

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

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

8.2.7.1. Средства криптографической защиты информации:

— 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 реализованы на основе алгоритмов, соответствующих национальным стандартам РФ, условиям договора с контрагентом и(или) стандартам организации;
— должны иметь строгий регламент использования ключей, предполагающий контроль со стороны администратора ИБ организации за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);
— должны обеспечивать реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей или при переходе АБС в нештатный режим работы;
— не должны содержать требований к ЭВМ по специальной проверке на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;
— не должны требовать дополнительной защиты от утечки по побочным каналам электромагнитного излучения.

8.2.7.2. При применении СКЗИ в АБС должны поддерживаться непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для всех звеньев АБС.

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

8.2.7.4. Для повышения уровня безопасности при эксплуатации СКЗИ и их ключевых систем в АБС хорошей практикой является реализация процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена электронными сообщениями, и все инциденты ИБ.

8.2.7.5. Внутренний порядок применения СКЗИ в АБС определяется руководством организации и должен включать:

— порядок ввода в действие;
— 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.

8.2.7.6. Ключи кодов аутентификации (КА) и/или электронной цифровой подписи (ЭЦП) должны изготавливаться в каждой организации самостоятельно. В случае изготовления ключей КА, ЭЦП для одной организации в другой организации БС РФ согласие первой организации считать данный ключ своим должно быть зафиксировано в договоре.

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

8.2.8.1. Система обеспечения информационной безопасности банковского платежного технологического процесса должна соответствовать требованиям пунктов 8.2.2—8.2.7 настоящего стандарта и иных нормативных документов по вопросам информационной безопасности, действие которых распространяется на банковскую систему Российской Федерации.

8.2.8.2. В качестве объектов защиты должны рассматриваться:

— банковский платежный технологический процесс;
— платежная информация (примечание к п. 3.8 настоящего стандарта);
— технологический процесс по управлению ролями и полномочиями сотрудников организации БС РФ, задействованных в обеспечении банковского платежного технологического процесса.

8.2.8.3. Банковский платежный технологический процесс должен быть однозначно определен (отражен) в нормативно-методических документах организации БС РФ.

8.2.8.4. Порядок обмена платежной информацией должен быть зафиксирован в договорах между участниками, осуществляющими обмен платежной информацией. В роли участников могут выступать организации БС РФ, юридические и физические лица.

8.2.8.5. Сотрудники организации БС РФ, в том числе администраторы автоматизированных систем и средств защиты информации, не должны обладать всей полнотой полномочий для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, а также проведения операций по изменению состояния банковских счетов.

8.2.8.6. Результаты технологических операций по обработке платежной информации должны быть контролируемы (проверены) и удостоверены лицами/автоматизированными процессами. Лица/автоматизированные процессы, осуществляющие обработку платежной информации и контроль (проверку) результатов обработки, должны быть независимы друг от друга.

8.2.8.7. При работе с платежной информацией необходимо проводить авторизацию и контроль целостности данной информации.

Лучшей практикой при автоматизированной обработке платежной информации является оснащение средств вычислительной техники (на которых осуществляются операции над платежной информацией) сертифицированными или разрешенными руководителем организации БС РФ к применению средствами защиты от НСД и средствами криптографической защиты информации.

8.2.8.8. Подготовленная клиентами организации БС РФ платежная информация, на основании которой совершаются расчетные, учетные и кассовые операции, предназначена для внутреннего использования в организации БС РФ и может быть передана иным организациям только в соответствии с действующим законодательством Российской Федерации.

Указанная информация относится к категории строгой отчетности. Ограничительные пометки (грифы) “Для служебного пользования”, “Конфиденциально” или “Банковская тайна” на документы, содержащие данную информацию, не проставляются.

Безопасность информации, отнесенной к банковской тайне, обеспечивается в соответствии со статьей 26 Федерального закона “О банках и банковской деятельности”.

8.2.8.9. Обязанности по администрированию средств защиты платежной информации для каждого технологического участка ее прохождения возлагаются приказом по организации БС РФ на сотрудников (сотрудника), задействованных на данном технологическом участке (администраторов информационной безопасности), с отражением этих функций в его должностных обязанностях.

Администратор информационной безопасности должен действовать на основании соответствующего нормативного документа, разработанного в организации БС РФ и утвержденного руководством организации БС РФ.

Хорошей практикой является назначение денежной надбавки администратору информационной безопасности к его должностному окладу.

8.2.8.10. Комплекс мер по обеспечению информационной безопасности банковского платежного технологического процесса должен предусматривать:

- защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации платежных документов;
- минимально необходимый, гарантированный доступ сотрудника организации БС РФ только к тем ресурсам банковского платежного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки платежной информации;
- контроль (мониторинг) исполнения установленной технологии подготовки, обработки, передачи и хранения платежной информации;
- аутентификацию обрабатываемой платежной информации;
- двустороннюю аутентификацию автоматизированных рабочих мест, участников обмена платежной информацией;
- восстановление платежной информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
- авторизованный ввод платежной информации в автоматизированные банковские системы двумя сотрудниками с последующей программной сверкой результатов ввода на совпадение (Dual Control, ISO TR 13569);
- сверку выходных платежных сообщений с соответствующими поступившими платежными сообщениями;
- гарантированную доставку платежных сообщений участникам обмена.

8.2.8.11. Организации БС РФ — члены международных платежных систем с использованием банковских карт должны обеспечивать выполнение требований данных систем по информационной безопасности.

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

8.2.9.1. Система обеспечения информационной безопасности банковского информационного технологического процесса должна соответствовать требованиям пунктов 8.2.2—8.2.7 настоящего стандарта и иных нормативных документов по вопросам информационной безопасности, действие которых распространяется на БС РФ.

8.2.9.2. В организации БС РФ неплатежная информация классифицируется как:

- открытая информация, предназначенная для официальной передачи во внешние организации и средства массовой информации;
- внутренняя банковская информация, предназначенная для использования исключительно сотрудниками организации БС РФ при выполнении ими своих служебных обязанностей;
- информация, содержащая сведения ограниченного распространения в соответствии с утвержденным организацией БС РФ Перечнем, подлежащая защите в соответствии с законодательством РФ, например, банковская тайна, персональные данные;
- информация, полученная из федеральных органов исполнительной власти и содержащая сведения ограниченного распространения;
- информация, содержащая сведения, составляющие государственную тайну.

Каждому виду информации соответствует свой необходимый уровень защиты (свой набор требований по защите).

