СТАНДАРТ БАНКА РОССИИ СТО БР ИББС-1.0-2006

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ПОЛОЖЕНИЯ

Дата введения: 2006-01-01

Издание официальное

г. Москва
2006

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 26 января 2006 года № Р-27.

2. ВЗАМЕН СТО БР ИББС-1.0-2004.

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 12
6.1. Общие принципы безопасного функционирования организации 12
6.2. Специальные принципы обеспечения информационной безопасности организации 12
7. Модели угроз и нарушителей информационной безопасности организаций БС РФ 13
8. Политика информационной безопасности организаций БС РФ 14
8.1. Состав и назначение политики информационной безопасности организации БС РФ 14
8.2. Общие (основные) требования по обеспечению информационной безопасности, отображаемые в политиках информационной безопасности организации БС РФ 14
8.2.1. Общие требования по обеспечению информационной безопасности для организации БС РФ 14
8.2.2. Общие требования по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу 15
8.2.3. Общие требования по обеспечению информационной безопасности автоматизированных банковских систем на стадиях жизненного цикла 15
8.2.4. Общие требования по обеспечению информационной безопасности при управлении доступом и регистрации 17
8.2.5. Общие требования по обеспечению информационной безопасности средствами антивирусной защиты 17
8.2.6. Общие требования по обеспечению информационной безопасности при использовании ресурсов сети Интернет 18
8.2.7. Общие требования по обеспечению информационной безопасности при использовании средств криптографической защиты информации 19
8.2.8. Общие требования по обеспечению информационной безопасности банковских платежных технологических процессов 20
8.2.9. Общие требования по обеспечению информационной безопасности банковских информационных технологических процессов 21
9. Система менеджмента информационной безопасности организации БС РФ 22
9.1. Планирование СМИБ 22
9.2. Реализация и эксплуатация СМИБ 23
9.3. Проверка (мониторинг и анализ) СМИБ 23
9.4. Совершенствование СМИБ 23
9.5. Система документации 23
9.6. Обеспечение непрерыности бизнеса (деятельности) и восстановление после прерываний 24
9.7. Служба информационной безопасности (уполномоченное лицо) организации БС РФ 24
10. Проверка и оценка информационной безопасности организации БС РФ 25
11. Модель зрелости процессов менеджмента информационной безопасности организации БС РФ 26
12. Направления развития стандарта 27
Библиография 27

Введение

Банковская система (БС) Российской Федерации (РФ) включает в себя Банк России, кредитные организации, а также филиалы и представительства иностранных банков [1]. Развитие и укрепление БС РФ, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ являются целями деятельности Банка России [2]. Важнейшим условием реализации этих целей является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) организаций БС РФ, их активов (в т.ч. информационных), который во многом определяется уровнем 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. В связи с этим 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, который является базовым для развивающей и обеспечивающей его группы стандартов, в целом составляющих комплекс стандартов 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: 2006-01-01

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(или) прямого использования устанавливаемых в нем положений во внутренних нормативных и методических документах организаций БС РФ, а также в договорах.

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

Настоящий стандарт может быть введен в действие организаций БС РФ в качестве обязательного к исполнению в случае, если такая необходимость существует.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 1.0-2004 Стандартизация в Российской Федерации. Основные положения

ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. Стандарты организаций. Общие положения

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

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

ГОСТ Р ИСО 9001-2001 Система менеджмента качества. Требования

ГОСТ Р ИСО 14001-98 Система управления окружающей средой. Требования и руководство по применению

ГОСТ Р ИСО/МЭК 15408-1÷3-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий

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 13335-1÷2 Information Technology. Security techniques. Management of information and communications technology security

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

ISO/IEC IS 15288-2002 Systems engineering. System Life Cycle Processes

ISO/IEC TR 15504-1÷5 Information technology. Process assessment

ISO/IEC TR 18028-1÷5 Information technology. Security techniques. IT network security

ISO/IEC TR 18043 Information technology. Selection, deployment and operations of intrusion detection systems (IDS)

ISO/IEC TR 18044-2004 Information Technology. Security techniques. Information security incident management

ISO/IEC IS 17799-2005 (second edition) (с 2007 года — ISO/IEC IS 27002) Information Technology. Code of practice for information security management

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

ITU-T Recommendation X.1051 Information security management system. Requirements for telecommunications (ISMS-T)

BSI PAS-56 Guide to Business Continuity Management (BCM)

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

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

3.2. **активы организации банковской системы Российской Федерации:** все, что имеет ценность для организации банковской системы Российской Федерации и находится в ее распоряжении.

