СТАНДАРТ БАНКА РОССИИ

СТО БР ИББС-1.1-2007

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2007-05-01

Москва
2007

Предисловие

1. ПРИНЯТ И ВВЕДЕН в действие Распоряжением Банка России от 28 апреля 2007 года № Р-345.

2. ВВЕДЕН ВПЕРВЫЕ.

Содержание

Введение

Одним из условий реализации целей деятельности организаций банковской системы Российской Федерации (БС РФ) является обеспечение необходимого и достаточного уровня их информационной безопасности (ИБ).

Основным из видов проверки уровня ИБ в организациях БС РФ является аудит ИБ. Мировой опыт в области обеспечения ИБ определяет аудит ИБ как важнейший процесс в непрерывном цикле процессов менеджмента ИБ организации.

Банк России является сторонником регулярного проведения аудита ИБ в организациях БС РФ.

Основными целями аудита ИБ организаций БС РФ являются:

— повышение доверия к организациям БС РФ;
— оценка соответствия ИБ организаций БС РФ критериям аудита ИБ, установленным согласно требованиям стандарта Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0).

СТАНДАРТ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения: 2007-05-01

1. Область применения

Настоящий стандарт распространяется на организации БС РФ, а также на организации, проводящие аудит ИБ организаций БС РФ, и устанавливает требования к проведению внешнего аудита ИБ организаций БС РФ.

Настоящий стандарт рекомендован для применения путем включения ссылок на него и использования устанавливаемых в нем положений и требований при разработке программ аудита ИБ, а также при разработке других нормативных документов организаций БС РФ по обеспечению ИБ.

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

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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

СТО БР ИББС-1.0

3. Термины и определения

В настоящем стандарте применены термины по СТО БР ИББС-1.0, а также следующие термины (в алфавитном порядке) с соответствующими определениями.

3.1. **Внешний аудит информационной безопасности организации банковской системы Российской Федерации; аудит информационной безопасности:** Систематический, независимый и документируемый процесс получения свидетельств аудита деятельности организации БС РФ по обеспечению ИБ и установления степени выполнения в организации БС РФ установленных критериев аудита ИБ, проводимый внешней по отношению к проверяемой независимой проверяющей организацией.

3.2. **Аудитор (эксперт):** Лицо, обладающее компетентностью для проведения аудита информационной безопасности.

3.3. **Аудиторская группа:** Один или несколько аудиторов, проводящих аудит информационной безопасности, при необходимости поддерживаемые техническими экспертами.

3.4. **Выводы аудита информационной безопасности; выводы аудита ИБ:** Результат оценки собранных свидетельств аудита информационной безопасности на соответствие критериям аудита информационной безопасности.

Примечание. Выводы аудита информационной безопасности указывают на степень соответствия ИБ организации БС РФ критериям аудита ИБ.

3.5. **Заказчик аудита информационной безопасности; заказчик аудита ИБ:** Организация или лицо, заказавшие аудит информационной безопасности.

Примечание. Заказчик может быть проверяемой организацией или любой другой организацией, которая имеет законное право потребовать аудит информационной безопасности.

3.6. **Заключение по результатам аудита информационной безопасности (аудиторское заключение); заключение по результатам аудита ИБ:** Качественная и/или количественная оценки степени соответствия установленным критериям аудита информационной безопасности, представленные аудиторской группой после рассмотрения всех выводов аудита информационной безопасности в соответствии с целями аудита информационной безопасности.

3.7. **Критерии аудита (самооценки) информационной безопасности; критерии аудита (самооценки) ИБ:** Совокупность требований в области информационной безопасности, определенных в соответствии с положениями СТО БР ИББС-1.0 или его частью, и характеризующая некоторый уровень информационной безопасности.

Примечание. Критерии аудита (самооценки) информационной безопасности используются для сопоставления с ними свидетельств аудита (самооценки) информационной безопасности.

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

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

3.9. **Проверяемая организация:** Организация банковской системы Российской Федерации, в которой проводится аудит информационной безопасности.

3.10. **Проверяющая организация (аудиторская организация):** Организация, проводящая аудит информационной безопасности.

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

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

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

Примечание. Свидетельства аудита (самооценки) информационной безопасности могут быть качественными или количественными.