Так как требования по защите двух последних видов информации определяются государственными нормативно-методическими документами, то вопросы обеспечения защиты информации, содержащей указанные сведения, в настоящем стандарте не рассматриваются. Автоматизированные системы организации БС РФ, обрабатывающие, хранящие и/или передающие такую информацию, должны быть физически изолированы от прочих автоматизированных систем данной организации.

8.2.9.3. В качестве объектов защиты должны рассматриваться:

- информационные ресурсы;
- управляющая информация АБС;
- банковский информационный технологический процесс.

8.2.9.4. Организация БС РФ несет ответственность за:

- достоверность информации, официально предоставляемой внешним организациям и гражданам;
- достоверность и выполнение регламента предоставления внешним организациям и гражданам информации, обязательность и порядок предоставления которой определены законодательством Российской Федерации и/или нормативными документами Банка России;
- обеспечение соответствующего законодательству Российской Федерации уровня защиты как собственной информации, так и информации, официально полученной из внешних организаций и от граждан.

8.2.9.5. Если в АБС обрабатывается информация, требующая по решению руководства защиты, то соответствующим распоряжением должен быть назначен администратор информационной безопасности. Допускается назначение одного администратора информационной безопасности на несколько АБС, а также совмещение выполнения указанных функций с другими обязанностями.

При этом совмещение в одном лице функций администратора АБС и администратора информационной безопасности АБС не допускается.

8.2.9.6. Администратор АБС не должен иметь служебных полномочий (а при возможности и технических средств) по настройке параметров системы, влияющих на полномочия пользователей по доступу к информации. Однако он должен иметь право добавить в систему нового пользователя без всяких полномочий по доступу к информации, а также удалить из системы такого пользователя.

Администратор информационной безопасности АБС должен иметь служебные полномочия и технические возможности по контролю действий соответствующих администраторов АБС (без вмешательства в их действия) и пользователей, а также полномочия (а при возможности и технические средства) по настройке для каждого пользователя только тех параметров системы, которые определяют права доступа к информации. Устанавливаемые права доступа к информации должны назначаться подразделением организации БС РФ, ответственным за эту информацию (владельцем информационного актива).

Администратор информационной безопасности не должен иметь права добавить нового пользователя в АБС, а также удалить из нее существующего пользователя.

В случае отсутствия у администратора информационной безопасности технических возможностей по настройке параметров АБС, влияющих на полномочия пользователей по доступу к информации, эти настройки выполняются администратором АБС, но с обязательным предварительным согласованием устанавливаемых прав доступа пользователей к информации с администратором информационной безопасности.

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

8.2.9.7. Процессы подготовки, ввода, обработки и хранения информации, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств должны быть регламентированы и обеспечены инструктивными и методическими материалами, согласованными со службой информационной безопасности.

8.2.9.8. Должна осуществляться и быть регламентирована процедура периодического тестирования всех реализованных программно-техническими средствами функций (требований) по обеспечению ИБ. Регламентирующие документы должны быть согласованы со службой информационной безопасности.

8.2.9.9. Должна осуществляться и быть регламентирована процедура восстановления системы обеспечения ИБ.

9. Управление информационной безопасностью организации БС РФ

9.1. Управление ИБ организации БС РФ включает в себя:

- разработку политики информационной безопасности;
- разработку технических, организационных и административных планов обеспечения реализации политики информационной безопасности;
- разработку нормативно-методических документов обеспечения ИБ;
- создание административного и кадрового обеспечения комплекса средств управления ИБ организации;
- обеспечение штатного функционирования комплекса средств ИБ организации;
- осуществление контроля (мониторинга) функционирования системы управления ИБ организации;
- обучение с целью поддержки (повышения) квалификации персонала организации;
- оценку рисков, связанных с нарушениями ИБ.

9.2. Для реализации этих задач рекомендуется иметь в составе организации (самостоятельную или в составе службы безопасности) службу (уполномоченное лицо) по информационной безопасности. Службу (уполномоченное лицо) по информационной безопасности рекомендуется наделить следующими полномочиями:

- управлять всеми планами по обеспечению ИБ организации;
- разрабатывать и вносить предложения по изменению политики ИБ организации;
- изменять существующие и принимать новые нормативно-методические документы по обеспечению ИБ организации;
- выбирать средства управления и обеспечения ИБ организации;
- контролировать пользователей, в первую очередь пользователей, имеющих максимальные полномочия;
- контролировать активность, связанную с доступом и использованием средств антивирусной защиты, а также с применением других средств обеспечения ИБ;
- осуществлять мониторинг событий, связанных с ИБ;
- расследовать события, связанные с нарушениями ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших противоправные действия, например, нарушивших требования инструкций, руководств и т.п. по обеспечению ИБ организации;
- участвовать в действиях по восстановлению работоспособности АБС после сбоев и аварий;
- создавать, поддерживать и совершенствовать систему управления ИБ организации.

Хорошей практикой является создание службы ИБ и выделение ей своего собственного бюджета.

Хорошей практикой является, когда служба ИБ организации имеет собственного куратора на уровне первого лица в руководстве организации БС РФ (или заместителя председателя правления и т.п.). При этом служба ИБ и служба информатизации (автоматизации) не должны иметь общего куратора.

9.3. Система управления ИБ реализуется службой ИБ в виде совокупности взаимозависимых и постоянно действующих процессов (контроля, мониторинга, анализа и т.д.) штатного функционирования используемых защитных мер и должного исполнения персоналом предъявляемых к ним требований ИБ.

9.4. Для успешного функционирования системы управления ИБ и поддержки действующих в ней процессов стандарт BS 7799-2 рекомендует выделять четыре основных процесса: *планирование процессов выполнения требований ИБ; реализация и эксплуатация защитных мер; проверка процессов выполнения требований ИБ и защитных мер; совершенствование процессов выполнения требований ИБ и защитных мер.* Их выполнение должно быть реализовано в виде непрерывного цикла — "планирование — реализация — проверка — совершенствование — планирование — ...".

9.5. *Планирование процессов выполнения требований ИБ* должно включать в себя определение целей и политики ИБ, требований ИБ и процессов их реализации. К *планированию* следует относить процессы формирования политики ИБ, формирования требований ИБ, оценки рисков, выбора защитных мер. Процессы выполнения требований ИБ должны быть спланированы так, чтобы они позволили выбрать защитные меры, обеспечивающие достижение результатов в соответствии с установленными целями и политиками ИБ[1].