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. **автоматизированная банковская система:** автоматизированная система, реализующая банковский технологический процесс или его часть.

3.4. **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 руководителей организации БС РФ, ее персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами.

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

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

3.6. **информационная безопасность организации банковской системы Российской Федерации:** состояние защищенности интересов (целей) организации банковской системы Российской Федерации 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.

3.7. **менеджмент:** скоординированная деятельность по руководству и управлению.

Примечание.

В английском языке термин “management” иногда относится к людям, т.е. к лицу или группе работников, наделенных полномочиями и ответственностью для руководства и управления организацией. Когда “management” используется в этом смысле, его следует всегда применять с определяющими словами с целью избежания путаницы с понятием “management”, определенным выше. Например, не одобряется выражение “руководство должно…”, в то время как “высшее руководство должно…” — приемлемо.

3.8. **система менеджмента информационной безопасности организации банковской системы Российской Федерации;** СМИБ: часть общей системы менеджмента организации банковской системы Российской Федерации, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности организации банковской системы Российской Федерации [ISO/IEC IS 27001].

Примечание.

Система менеджмента включает структуру, политики, деятельности по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

3.9. **осознание информационной безопасности:** понимание организацией необходимости самостоятельно на основе принятых в ней ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по обеспечению информационной безопасности, а также поддерживать эту деятельность адекватно прогнозу.

Примечание.

Осознание информационной безопасности является внутренним побудительным мотивом организации инициировать и поддерживать деятельность по менеджменту информационной безопасности, в отличие от побуждения или принуждения, когда решение об инициировании и поддержке деятельности по менеджменту информационной безопасности определяется соответственно либо возникшими проблемами организации, такими, как инцидент информационной безопасности, либо внешними факторами, например, требованиями законов.

3.10. **политика информационной безопасности организации банковской системы Российской Федерации:** одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется организация банковской системы Российской Федерации в своей деятельности.

3.11. **инцидент информационной безопасности организации банковской системы Российской Федерации:** событие, вызывающее действительное, предпринимаемое или вероятное нарушение информационной безопасности организации банковской системы Российской Федерации.

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.

3.12. **риск:** неопределенность, предполагающая возможность потерь (ущерба).

3.13. **менеджмент риска:** скоординированные действия по руководству и управлению в отношении риска с целью его минимизации.

Примечание.

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

3.14. **риск нарушения информационной безопасности организации банковской системы Российской Федерации:** неопределенность, предполагающая возможность ущерба состояния защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз в информационной сфере.

3.15. **мониторинг информационной безопасности организации банковской системы Российской Федерации (мониторинг ИБ):** постоянное наблюдение за событиями мониторинга ИБ, сбор, анализ и обобщение результатов наблюдения.

3.16. **аудит информационной безопасности организации банковской системы Российской Федерации:** периодический, независимый 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 самодекларации 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. Независимость при аудите предполагает полную свободу аудитора (самостоятельность) в отборе и анализе свидетельства аудита (изложение фактов или другой информации, связанной с критериями аудита) в отношении объекта аудита.

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 банковской системы Российской Федерации.

4. Обозначения и сокращения

АБС — автоматизированная банковская система;
БС — банковская система;
ЖЦ — жизненный цикл;
ИБ — информационная безопасность;
КА — код аутентификации;
ЛВС — локальная вычислительная сеть;
РФ — Российская Федерация;
СКЗИ — средство криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
ЭВМ — электронная вычислительная машина;
ЭЦП — электронная цифровая подпись.

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

5.1. Любая целенаправленная деятельность (бизнес) порождает риски, сущность которых — естественная неопределенность будущего. Это — объективная реальность, и понизить эти риски можно лишь до уровня неопределенности сущностей, характеризующих природу бизнеса. Оставшаяся часть риска, определяемого факторами среды деятельности организации БС РФ, на которые организация не в силах влиять, должна быть неизбежно принята. При этом степень необходимой защищенности информационной сферы организации определяется анализом и оценкой рисков ИБ, которые должны быть согласованы с рисками основной (бизнес) деятельности организации БС РФ.