3.13. **Самооценка информационной безопасности организации банковской системы Российской Федерации; самооценка ИБ:** Систематический и документируемый процесс получения свидетельств самооценки в деятельности организации БС РФ по обеспечению ИБ и установления степени выполнения в организации БС РФ установленных критериев самооценки ИБ. Самооценка ИБ выполняется самостоятельно сотрудниками организации БС РФ.

3.14. **Технический эксперт:** Лицо, предоставляющее аудиторской группе свои знания и/или опыт по специальным вопросам.

4. Исходная концептуальная схема (парадигма) аудита информационной безопасности организаций БС РФ

4.1. В основе исходной концептуальной схемы аудита ИБ организаций БС РФ лежит, с одной стороны, желание собственника доказать достижение организацией БС РФ высокого уровня ИБ и таким образом повысить доверие к ней, с другой стороны — стремление аудиторов с помощью проведения независимой и компетентной оценки определить истинный (в пределах возможностей аудита ИБ) уровень организации работ в области ИБ и степень соответствия ИБ организации БС РФ установленным требованиям (критериям аудита).

4.2. Уровень ИБ организации БС РФ соответствует высокому уровню ИБ, если процессы системы обеспечения ИБ проводятся осознанно на основе прогноза, мониторинга и анализа внутренней и внешней среды, развития и изменения целей бизнеса (деятельности) организации БС РФ.

4.3. Возможное изменение внешней среды ведения бизнеса (деятельности) организации БС РФ, изменение и возрастание рисков ИБ вследствие естественных и/или преднамеренных изменений во внешней и внутренней среде организации БС РФ является причиной для регулярного проведения аудита ИБ в организации БС РФ, что позволяет своевременно принимать меры по поддержанию ИБ на необходимом уровне.

4.4. Оценка соответствия ИБ организации БС РФ критериям аудита ИБ проводится на основе документов по обеспечению ИБ и фактов, свидетельствующих о выполнении, частичном выполнении или невыполнении установленных требований ИБ.

5. Основные принципы проведения аудита информационной безопасности организаций БС РФ

5.1. **Независимость аудита ИБ.** Аудиторы независимы в своей деятельности и неответственны за деятельность, которая подвергается аудиту ИБ. Независимость является основанием для беспристрастности при проведении аудита ИБ и объективности при формировании заключения по результатам аудита ИБ.

5.2. **Полнота аудита ИБ.** Аудит ИБ должен охватывать все области аудита ИБ, соответствующие аудиторскому заданию. Кроме того, полнота аудита ИБ определяется достаточностью затребованных и предоставленных материалов, документов и уровнем их соответствия поставленным задачам. Полнота аудита ИБ является необходимым условием для формирования объективных заключений по результатам аудита ИБ.

5.3. **Оценка на основе свидетельств аудита ИБ.** При периодическом проведении аудита ИБ оценка на основе свидетельств аудита ИБ является единственным способом, позволяющим получить повторяемое заключение по результатам аудита ИБ, что повышает доверие к такому заключению. Для повторяемости заключения свидетельства аудита ИБ должны быть проверяемыми.

5.4. **Достоверность свидетельств аудита ИБ.** У аудиторов должна быть уверенность в достоверности свидетельств аудита ИБ. Доверие к документальным свидетельствам аудита ИБ повышается при подтверждении их достоверности третьей стороной или руководством организации БС РФ. Доверие к фактам, полученным при опросе сотрудников проверяемой организации, повышается при подтверждении данных фактов из различных источников. Доверие к фактам, полученным при наблюдении за деятельностью проверяемой организации в области ИБ, повышается, если они получены непосредственно при функционировании проверяемых процедур или процессов.

5.5. **Компетентность.** Доверие к процессу и результатам аудита ИБ зависит от компетентности тех, кто проводит аудит ИБ, и от этичности их поведения. Компетентность базируется на способности аудитора применять знания и навыки.

5.6. **Этичность поведения.** Этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, беспристрастность.

6. Менеджмент программы аудита информационной безопасности

6.1. Программа аудита ИБ включает деятельность, необходимую для планирования и организации определенного количества аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения аудитов ИБ в заданные сроки.

Программа аудита ИБ разрабатывается организацией БС РФ. В общем случае могут быть разработаны несколько программ аудита ИБ.