9.6. *Реализация и эксплуатация защитных мер* должна включать в себя внедрение выбранных защитных мер (организационных мер, технических средств обеспечения ИБ и пр.) с помощью процессов оптимального размещения и тестирования на их соответствие установленным требованиям ИБ.

9.7. *Проверка процессов выполнения требований ИБ и защитных мер* должна включать в себя проверку и оценку соответствия процессов выполнения требований ИБ установленным требованиям ИБ, а также проверку и оценку соответствия ИБ организации требованиям настоящего стандарта. Проверка и оценка должны производиться с помощью процессов аудита ИБ, мониторинга ИБ.

9.8. *Совершенствование процессов выполнения требований ИБ и защитных мер* должно включать в себя корректирующие и превентивные действия в отношении процессов выполнения требований ИБ и защитных мер по результатам оценки соответствия реализации процессов ИБ в организации и изменений в среде организации. Корректирующие действия должны включать определение причин несоответствия или характера изменений в среде организации, корректировки процессов выполнения требований ИБ и защитных мер. Превентивные действия должны включать процессы определения потенциальных причин несоответствия, а также реализацию превентивных изменений.

9.9. Качество функционирования системы управления ИБ следует оценивать по полноте, адекватности и уровню зрелости поддерживаемых ею процессов.

9.10. Организационная основа управления ИБ в организациях должна определяться целями бизнеса организации на финансовом рынке, размерами организации, наличием сети филиалов и другими факторами.

Для организаций, имеющих сеть филиалов или региональных представительств, рекомендуется выделить соответствующие подразделения ИБ на местах, обеспечив их необходимыми ресурсами и нормативной базой.

10. Модель зрелости процессов управления информационной безопасностью организаций БС РФ

10.1. Модель зрелости является мерой проработанности процессов управления ИБ, применяемых в рамках организации.

10.2. Уровень проработанности процессов управления ИБ определяется тем, насколько полно и последовательно менеджмент банка руководствуется принципами ИБ, реализует политики и требования ИБ, использует накопленный опыт и совершенствует систему управления ИБ.

10.3. Модель зрелости предназначена для определения:

- текущего статуса организации;
- положения (рейтинга) данной организации в рамках БС РФ;
- направлений дальнейшего развития с учетом рекомендаций международных стандартов;
- перспективных целей организации в части совершенствования ИБ.

10.4. Модель зрелости процессов управления ИБ организации в настоящем стандарте основывается на модели зрелости, определенной стандартом COBIT, которая определяет шесть уровней зрелости организации — с нулевого по пятый.

Нулевой уровень характеризует полное отсутствие каких-либо процессов управления ИБ в рамках деятельности организации. Организация не осознает существования проблем ИБ.

---

[1] Для соответствующих областей ИБ (организационных, административных, технических и т.д.) защитные меры могут быть выбраны на основе рекомендаций, изложенных в стандартах ISO/IEC IS 17799, ГОСТ Р ИСО/МЭК 15408, руководстве ISO TR 13569 и др.

Первый уровень (“начальный”) характеризует наличие документально зафиксированных свидетельств осознания организацией существования проблем обеспечения ИБ. Однако используемые процессы управления ИБ не стандартизованы, применяются эпизодически и бессистемно. Общий подход к управлению ИБ не выработан.

Второй уровень (“повторяемый”) характеризует проработанность процессов управления ИБ до уровня, когда их выполнение обеспечивается различными людьми, решающими одну и ту же задачу. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а ответственность возложена на исполнителя. Руководство организации в значительной степени полагается на знания исполнителей, что влечет за собой высокую вероятность возможных ошибок.

Третий уровень (“определенный”) характеризует то, что процессы стандартизованы, документированы и доведены до персонала посредством обучения. Однако порядок использования данных процессов оставлен на усмотрение самого персонала. Это определяет вероятность отклонений от стандартных процедур, которые могут быть не выявлены. Применяемые процедуры не оптимальны и недостаточно современны, но являются отражением практики, используемой в организации.

Четвертый уровень (“управляемый”) характеризует то, что обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов управления ИБ обеспечивается их оптимизация. Процессы управления ИБ находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации управления ИБ используются частично и в ограниченном объеме.

Пятый уровень (“оптимизированный”) характеризует проработанность процессов управления ИБ до уровня лучшей практики, основанной на результатах непрерывного совершенствования и сравнения уровня зрелости относительно других организаций. Защитные меры в организации используются комплексно, обеспечивая основу совершенствования процессов управления ИБ. Организация способна к быстрой адаптации при изменениях в окружении и бизнесе.

10.5. Модель зрелости управления ИБ организации ориентирована на оценку процессов управления ИБ, указанных в разделе 9 настоящего стандарта, и оценку выполнения базовых требований ИБ в организации.

10.6. Рекомендуемыми уровнями зрелости процессов управления ИБ для организаций, способными обеспечить качественное предоставление основного набора банковских услуг, являются уровни не ниже четвертого.

10.7. С учетом состава процессов управления ИБ четвертый уровень зрелости характеризуется следующими основными показателями:

- разработана нормативная и распорядительная документация по ИБ (политика ИБ, должностные инструкции для персонала и т.п.);
- создана организационная структура управления ИБ. Четко определена ответственность персонала за деятельность, связанную с обеспечением ИБ;
- финансирование ИБ осуществляется по отдельной статье бюджета организации;
- есть назначенный куратор службы ИБ;
- осуществляется приобретение необходимых средств обеспечения ИБ;
- защитные меры (технические, технологические, организационные) встроены в АБС и банковские технологические процессы. В процессе внедрения защитных мер используется анализ затрат и результатов;
- последовательно выполняется анализ ИБ организации и рисков нарушения ИБ, а также возможных негативных воздействий;
- краткие занятия с работниками организации по вопросам обеспечения ИБ носят обязательный характер;
- введена аттестация персонала по вопросам обеспечения безопасности;
- проверки на возможность вторжения в АБС являются стандартизованным и формализованным процессом;
- осуществляется оценка соответствия организации требованиям ИБ;
- стандартизованы идентификация, аутентификация и авторизация пользователей. Защитные меры совершенствуются с учетом накопленного в организации практического опыта;
- уровень стандартизации и документирования процессов управления ИБ позволяет проводить аудит ИБ в достаточном объеме;
- процессы обеспечения ИБ координируются со службой безопасности всей организации;
- деятельность по обеспечению ИБ увязана с целями бизнеса;
- руководство организации понимает проблемы ИБ и участвует в их решении через назначенного куратора службы ИБ из состава высшего руководства организации.