5.2. Деятельность организации БС РФ осуществляется через реализацию трех групп высокоуровневых процессов: основные процессы (процессы основной деятельности), вспомогательные процессы (процессы по видам обеспечения), процессы менеджмента (управления) организацией. Процессы по обеспечению ИБ организации БС РФ составляют один из видов вспомогательных процессов, реализующих поддержку (обеспечение) процессов основной деятельности организации в целях достижения ею максимально возможного результата.

5.3. 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, может быть нанесен ущерб.

---

[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).

5.4. Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является нецелевое использование предоставленного контроля над информационными активами, а также сокрытие следов своей деятельности. Внешний злоумышленник скорее да, чем нет, может иметь сообщника(ов) внутри организации.

5.5. 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.

5.6. Злоумышленник изучает объект нападения, как правило, не только теоретически, никак не проявляя себя, но и практически, путем эксперимента, подбора "отмычек" к системе менеджмента ИБ (СМИБ) 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 ИБ (подразделения (лица) в организации, ответственные за обеспечение ИБ).

5.7. Сложно и ресурсоемко, а значит, малоэффективно искать следы такой активности и по факту настраивать СМИБ. Поэтому главный инструмент собственника — основанный на опыте прогноз (составление модели угроз и модели нарушителя)[1], а также работа с персоналом организации по повышению его бдительности в возможных критических условиях, готовности и способности к адекватным действиям в условиях потенциальной злоумышленной активности.

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

5.8. Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ для собственника — разработать на основе точного прогноза, базирующегося в том числе и на анализе и оценке рисков ИБ, политику ИБ организации и в соответствии с ней реализовать, эксплуатировать и совершенствовать СМИБ организации.

5.9. Политика ИБ организаций БС РФ разрабатывается на основе принципов обеспечения ИБ организаций БС РФ, моделей угроз и нарушителей, идентификации активов, подлежащих защите, оценки рисков с учетом особенностей бизнеса и технологий, а также 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).

При этом собственник принимает решение относительно принятия конкретного риска или же внедрения мер контроля и процедур по обработке существующих рисков.

При принятии решений о внедрении защитных мер (мер контроля) для противодействия идентифицированным угрозам (рискам) собственник должен учитывать, что тем самым он увеличивает сложность своей системы управления ИБ, а повышение сложности управления ИБ порождает новые уязвимости. Поэтому при выборе решения о внедрении защитных мер для обработки существующих рисков, а не принятия или переноса рисков должны учитываться вопросы эксплуатации защитных мер и их влияния на структуру рисков организации.

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.

При разработке моделей угроз и моделей нарушителя необходимо учитывать, что по сложившейся уже практике существующая сложность современных банковских технологий приводит к их меньшей привлекательности для злоумышленника, чем персонал и система управления безопасностью организации. Поэтому все точки в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации, должны тщательно контролироваться.

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

---

[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.

5.12. 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 нарушения ИБ.

Для того чтобы этого не допустить, необходимо определить процессы, обеспечивающие контроль (мониторинг и аудит ИБ организаций БС РФ), а также оценку эффективности СМИБ организаций БС РФ (так называемый "процессный подход"), что должно стать основой для дальнейшего планирования ИБ. Указанные процессы должны реализовываться в рамках циклической модели менеджмента ИБ: "планирование — реализация — проверка — совершенствование — планирование — ...", отвечающей принципам и моделям корпоративного менеджмента в организациях [3], включая менеджмент в банковском деле [4, 5].

При этом эффективность и результативность обеспечения ИБ, включая соответствующие процессы ИБ, должны оцениваться с позиции содействия (пользы) в достижении целей деятельности организации.

5.13. Обеспечение ИБ организаций БС РФ основывается на "процессном подходе" для установления, реализации, эксплуатации, мониторинга, обслуживания и повышения эффективности СМИБ.

Любое действие, использующее ресурсы и управляемое для обеспечения преобразования неких входных ресурсов, информации и иных сущностей в выходы, определяется как "процесс". Выход одного процесса может быть входом для другого процесса. Представление деятельностей по обеспечению ИБ в виде системы процессов в пределах организации вместе с идентификацией, взаимодействиями и их координацией и управлением определяется как "процессный подход".