Рекомендованная последовательность процессов менеджмента программы аудита ИБ представлена на рисунке 1[1].

6.2. Руководство организации БС РФ должно распределять полномочия и ответственность за управление программой аудита ИБ.

Ответственные за управление программой аудита ИБ лица должны иметь представление о принципах аудита ИБ, компетентности аудиторов, содержании этапов аудита ИБ, а также обладать знаниями по обеспечению ИБ.

Ответственные за управление программой аудита ИБ лица должны:

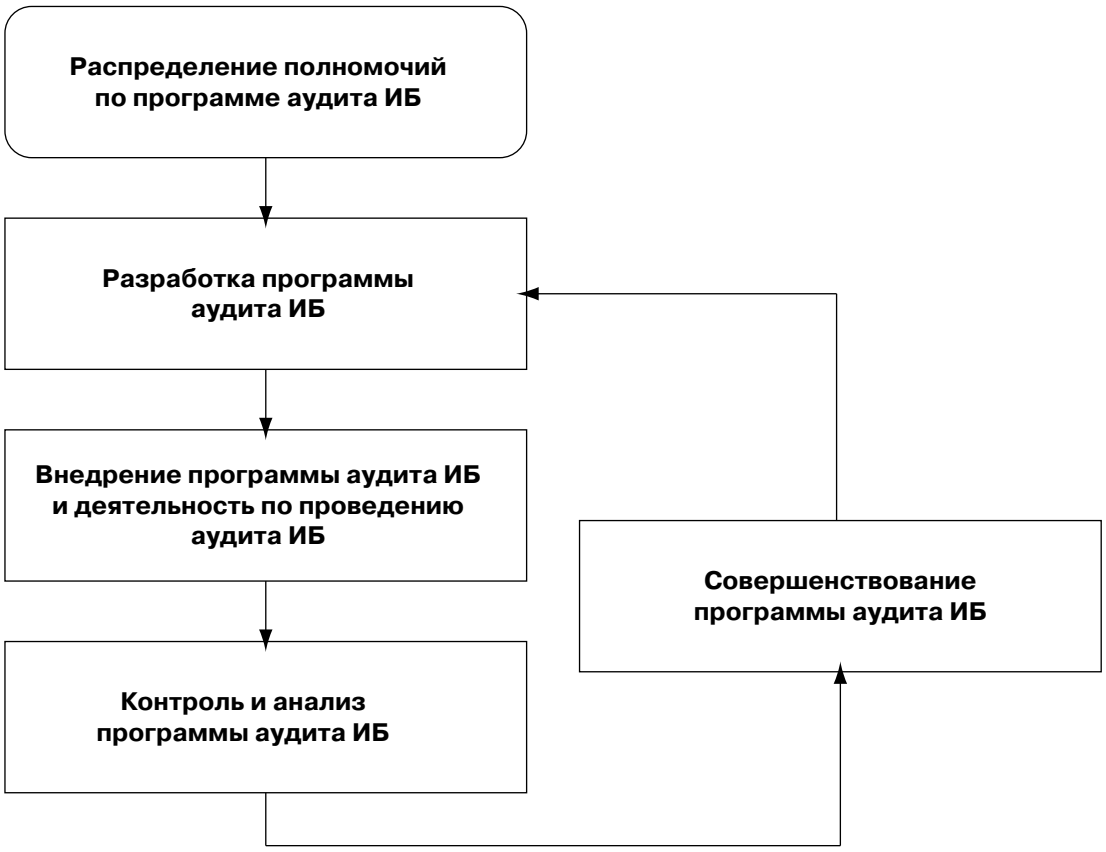
— разрабатывать, внедрять, контролировать, анализировать и совершенствовать программу аудита ИБ;
— определять потребность программы аудита ИБ в ресурсах;
— способствовать принятию решений об обеспечении программы аудита ИБ необходимыми ресурсами.

---

[1] Последовательность процессов менеджмента программ аудита гармонизирована с моделью менеджмента ИБ, определенной разделом 5 СТО БР ИББС-1.0 и положениями международного стандарта [1].

6.3. Разработка программы аудита ИБ должна включать в себя определение целей, объема программы, а также необходимых финансовых, информационных и людских ресурсов для ее реализации.