10.8. Уровень зрелости следует оценивать для каждого из реализуемых в организации процессов управления ИБ, состав которых определяется целями организации, ее организационной структурой и т.д.

10.9. По результатам оценки зрелости каждого из процессов управления ИБ должен формироваться общий итоговый рейтинг зрелости организации.

Учет вклада уровня зрелости процессов в общий рейтинг зрелости организации следует осуществлять в соответствии с рейтингом процесса в обеспечении достижения целей управления ИБ.

Низкий уровень зрелости одного процесса управления ИБ может негативно повлиять на общий рейтинг зрелости организации. Например, если уровень зрелости процесса контроля (мониторинга или аудита) системы управления ИБ организации оценивается как низкий — нулевой, первый или второй, то общий рейтинг зрелости организации не может превышать уровень зрелости данного процесса.

11. Аудит и мониторинг информационной безопасности организаций БС РФ

11.1. Аудит ИБ организаций БС РФ может быть внутренним или внешним. Порядок и периодичность проведения внутреннего аудита ИБ организации в целом (или ее отдельных структурных подразделений) или АБС определяется руководством организации на основе потребностей в такой деятельности. Внешний аудит ИБ проводится независимыми аудиторами.

11.2. Цель аудита ИБ организации состоит в проверке и оценке ее соответствия требованиям настоящего стандарта и других принятых в организации нормативных актов по ИБ. Аудит ИБ должен проводиться периодически. Внешний аудит ИБ организаций БС РФ должен проводиться не реже одного раза в год.

11.3. При проведении аудита ИБ организации должны использоваться стандартные процедуры документальной проверки, опрос и интервью с руководством и персоналом организации. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего аудита ИБ в качестве дополнительного способа может применяться “проверка на месте”, которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования. Обстоятельства, при которых требуется дополнительный способ в рамках внутреннего аудита ИБ, должны быть определены и согласованы в плане проведения аудита ИБ в организации.

11.4. При проведении внутреннего аудита ИБ могут использоваться журналы регистрации инцидентов ИБ, ведущиеся службами безопасности организации и формируемые на основе данных мониторинга ИБ.

11.5. Мониторинг ИБ должен проводиться персоналом организации, ответственным за ИБ, с целью обнаружения и регистрации отклонений защитных мер от требований ИБ и оценки полноты реализации положений политики ИБ, инструкций и руководств обеспечения ИБ в организации.

Основными целями мониторинга ИБ в организации являются оперативное и постоянное наблюдение, сбор, анализ и обработка данных под заданные цели, определяемые системой управления ИБ в организации. Такими целями анализа могут быть:

— контроль за реализацией положений нормативных актов по обеспечению ИБ в организации;
— выявление нештатных (или злоумышленных) действий в АБС организации;
— выявление потенциальных нарушений ИБ.

Для целей оперативного и постоянного наблюдения объектов мониторинга могут использоваться как специализированные (например, программные) средства, так и штатные (входящие в коммерческие продукты и системы) средства регистрации действий пользователей, процессов и т.п.

11.6. При проведении внешнего аудита ИБ руководство организации должно обеспечить документальное и, если это необходимо, техническое подтверждение того, что:

— политика ИБ отражает требования бизнеса и цели организации;
— организационная структура управления ИБ создана;
— процессы выполнения требований ИБ исполняются и удовлетворяют поставленным целям;
— защитные меры (например, межсетевые экраны, средства управления физическим доступом) настроены и используются правильно;
— остаточные риски оценены и остаются приемлемыми для организации;
— система управления ИБ соответствует определенному уровню зрелости управления ИБ;
— рекомендации предшествующих аудитов ИБ реализованы.

11.7. Аудиторский отчет должен храниться в организации в течение установленного времени. Доступ к аудиторскому отчету должен быть разрешен только руководству организации и руководителям подразделения (лицам), ответственным за ИБ в организации.

12. Направления развития стандарта

Реализация положений настоящего стандарта обеспечивается соответствующими руководствами, методическими указаниями и системой оценки ИБ в организациях БС РФ.

Положения настоящего стандарта могут уточняться и расширяться по предложениям, поступившим от организаций — разработчиков данного стандарта или иных организаций, использующих стандарт в практической деятельности. Данные предложения должны быть одобрены Банком России и могут быть включены в стандарт в соответствии с регламентом деятельности Технического комитета по стандартизации 362 Федерального агентства по техническому регулированию и метрологии.

БИБЛИОГРАФИЯ

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

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

Приложение А

Терминосистемы, используемые в стандарте (справочное)

А.1. Информационная безопасность организации банковской системы

А.1.1. **Информационная безопасность организации банковской системы Российской Федерации:** Состояние защищенности интересов (целей) организации БС РФ в условиях угроз в информационной сфере.

Примечания.

1. Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

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.

А.1.2. **Организация:** Юридическое лицо, которое имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде.

[ГОСТ Р 40.002-2000, статья 3.6]

А.1.3. **Банковская система Российской Федерации:** Банк России и кредитные организации, а также филиалы и представительства иностранных банков.

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

А.1.4. **Безопасность:** Отсутствие недопустимого риска.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.1]

А.1.5. **Безопасность Российской Федерации:** Состояние защищенности жизненно важных интересов личности, общества и государства.

[Закон Российской Федерации “О безопасности”]

А.1.6. **Безопасность информации:** Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз.

[Гостехкомиссия России. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения, статья 21]

А.1.7. **Информационная безопасность Российской Федерации:** Состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

[Доктрина информационной безопасности Российской Федерации от 09.09.2000]

А.1.8. **Информация:** Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

[ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию, пункт 2.1]

А.1.9. **Риск:** Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.2]

А.1.10. **Допустимый риск:** Риск, который в данной ситуации считается приемлемым для руководства.

А.1.11. **Вероятность:** Мера того, что событие может произойти.

Примечание.

ГОСТ Р 50799.10 дает математическое определение вероятности: “действительное число в интервале от 0 до 1, относящееся к случайному событию”. Число может отражать относительную частоту в серии наблюдений или степень уверенности в том, что некоторое событие произойдет. Для высокой степени уверенности вероятность близка к единице.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3]

А.1.12. **Ущерб:** Физическое повреждение или другой вред здоровью людей, имуществу (активам) или окружающей среде.

А.1.13. **Управление информационной безопасностью организации банковской системы Российской Федерации:** Совокупность целенаправленных действий, осуществляемых для достижения заявленных целей организации БС РФ в условиях угроз в информационной сфере.