"Процессный подход" к обеспечению ИБ организаций БС РФ требует, чтобы персонал организации, клиенты, пользователи, контрагенты и иные заинтересованные стороны придавали особое значение:

а) пониманию требований информационной безопасности бизнеса и потребности устанавливать политику и цели для информационной безопасности;
б) реализации и надлежащей эксплуатации средств управления ИБ (защитных мер) в контексте управления общим риском деятельности (бизнеса) организации;
в) мониторингу и анализу работы и эффективности СМИБ;
г) непрерывному усовершенствованию СМИБ на основе объективного измерения.

5.14. Рисунок 1 иллюстрирует модель непрерывного циклического процесса менеджмента ИБ организации (модель Деминга), определенную требованиями раздела 4 международного стандарта ISO/IEC IS 27001[1].

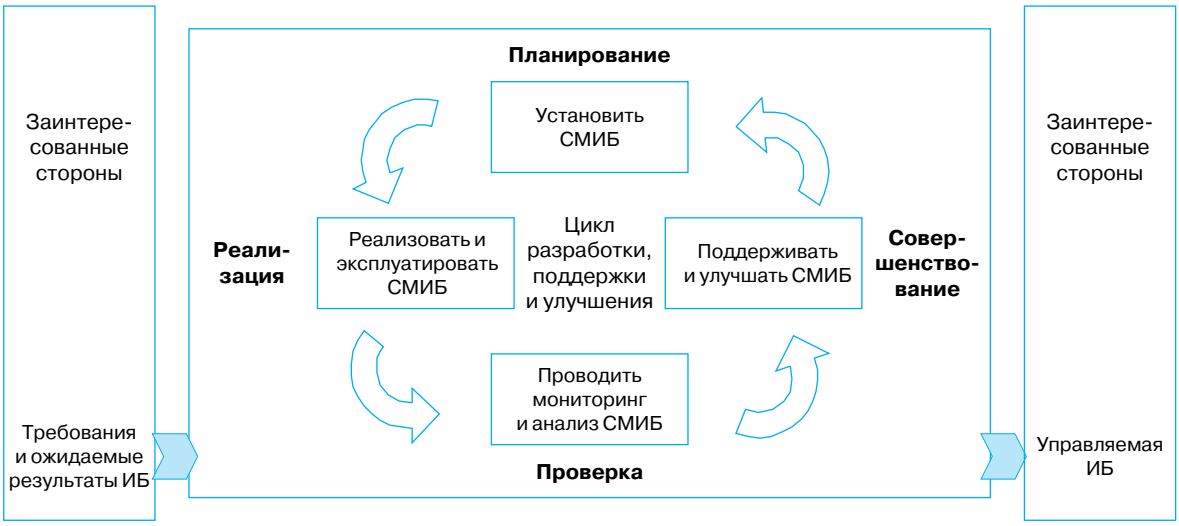

Рисунок 1. Элементы процесса менеджмента ИБ

На стадии планирования устанавливают политики информационной безопасности, цели, задачи, процессы и процедуры, адекватные потребностям в менеджменте риска ИБ и совер-

[1] Циклическая модель менеджмента Деминга, известная под названием модели "планирование – реализация – проверка – совершенствование – планирование – ..." и являющаяся основой международных стандартов менеджмента информационной безопасности (ISO/IEC IS 27001), менеджмента качества (ГОСТ Р ИСО 9001) и других стандартов, может применяться ко всем процессам СМИБ.

шенствованию СМИБ, для достижения результатов в соответствии с политиками и целями организации.

На стадии реализации осуществляются внедрение и поддержка политики информационной безопасности организации, средств управления (защитных мер), регламентов, процессов и процедур СМИБ организации.

На стадии проверки осуществляются оценка и, если необходимо, измерение эффективности процессов менеджмента ИБ организации на соответствие требованиям политики информационной безопасности, целям и установленным практикам, обеспечивается отчетность высшему руководству о результатах для проведения соответствующего анализа.

На стадии совершенствования осуществляются выработка и принятие корректирующих и превентивных действий, основанных на результатах анализа, для достижения непрерывного усовершенствования СМИБ организации.

5.15. Использование для обеспечения ИБ организаций БС РФ “процессного подхода” на базе циклической модели Деминга, который является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ГОСТ Р ИСО 14001, позволит обеспечить поддержку и интеграцию требований к различным системам менеджмента в рамках общего корпоративного менеджмента в организациях БС РФ. Требования настоящего стандарта к СМИБ для организаций БС РФ имеют прикладную практическую направленность, определяющую условия, цели и задачи применения в организациях БС РФ высокоуровневых международных стандартов для СМИБ организаций. Подобным прикладным стандартом является Рекомендация Международного союза электросвязи X.1051, обеспечивающая практическую основу по применению положений международного стандарта ISO/IEC IS 27001 в организациях, чей бизнес лежит в области телекоммуникаций.