Рисунок 1. Последовательность процессов менеджмента программы аудита ИБ



Целью программы аудита ИБ является оценка соответствия ИБ организации БС РФ критериям аудита и содействие в повышении при необходимости уровня ИБ организации БС РФ.

На объем программы аудита ИБ влияют размер и сложность структуры организации БС РФ, область каждого аудита ИБ и частота проводимых аудитов ИБ.

6.4. Внедрение программы аудита ИБ должно включать в себя:

- доведение программы аудита ИБ до участвующих в ее реализации сторон;
- планирование аудитов ИБ;
- определение привлекаемых аудиторских организаций и предоставляемых ресурсов для проведения аудитов ИБ;
- проведение аудитов ИБ в соответствии с программой аудита ИБ;
- анализ и утверждение отчетов по результатам аудитов ИБ;
- определение действий по результатам аудитов ИБ.

6.5. В организации БС РФ должны проводиться контроль внедрения программы аудита ИБ, анализ достижения целей программы аудита ИБ и определение возможностей для ее совершенствования. О результатах анализа должно информироваться руководство организации БС РФ.

Контроль и анализ программы аудита ИБ должны включать в себя:

- проверку возможностей аудиторских групп, служб или лиц по реализации аудита ИБ. Подтверждением возможности по реализации аудита могут являться информация об образовании и опыте работы членов аудиторской группы, сертификаты, подтверждающие квалификацию членов аудиторской группы;
- анализ достижения целей аудита ИБ и программы аудита ИБ в целом;
- анализ отчетов и заключений по результатам аудита ИБ.

6.6. Совершенствование программы аудита ИБ состоит в определении корректирующих и превентивных действий по совершенствованию программы аудита ИБ, включающих в себя пересмотр и корректировку сроков проведения аудитов ИБ и необходимых ресурсов, улучшение методов подготовки свидетельств аудита ИБ.

7. Проведение аудита информационной безопасности

7.1. Требования к взаимоотношениям представителей аудиторской организации с представителями проверяемой организации

7.1.1. В процессе общения представители аудиторской организации и представители проверяемой организации на всех этапах проведения аудита ИБ должны демонстрировать честность, открытость, желание обсуждать и по возможности разрешать возникшие разногласия.

Аудиторская организация должна информировать проверяемую организацию обо всех мероприятиях, проводимых в рамках аудиторской проверки.

Проверяемая организация должна обеспечивать предоставление аудиторской организации всей необходимой для проведения аудита ИБ информации.

7.1.2. Аудиторское задание на проведение аудита ИБ должно оформляться договором в соответствии с требованиями законодательства РФ.

Хорошими практиками являются:

— направление официального предложения аудиторской организации со стороны проверяемой организации или заказчика аудита, например, государственного надзорного органа, о заключении договора на проведение аудита ИБ;
— направление аудиторской организацией письма о проведении аудита ИБ руководству проверяемой организации до заключения договора на проведение аудита ИБ с целью согласования условий предстоящего договора.

В договоре на проведение аудита ИБ необходимо зафиксировать критерии аудита ИБ, по которым должно быть выражено мнение аудиторской организации.

7.1.3. При подготовке к проведению аудита ИБ и в процессе его проведения аудиторская группа вправе самостоятельно принимать решение об источниках, методах получения и достоверности свидетельств аудита ИБ (см. пункт 7.2.10), необходимых для составления заключения по результатам аудита ИБ, если иное не оговорено в договоре на проведение аудита ИБ.

7.1.4. В процессе проведения аудита ИБ руководитель аудиторской группы должен периодически доводить до сведения проверяемой организации и заказчика аудита информацию о ходе аудита ИБ и любых возникающих проблемах. Свидетельства, собранные при проведении аудита ИБ, которые выявляют критические для ИБ проверяемой организации уязвимости (по мнению руководителя аудиторской группы), должны быть немедленно доведены до сведения проверяемой организации и, если необходимо, до сведения заказчика аудита ИБ.

Если имеющееся свидетельство аудита ИБ (или его отсутствие) указывает на то, что цель аудита ИБ недостижима, то руководитель аудиторской группы должен сообщить причины заказчику аудита ИБ и проверяемой организации для определения дальнейших действий. Эти действия могут включать либо изменение цели или областей аудита ИБ, либо прекращение аудита ИБ.