Примечание.

Совокупность действий включает оценку ситуации и состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер (средств управления информационной безопасностью).

А.1.14. **Оценка соответствия информационной безопасности организации банковской системы Российской Федерации установленным требованиям:** Любая деятельность, связанная с прямым или косвенным определением того, что выполняются или не выполняются соответствующие требования информационной безопасности в организации БС РФ.

А.1.15. **Аудит информационной безопасности организации банковской системы Российской Федерации:** Периодический, независимый от объекта аудита и документированный процесс получения свидетельств аудита и объективной их оценки с целью определения степени выполнения в организациях БС РФ установленных требований по обеспечению информационной безопасности.

Примечания.

1. Внутренние аудиты (“аудиты первой стороной”) проводятся самой организацией или от ее имени для анализа менеджмента или других внутренних целей и могут служить основанием для самодеклараций организации о соответствии требованиям по ИБ.

2. Внешние аудиты включают “аудиты второй стороной” и “аудиты третьей стороной”. Аудиты второй стороной проводятся сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами от их имени. Аудиты третьей стороной проводятся внешними независимыми организациями.

А.1.16. **Модель зрелости процессов управления информационной безопасностью организации банковской системы Российской Федерации:** Схема для измерения проработанности процессов менеджмента информационной безопасностью организации БС РФ.

А.1.17. **Мониторинг информационной безопасности организации банковской системы Российской Федерации:** Постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности в организации БС РФ, сбор, анализ и обобщение результатов наблюдения под заданные цели.

Примечания.

1. Объектом мониторинга в зависимости от целей могут быть автоматизированная банковская система или ее часть, банковские информационные технологические процессы, информационные банковские услуги и пр.

2. Цели мониторинга информационной безопасности определяются службой безопасности организации БС РФ.

А.1.18. **Нормативный документ:** Документ, устанавливающий правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов.

Примечания.

1. Под документом следует понимать зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать.

2. Термины, обозначающие различные виды нормативных документов, определяются в дальнейшем исходя из того, что документ и его содержание рассматриваются как единое целое.

[ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения, статья 4.1]

А.1.19. **Положение (нормативного документа):** Логическая единица содержания нормативного документа, которая имеет форму требования, правила, рекомендации или комментария.

[ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения, статья 6.1]

А.1.20. **Требование:** Положение нормативного документа, содержащее критерии, которые должны быть соблюдены.

[ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения, статья 6.1.1]

А.1.21. **Правило:** Положение нормативного документа, описывающее действие, которое должно быть выполнено.

[ГОСТ 1.1-2002 Межгосударственная система стандартизации. Термины и определения, статья 6.1.2]

А.1.22. **Политика информационной безопасности организации:** Одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

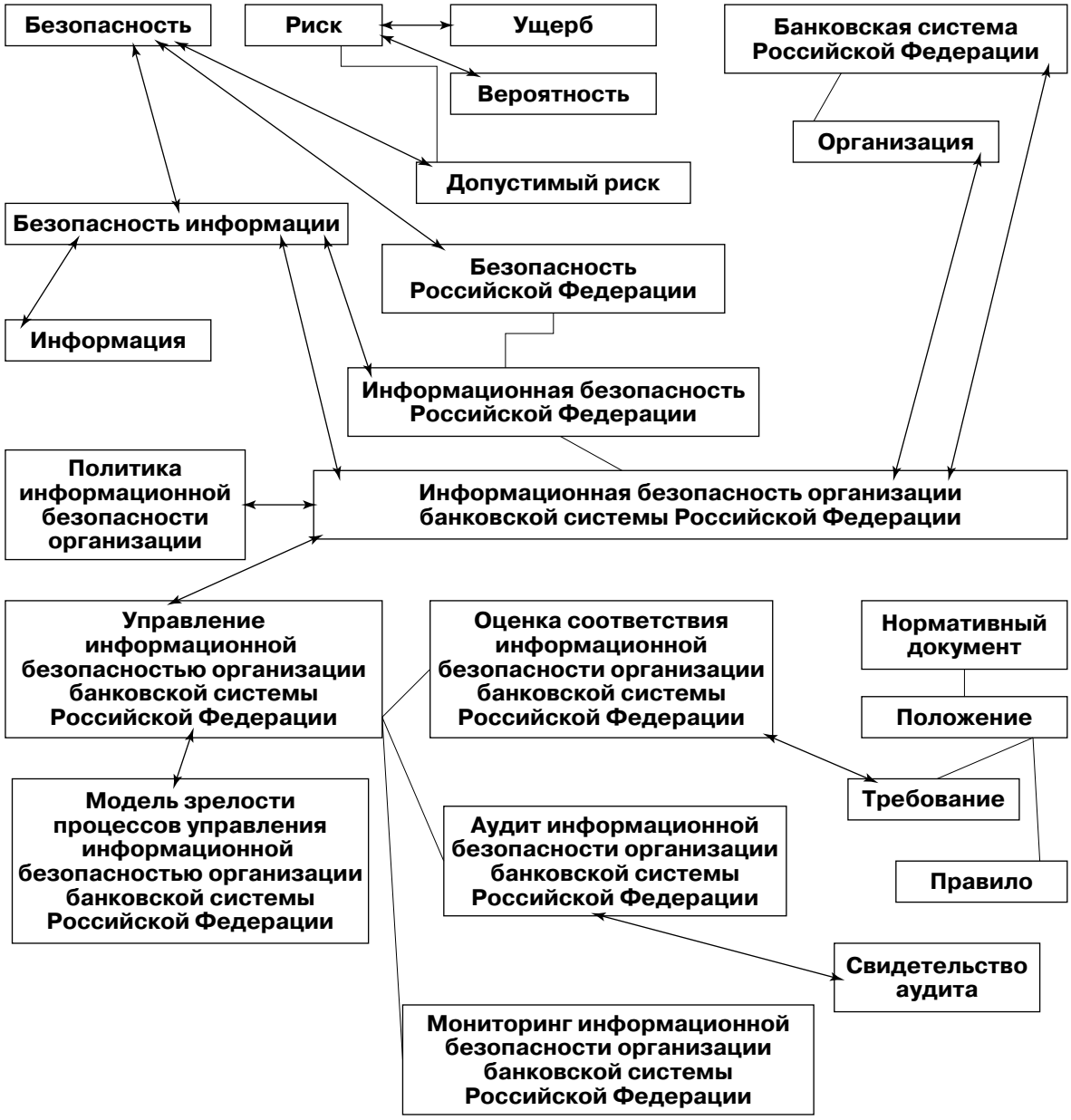
А.1.23. **Свидетельство аудита:** Записи, изложение фактов или другой информации, связанной с критериями аудита, которые могут быть перепроверены.