5.16. Обеспечение ИБ организации включает реализацию и поддержку процессов осознания ИБ и процессов менеджмента ИБ.

Процессы осознания ИБ организации имеют отношение к руководству организации и определяют его ответственность в части реализации принципов обеспечения информационной безопасности организаций БС РФ, определенных положениями настоящего стандарта, а также требованиями раздела 5 “Ответственность высшего руководства организации” международного стандарта ISO/IEC IS 27001.

Процессы осознания ИБ должны охватывать всю организацию, а процессами менеджмента ИБ может быть охвачена ее часть или части. Обоснованием тому может быть ограниченность в ресурсах или времени. Необходимо стремиться к тому, чтобы процессы менеджмента ИБ организации распространялись на всю ее деятельность.

5.17. Стратегия обеспечения ИБ организаций БС РФ, таким образом, заключается в развертывании, эксплуатации и совершенствовании СМИБ организации, включающей деятельность (процессы) менеджмента ИБ и стимулируемой и управляемой процессами осознания ИБ. Деятельность (процессы) СМИБ организации должна обеспечивать достижение целей деятельности организации в условиях:

— штатного функционирования;
— возникновения локальных инцидентов и проблем ИБ;
— возникновения широкомасштабных катастроф и аварий различной природы, последствия которых имеют или могут иметь отношение к ИБ организации БС РФ.

При этом менеджмент ИБ есть часть общего корпоративного менеджмента организации БС РФ, которая ориентирована на содействие достижению целей деятельности организации через обеспечение защищенности ее информационной сферы. Менеджмент ИБ не должен рассматриваться как самостоятельный вид деятельности в организации. Осознание ИБ обеспечивает основу эффективного функционирования СМИБ организации, где под эффективностью понимается соотношение между достигнутым результатом и использованными ресурсами.

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[1], 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.

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.

---

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

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.

---

[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.

7.11. 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.

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 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 организации 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 СМИБ 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 БС РФ

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 договоры (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 17799-2005 следует включать в трудовые контракты (соглашения, договоры).

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 34.601-90 и документом ISO/IEC IS 15288-2002.

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 договоры 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];
— “необходимо знать”[3],

а также руководствоваться принципом “двойное управление”[4].

8.2.4.2. В составе АБС должны применяться встроенные механизмы защиты информации, а также могут 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.

---

[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].

[3] “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].

[4] “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].

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).

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.

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.

---

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

8.2.7.6. 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;
- 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. Допускаются 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 ИБ.

8.2.9.9. Должна осуществляться и быть регламентирована процедура восстановления всех реализованных программно-техническими средствами функций по обеспечению ИБ. Регламентирующие документы должны быть согласованы со службой ИБ.

9. Система менеджмента информационной безопасности организации БС РФ

9.1. Планирование СМИБ

Для успешного функционирования СМИБ организации БС РФ следует реализовать следующие процессы:

а) определение/уточнение области действия СМИБ и выбор подхода к оценке рисков ИБ. Определение/уточнение области действия СМИБ должно осуществляться на основе результатов оценки операционных рисков, а также оценки репутационных и правовых рисков деятельности организации БС РФ;

б) анализ и оценка рисков ИБ, варианты обработки рисков ИБ для наиболее критичных информационных активов и бизнес-процессов организации. При анализе и оценке рисков ИБ должны использоваться положения раздела 7 настоящего стандарта;

в) определение/уточнение политики для СМИБ организации;

г) выбор/уточнение целей ИБ и защитных мер и их обоснование для минимизации рисков ИБ. Цели ИБ и защитные меры могут быть выбраны на основе раздела 8 настоящего стандарта, а дополнительно на основе:

1) международного стандарта ISO/IEC IS 27001-2005 или положений международного стандарта ISO/IEC IS 17799-2005, обеспечивающего большую детализацию;

2) стандартов ISO TR 13569, COBIT, BSI PAS 56 и других руководств по обеспечению информационной безопасности;
3) ГОСТ Р ИСО/МЭК 15408-1÷3-2002 в части требований к продуктам информационных технологий;
4) стандартов ISO/IEC TR 18028, ISO/IEC TR 18043, ISO/IEC TR 18044 и других стандартов для отдельных областей обеспечения ИБ.