7.1.5. Аудиторская организация несет ответственность за:

— достоверность заключения по результатам аудита ИБ;
— соблюдение конфиденциальности сведений и документов, получаемых и составляемых в ходе аудиторской проверки организации (за исключением случаев, прямо предусмотренных действующим законодательством РФ). При необходимости требования по использованию документов проверяемой организации и отчета по аудиту ИБ должны определяться договором на проведение аудита ИБ.

7.1.6. Руководство проверяемой организации несет ответственность за:

— достоверность и полноту предоставляемой аудиторской организации информации;
— любые ограничения возможности осуществления аудиторской организацией своих обязательств.

7.1.7. Факты невыполнения требований, установленных в пункте 7.1.5, сообщаются в органы, контролирующие деятельность аудиторских организаций, и заказчику аудита ИБ.

Факты невыполнения требований, установленных в пункте 7.1.6, указываются в отчете об аудите ИБ и могут служить основанием для прекращения процесса аудита ИБ.

7.2. Требования к этапам проведения аудита информационной безопасности организаций БС РФ

7.2.1. Работы по проведению аудита ИБ организаций БС РФ должны включать следующие этапы:

— подготовка к проведению аудита ИБ;
— анализ документов;
— проведение аудита ИБ на месте;
— подготовка, утверждение и рассылка отчета по аудиту ИБ;
— завершение аудита ИБ.

7.2.2. Подготовка к проведению аудита ИБ должна начинаться с определения возможности проведения аудита ИБ, а также согласования и заключения договора на проведение аудита ИБ (см. пункт 7.1.2) между организацией БС РФ и аудиторской организацией. Дальнейшая подготовка аудиторской организации к проведению аудита ИБ должна заключаться в формировании аудиторской группы, назначении ее руководителя и установлении руководителем аудиторской группы контакта с проверяемой организацией.

Содержание договора на проведение аудита ИБ может иметь особенности, но, как правило, в нем рекомендуется указывать:

— область аудита ИБ;
— ответственность руководства проверяемой организации за подготовку и предоставление необходимых свидетельств аудита ИБ;
— требования к отчету аудита ИБ;
— порядок взаимодействия представителей проверяющей и проверяемой организаций;
— порядок сбора необходимых свидетельств аудита;
— цена проведения аудита ИБ;
— порядок привлечения к работе по каким-либо вопросам аудита ИБ других проверяющих организаций и(или) технических экспертов;
— необходимые ограничения ответственности проверяющей организации.

7.2.3. Аудиторская организация должна определить возможность проведения аудита ИБ на основании готовности к сотрудничеству со стороны проверяемой организации и наличия времени и соответствующих ресурсов.

Если проведение аудита ИБ признано невозможным, то по результатам консультаций с проверяемой организацией заказчику аудита должен быть предложен альтернативный вариант (перенос сроков проведения аудита, привлечение для проведения аудита ИБ другой аудиторской организации).

7.2.4. В аудиторской организации для проведения аудита ИБ должна быть сформирована аудиторская группа. Руководством аудиторской организации должен быть назначен руководитель аудиторской группы, ответственный за проведение аудита ИБ организации.

При определении размера и состава аудиторской группы прежде всего должна учитываться компетентность аудиторской группы, в основе которой лежит уровень квалификации ее участников.

Если аудиторы в аудиторской группе не обладают необходимыми знаниями и опытом по специальным вопросам, в группу включают технических экспертов. Технические эксперты должны работать под руководством аудиторов.

7.2.5. Руководитель аудиторской группы должен в соответствии с договором на проведение аудита установить контакт с проверяемой организацией прежде всего для установления способов обмена информацией с представителями проверяемой организации с целью подтверждения полномочий на проведение аудита ИБ и запроса доступа к необходимым документам проверяемой организации.

7.2.6. До проведения аудита ИБ на месте аудиторской группой должен быть проведен анализ требуемой документации проверяемой организации для определения соответствия положений, отраженных в документации, критериям аудита ИБ.

Если документация будет признана неадекватной, то руководитель аудиторской группы должен сообщить об этом заказчику аудита ИБ и проверяемой организации. Аудиторской группой должно быть принято решение, может ли аудит ИБ быть продолжен или его необходимо приостановить до момента решения всех вопросов по документации.