Примечание.

Свидетельство аудита может быть качественным или количественным.

Связи между понятиями данной группы графически представлены на рисунке А.1. Изображения связей заимствованы из ГОСТ Р ИСО/МЭК 9000-2001 “Системы менеджмента качества. Основные положения и словарь”. На рисунке линиями (веерными или в виде дерева) без стрелок показаны родовидовые связи, когда субординатные понятия в рамках иерархии наследуют признаки суперординатного понятия и содержат описания тех признаков, которые отличают их от суперординатных (вышестоящих) и координатных (соподчиненных) понятий. В виде грабель показаны партитивные отношения между понятиями, когда субординатные понятия в рамках одной иерархической системы являются частью одного суперординатного понятия. Чертой со стрелками с каждого конца показаны ассоциативные связи, определяющие природу взаимоотношений между понятиями в рамках данной системы понятий, например, причина и следствие, действие и место, действие и результат, инструмент и функция, материал и продукция.

Рисунок А.1. Понятия, относящиеся к информационной безопасности организации БС РФ



А.2. Банковские технологии и технологические процессы

А.2.1. **Банковская технология:** Система методов, способов, приемов деятельности в банковской отрасли.

А.2.2. **Банковский технологический процесс:** Технологический процесс, содержащий операции по изменению и(или) определению состояния банковской информации, используемой при функционировании или необходимой для реализации банковских услуг, функционирования организации БС РФ.

Примечания.

1. Операции над банковской информацией могут выполняться вручную или быть автоматизированными, например, с помощью комплексов средств автоматизации автоматизированных банковских систем.

2. Операции над банковской информацией требуют указания ролей их участников (исполнителей и лиц, принимающих решения или имеющих полномочия по изменению технологических процессов, в том числе персонала автоматизированных банковских систем).

А.2.3. **Банковский платежный технологический процесс:** Часть банковского технологического процесса, содержащая расчетные, учетные, кассовые и иные банковские операции над платежной информацией, связанные с перемещением денежных средств с одного счета на другой, открытием (закрытием) счетов или контролем за данными операциями.

Примечание.

Платежная информация может включать в себя платежные (расчетные) сообщения и информацию, связанную с проведением расчетных, учетных, кассовых и иных технологических операций.

А.2.4. **Банковский информационный технологический процесс:** Часть банковского технологического процесса, содержащая операции над неплатежной информацией, необходимой для функционирования организации БС РФ.

Примечание.

Неплатежная информация, необходимая для функционирования организации БС РФ, может включать в себя данные статистической отчетности и внутрихозяйственной деятельности, аналитическую, финансовую, справочную информацию.

А.2.5. **Автоматизированная банковская система:** Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая банковскую информационную технологию выполнения установленных функций.

А.2.6. **Банковская информационная технология:** Приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования финансовой или другой связанной с функционированием организаций БС РФ информации.

А.2.7. **Роль в организации:** Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом в организации.

Примечания.

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

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

А.2.8. **Технология:** Система взаимосвязанных методов, способов, приемов предметной деятельности.

[ГОСТ Р 52069.0-2003 Защита информации. Система стандартов. Основные положения, пункт 3.10]

А.2.9. **Банк:** Кредитная организация, которая имеет исключительное право осуществлять в совокупности следующие банковские операции: привлечение во вклады денежных средств физических и юридических лиц; размещение указанных средств от своего имени и за свой счет на условиях возвратности, платности, срочности; открытие и ведение банковских счетов физических и юридических лиц.

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

А.2.10. **Процесс:** Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

Примечания.

1. Входами к процессу обычно являются выходы других процессов.

2. Процессы в организации, как правило, планируются и осуществляются в управляемых условиях с целью добавления ценности.

3. Процесс, в котором подтверждение соответствия конечной продукции затруднено или экономически нецелесообразно, часто относят к “специальному процессу”.

[ГОСТ Р ИСО 9000-2001 Системы менеджмента качества. Основные положения и словарь, статья 3.4.1]

А.2.11. **Технологический процесс:** Процесс, содержащий целенаправленные действия по изменению и(или) определению состояния предмета труда.

Примечания.

1. Технологический процесс может быть отнесен к изделию, его составной части или к методам обработки, формообразования и сборки.

2. К предметам труда относятся заготовки и изделия.

[ГОСТ 3.1109-82 Единая система технологической документации. Термины и определения основных понятий, статья 1]

А.2.12. **Автоматизированная система:** Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Примечания.

1. В зависимости от вида деятельности выделяют, например, следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др.

2. В зависимости от вида управляемого объекта (процесса) АСУ делят, например, на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д.

[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения, статья 1.1]

А.2.13. **Информационная технология:** Приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных.

[ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения, Приложение]

А.2.14. **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.