Обоснование по обработке рисков с учетом применения защитных мер должно быть подготовлено в виде отдельного документа (аналогичного документу "Statement of applicability" по ISO/IEC IS 27001), являющегося основой для разработки плана обработки рисков ИБ;

д) принятие менеджментом организации БС РФ остаточных рисков и решения о реализации и эксплуатации/совершенствовании СМИБ. Остаточные риски ИБ должны быть соотнесены с рисками банковской деятельности и оценено их влияние на достижение целей деятельности организации БС РФ.

9.2. Реализация и эксплуатация СМИБ

Организации БС РФ следует реализовать следующие процессы:

а) разработка плана обработки рисков ИБ;
б) реализация плана обработки рисков ИБ и реализация защитных мер, управление работами и ресурсами, связанными с реализацией СМИБ;
в) реализация программ по обучению и осведомленности ИБ. Реализация процесса по обучению и осведомленности ИБ должна обеспечиваться с учетом требований раздела 8 международного стандарта ISO/IEC IS 17799-2005;
г) обнаружение и реагирование на инциденты безопасности. Реализация процесса обнаружения и реагирования на инциденты безопасности должна обеспечиваться с учетом требований раздела 13 международного стандарта ISO/IEC IS 17799-2005 и технического отчета ISO/IEC TR 18044;
д) обеспечение непрерывности бизнеса и восстановления после прерываний. Обеспечение непрерывности бизнеса и восстановления после прерываний должны обеспечиваться с учетом требований раздела 14 международного стандарта ISO/IEC IS 17799-2005 и положений BSI PAS-56.

9.3. Проверка (мониторинг и анализ) СМИБ

Процессы мониторинга и анализа СМИБ организации должны быть интегрированы в систему внутреннего контроля организаций БС РФ.

Организации следует реализовать следующие процессы мониторинга и анализа СМИБ:

а) мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ;
б) анализ эффективности СМИБ, включая анализ уровней остаточного и приемлемого рисков ИБ;
в) внутренний аудит СМИБ;
г) анализ СМИБ со стороны высшего руководства;
д) проведение периодического внешнего аудита СМИБ.

9.4. Совершенствование СМИБ

Организации следует реализовать следующие процессы:

а) реализация тактических улучшений в СМИБ, осуществляемых в рамках полномочий служб (ответственных) ИБ организации;
б) реализация стратегических улучшений СМИБ, требующих принятия решений на уровне руководства организации и инициирования процессов планирования СМИБ. Использование опыта;
в) информирование об изменениях и их согласование с заинтересованными сторонами;
г) оценка достижения поставленных целей и потребностей в развитии СМИБ.

9.5. Система документации

Организации следует использовать систему менеджмента документации для СМИБ. Документы в данной системе необходимо соответствующим образом защищать и контролировать. Данная система должна также включать любые записи, которые создаются или поддерживаются для обеспечения свидетельств эффективной работы СМИБ.

9.6. Обеспечение непрерывности бизнеса (деятельности) и восстановление после прерываний

Организации следует разработать и внедрить план обеспечения непрерывности бизнеса (деятельности) и восстановления после прерываний. Данный план и соответствующие процессы восстановления должны пересматриваться на регулярной основе и своевременно обновляться (например, при существенных изменениях в операционной деятельности, организационной структуре, бизнес-процессах и автоматизированных банковских системах). Эффективность документированных процедур восстановления необходимо периодически проверять и тестировать (как минимум на полугодовой основе). С данным планом должны быть ознакомлены все сотрудники, отвечающие за его выполнение и вовлеченные в процессы восстановления.

В качестве методологической основы при разработке плана могут быть использованы общепринятые международные стандарты, регулирующие вопросы менеджмента непрерывности бизнеса (например, BSI PAS-56).

9.7. Служба информационной безопасности (уполномоченное лицо) организации БС РФ

9.7.1. Для реализации задач развертывания и эксплуатации СМИБ организации рекомендуется иметь в своем составе (самостоятельную или в составе службы безопасности) службу ИБ (уполномоченное лицо). Службу ИБ (уполномоченное лицо) 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 связанную 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 (Председателя или заместителя Председателя правления и т.п.). При этом служба ИБ и служба информатизации (автоматизации) не должны иметь общего куратора.

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

Организациям, имеющим сеть филиалов или региональных представительств, рекомендуется выделить соответствующие подразделения ИБ на местах, обеспечив их соответствующими ресурсами и нормативной базой.

10. Проверка и оценка информационной безопасности организации БС РФ

10.1. Проверка и оценка ИБ организации может быть произведена с помощью аудита, самооценки и мониторинга ИБ.

10.2. Аудит ИБ организации БС РФ может быть внутренним или внешним (см. п. 7.3.4). Цель, порядок и периодичность проведения аудитов ИБ организации в целом (или ее отдельных структурных подразделений) или АБС определяется руководством организации на основе потребностей в такой деятельности и фиксируется в программе аудита ИБ.

10.3. Цель аудита ИБ организации состоит в проверке и оценке соответствия ИБ требованиям настоящего стандарта. Заключение по результатам проведения аудита ИБ организации должно показывать:

— текущий уровень ИБ организации;
— уровень зрелости процессов менеджмента ИБ организации;
— уровень осознания ИБ организации.

10.4. 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.

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

10.6. 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.

10.7. 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.

10.8. Хорошей практикой подготовки к аудиту ИБ и проверки уровня ИБ организации БС РФ является проведение самооценки ИБ. Самооценка ИБ проводится собственными силами и по инициативе руководства организации. При проведении самооценки ИБ должны использоваться журналы регистрации инцидентов ИБ, ведущиеся службами безопасности организации и формируемые на основе данных мониторинга ИБ, проверяться эффективность реализованных защитных мер путем тестовых проверок (могут быть проверки на проникновение).

10.9. Мониторинг ИБ должен проводиться персоналом организации, ответственным за ИБ, с целью обнаружения и регистрации отклонений функционирования 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 руководством цели. 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 инцидентов 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. Модель зрелости процессов менеджмента информационной безопасности организации БС РФ

11.1. Модель зрелости является мерой оценки полноты, адекватности и эффективности процессов менеджмента ИБ.

11.2. Уровень проработанности процессов менеджмента ИБ определяется тем, насколько полно и последовательно менеджмент организации руководствуется принципами ИБ, реализует политики и требования ИБ, использует накопленный опыт и совершенствует СМИБ.

11.3. Оценка зрелости процессов менеджмента ИБ организации основывается на рассмотрении совокупности параметров для каждого из этих процессов, отражающих достижение того или иного уровня зрелости данного процесса.

11.4. Модель зрелости процессов менеджмента ИБ организации настоящего стандарта основывается на универсальной модели зрелости процессов, определенной стандартом COBIT, которая определяет шесть уровней зрелости организации — с нулевого по пятый.

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

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

Второй уровень (“повторяемый”) характеризует проработанность процессов менеджмента 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 менеджмента ИБ обеспечивается их оптимизация. Процессы менеджмента ИБ находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации менеджмента ИБ используются частично и в ограниченном объеме.

Пятый уровень (“оптимизированный”) характеризует проработанность процессов менеджмента 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 менеджмента ИБ. Организация способна к быстрой адаптации при изменениях в окружении и бизнесе.

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

11.6. Достижение четвертого уровня зрелости процессов менеджмента ИБ характеризуется следующими параметрами:

- разработана и совершенствуется нормативная и распорядительная документация по ИБ (политика ИБ, регламенты и положения ИБ, должностные инструкции 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, непрерывно совершенствуются и основываются на хорошей практике. В процессе внедрения защитных мер используется анализ затрат и результатов, обеспечивается их оптимизация;

— 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.

11.7. Результаты оценки зрелости каждого из процессов менеджмента ИБ должны учитываться в общем итоговом рейтинге зрелости организации.

12. Направления развития стандарта

Реализация положений настоящего стандарта должна обеспечиваться положениями стандартов из комплекса стандартов Банка России СТО БР ИББС, 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.
[3] Корпоративный менеджмент: Справочник для профессионалов / И.И. Мазур, В.Д. Шапиро, Н.Г. Ольдерогге и др.; Под общ. ред. И.И. Мазура. — М.: Высшая школа, 2003. — 1077 с.
[4] Банковский менеджмент, Питер С. Роуз — М.: “Дело Лтд”,1995. — 768 с.
[5] Основы банковской деятельности, Афанасьева Л.П., Богатырев В.И., Журкина Н.Г. и др. — М., 2003.

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