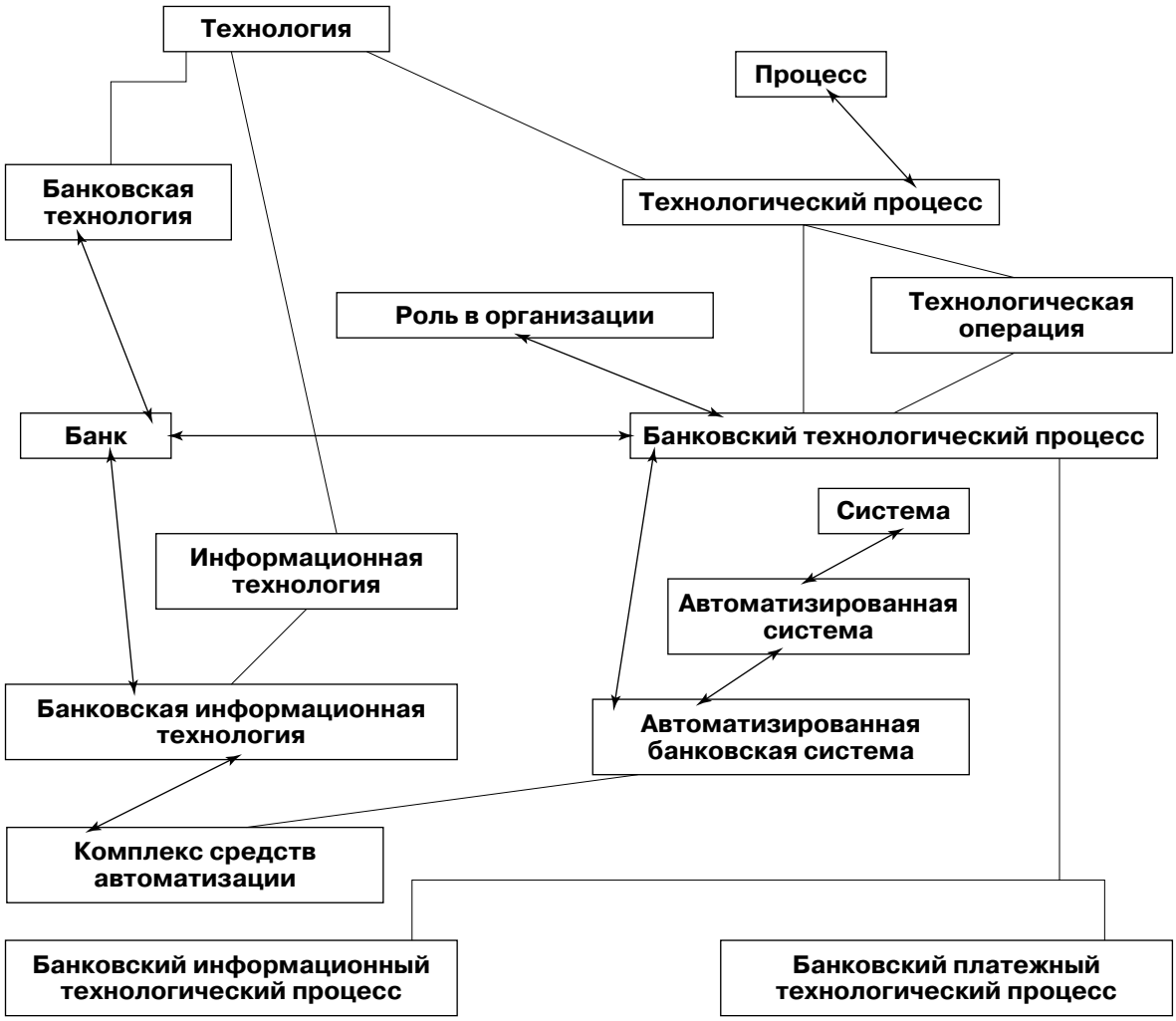
[Рекомендации по стандартизации Р 50.1.031-2001 Информационные технологии поддержки жизненного цикла продукции. Терминологический словарь. Часть 1. Стадии жизненного цикла продукции, статья 3.1.5]

А.2.15. **Комплекс средств автоматизации АС:** Совокупность всех компонентов автоматизированной системы, за исключением людей.

[ГОСТ 34.003 Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения, статья 2.12]

Связи между понятиями данной группы графически представлены на рисунке А.2.

Рисунок А.2. Понятия, относящиеся к банковским технологиям и банковским технологическим процессам



А.3. Риск и инцидент информационной безопасности организации БС РФ

А.3.1. **Риск:** Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.2]

А.3.2. **Вероятность:** Мера того, что событие может произойти.

Примечание.

ГОСТ Р 50799.10 дает математическое определение вероятности: “действительное число в интервале от 0 до 1, относящееся к случайному событию”. Число может отражать относительную частоту в серии наблюдений или степень уверенности в том, что некоторое событие произойдет. Для высокой степени уверенности вероятность близка к единице.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3]

А.3.3. **Ущерб:** Физическое повреждение или другой вред здоровью людей, имуществу или окружающей среде.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.3]

А.3.4. **Инцидент информационной безопасности:** Действительное, предпринимаемое или вероятное нарушение информационной безопасности.

Примечание.

Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности, учетности или неотказуемости.

А.3.5. **Информационная безопасность организации банковской системы Российской Федерации:** Состояние защищенности интересов (целей) организации БС РФ в информационной сфере.

Примечание.

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

А.3.6. **Риск инцидента информационной безопасности организации банковской системы Российской Федерации:** Сочетание вероятности нанесения ущерба и тяжести этого ущерба от действительного, предпринимаемого или вероятного нарушения состояния защищенности интересов (целей) организации БС РФ в информационной сфере.

А.3.7. **Нарушение информационной безопасности организации банковской системы Российской Федерации:** Событие, вызывающее ущерб состояния защищенности интересов (целей) организации БС РФ в информационной сфере.

А.3.8. **Вызывающее ущерб событие:** Событие, при котором опасная ситуация приводит к ущербу.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.4]

А.3.9. **Опасная ситуация:** Обстоятельства, в которых люди, имущество или окружающая среда подвергаются опасности.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.6]

А.3.10. **Опасность:** Потенциальный источник возникновения ущерба.

Примечание.

Термин “опасность” может быть конкретизирован в части определения природы опасности или вида ожидаемого ущерба (например, опасность электрического шока, опасность разрушения, травматическая опасность, токсическая опасность, опасность пожара, опасность утонуть).

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.5]

А.3.11. **Остаточный риск:** Риск, остающийся после предпринятых защитных мер.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.9]

А.3.12. **Защитная мера:** Мера, используемая для уменьшения риска.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.8]

А.3.13. **Анализ риска:** Систематическое использование информации для выявления опасности и количественной оценки риска.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.10]

А.3.14. **Оценивание риска:** Основанная на результатах анализа риска процедура проверки, устанавливающая, не превышен ли допустимый риск.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.11]

А.3.15. **Оценка риска:** Общий процесс анализа и оценивания риска.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.12]

А.3.16. **Допустимый риск:** Риск, который в данной ситуации считают приемлемым при существующих общественных ценностях.

[ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты, пункт 3.7]

А.3.17. **Управление риском:** Действия, осуществляемые для выполнения решений в рамках менеджмента риска.

Примечание.

Управление риском может включать в себя мониторинг, переоценивание и действия, направленные на обеспечение соответствия принятым решениям.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.2]

А.3.18. **Менеджмент риска:** Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание.

Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.1.7]

А.3.19. **Обработка риска:** Процесс выбора и осуществления мер по модификации риска.

Примечания.

1. Термин “обработка риска” иногда используют для обозначения самих мер.

2. Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.1]

А.3.20. **Принятие риска:** Решение принять риск.

Примечание.

Принятие риска зависит от критериев риска.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.10]

А.3.21. **Коммуникация риска:** Обмен информацией о риске или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами.

Примечание.

Информация может касаться существования, природы, формы, вероятности, тяжести, приемлемости, мероприятий или других аспектов риска.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.2.4]

А.3.22. **Оптимизация риска:** Процесс, связанный с риском, направленный на минимизацию негативных и максимальное использование позитивных последствий и, соответственно, их вероятности.

Примечания.

1. С точки зрения безопасности оптимизация риска направлена на снижение риска.

2. Оптимизация риска зависит от критериев риска с учетом стоимости и законодательных требований.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.3]

А.3.23. **Перенос риска:** Разделение с другой стороной бремени потерь или выгод от риска.

Примечания.

1. Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.

2. Перенос риска может быть осуществлен страхованием или другими соглашениями.

3. Перенос риска может создавать новый риск или модифицировать существующий риск.

4. Перемещение источника не является переносом риска.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.7]

А.3.24. **Сохранение риска:** Принятие бремени потерь или выгоды от конкретного риска.

Примечание.

Сохранение риска не включает в себя обработку риска в результате страхования или перенос риска другими средствами.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.9]

А.3.25. **Критерии риска:** Правила, по которым оценивают значимость риска.

Примечание.

Критерии риска могут включать в себя сопутствующие стоимость и выгоды, законодательные и обязательные требования, социально-экономические и экологические аспекты, озабоченность причастных сторон, приоритеты и другие затраты на оценку.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.1.6]

А.3.26. **Снижение риска:** Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.4.4]

А.3.27. **Причастная сторона:** Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными действию риска.

Примечания.

1. Лицо, принимающее решение, также является причастной стороной.

2. Причастная сторона включает в себя заинтересованную сторону, но имеет более широкое значение, чем заинтересованная сторона.

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.2.1]

А.3.28. **Заинтересованная сторона:** Лицо или группа лиц, заинтересованные в деятельности или успехе организации.

Примеры: потребители, владельцы, работники организации, поставщики, банкиры, ассоциации, партнеры или общество.

Примечание.

Группа лиц может состоять из организации, ее части или нескольких организаций (ГОСТ Р ИСО 9000).

[ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения, статья 3.2.2]

Связи между понятиями данной группы графически представлены на рисунке А.3.

Рисунок А.3. Понятия, относящиеся к рискам и инцидентам информационной безопасности организации БС РФ

А.4. Информационные активы организации БС РФ

А.4.1. **Информационные активы организации банковской системы Российской Федерации:** Активы организации БС РФ, представляющие ценность для нее с точки зрения достижения целей и имеющие отношение к ее информационной сфере.

А.4.2. **Активы организации банковской системы Российской Федерации:** Все, представляющее ценность для организации БС РФ с точки зрения достижения ее целей.

Примечание.

К активам организации БС РФ могут относиться:

- банковские ресурсы (финансовые, людские, вычислительные, телекоммуникационные и пр.);
- информационные активы, в т.ч. различные виды банковской информации (платежной, финансово-аналитической служебной, управляющей и пр.) на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение;
- банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы, процессы жизненного цикла автоматизированных банковских систем и др.);
- банковские продукты и услуги, предоставляемые клиентам.

А.4.3. **Активы:** Все, что имеет ценность для организации.

[ISO/IEC TR 13335-1: 1996 Information technology — Guidelines for the management of IT Security (GMITS) — Part 1: Concepts and models for IT Security, пункт 3.2]

А.4.4. **Ресурс:** Объект, который используется или использован в течение выполнения процесса.

Примечания.

1. Ресурс может включать разнообразные объекты типа персонала, средств обслуживания, капитального оборудования, инструментов и предприятий коммунального обслуживания типа электроэнергии, воды, топлива и инфраструктуры связи.

2. Ресурсы могут быть многократного использования, возобновляемые или расходуемые.

[ISO/IEC 15288 Information technology — Life Cycle Management — System Life Cycle Processes]

А.4.5. **Процесс:** Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

Примечания.

1. Входами к процессу обычно являются выходы других процессов.

2. Процессы в организации, как правило, планируются и осуществляются в управляемых условиях с целью добавления ценности.

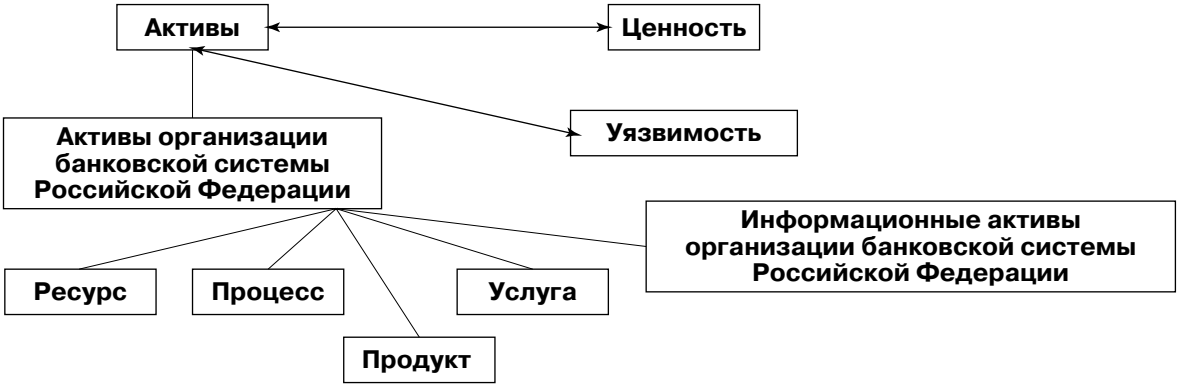
3. Процесс, в котором подтверждение соответствия конечной продукции затруднено или экономически нецелесообразно, часто относят к “специальному процессу”.

[ГОСТ Р ИСО 9000-2001, статья 3.4.1]

А.4.6. **Ценность:** Имущество, деньги, нематериальные блага, а также их свойства или отношения.

[ГОСТ Р 22.10.01-2001 Безопасность в чрезвычайных ситуациях. Оценка ущерба. Термины и определения, статья 2.1.14]

Рисунок А.4. Понятия, относящиеся к информационным активам организации БС РФ



А.4.7. **Продукт:** Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

[ГОСТ Р ИСО/МЭК 15408-2002 Критерии оценки безопасности информационных технологий, пункт 2.3]

А.4.8. **Услуга:** Действия субъектов (собственников и владельцев) по обеспечению пользователей продуктами.

Связи между понятиями данной группы графически представлены на рисунке А.4.

А.4.9. **Уязвимость:** Недостатки или слабые места активов, которые могут быть использованы угрозой.