7.2.7. Если аудиторской группой принято решение о продолжении аудита ИБ, то руководитель аудиторской группы должен подготовить план аудита ИБ на месте и согласовать его с заказчиком аудита и проверяемой организацией.

План аудита ИБ на месте должен включать:
— цель аудита ИБ;
— критерии аудита ИБ;
— область аудита ИБ;
— дату и продолжительность проведения аудита ИБ на месте;
— роли членов аудиторской группы и сопровождающих лиц со стороны проверяемой организации;
— результаты анализа документов, предоставленных проверяемой организацией для проведения аудита ИБ, и оценку свидетельств аудита ИБ;
— описание деятельности и мероприятий по проведению аудита ИБ на месте;
— распределение ресурсов при проведении аудита.

Согласованный план должен быть представлен проверяемой организации перед началом аудита ИБ на месте.

7.2.8. Проведение аудита ИБ на месте должно включать следующие работы:
— проведение вступительного совещания;
— сбор дополнительных свидетельств аудита ИБ;
— оценка свидетельств аудита ИБ;
— подготовка заключения по результатам аудита ИБ;
— проведение заключительного совещания.

7.2.9. Вступительное совещание с участием аудиторской группы и лиц, ответственных за подразделения или процессы, подлежащие проверке, должно проводиться с целью изложения действий по проведению аудита ИБ и подтверждения способов обмена информацией между аудиторской группой и представителями проверяемой организации. Председательствовать на совещании должен руководитель аудиторской группы.

Изложение действий по проведению аудита ИБ заключается прежде всего в рассмотрении вопросов о процедурах аудиторской проверки, источниках, методах получения и достоверности свидетельств аудита ИБ, необходимых для составления заключения по результатам аудита ИБ.

7.2.10. Основными источниками свидетельств аудита ИБ должны являться:
— документы проверяемой организации и третьих лиц, относящиеся к обеспечению ИБ организации;
— устные высказывания и письменные ответы сотрудников проверяемой организации в процессе проводимых опросов;
— результаты наблюдений аудиторов за деятельностью организации в области ИБ.

Основными методами получения свидетельств аудита ИБ должны являться:
— проверка и анализ документов, касающихся обеспечения ИБ организации;
— наблюдение за деятельностью организации в области ИБ;
— опрос сотрудников проверяемой организации и независимой (третьей) стороны.

По степени достоверности (от наибольшей к наименьшей) свидетельства аудита ИБ делятся следующим образом:
— свидетельства, полученные от третьей стороны в письменном виде;
— свидетельства, полученные от проверяемой организации и подтвержденные третьей стороной в письменном виде;
— свидетельства, полученные в ходе проведения аудиторских процедур (наблюдения за деятельностью, анализа данных системы мониторинга ИБ и т.д.);
— свидетельства, полученные в форме документов;
— свидетельства, полученные в устной форме.

7.2.11. При сборе свидетельств аудита ИБ аудиторы должны исходить из того, что деятельность проверяемой организации в области ИБ осуществляется в соответствии с критериями аудита, если этому есть доказательства. Аудиторы должны проявлять достаточную степень профессионального скептицизма в отношении собираемых свидетельств аудита ИБ, принимая во внимание возможность наличия различного вида нарушений при обеспечении ИБ в проверяемой организации.

Проверка и анализ документов могут проводиться на всех этапах аудиторской проверки. Проверка и анализ документов позволяют аудитору получить свидетельства аудита ИБ, обладающие наибольшей полнотой и удобством восприятия и использования по сравнению с другими методами получения свидетельств аудита ИБ. Однако эти свидетельства аудита ИБ имеют различную степень достоверности в зависимости от их характера и источника, а также от эффективности внутреннего контроля организации за процессом подготовки и обработки представленных документов.

Устный опрос может проводиться на всех этапах аудиторской проверки. Результаты устных опросов должны оформляться в виде протокола или краткого конспекта, в котором обязательно должны быть указаны фамилия, имя, отчество сотрудника аудиторской организации, проводившего опрос, фамилия, имя, отчество опрашиваемого лица, а также представлены их подписи. Для проведения типовых опросов могут быть подготовлены бланки с перечнями интересующих вопросов. Письменная информация по итогам устных опросов должна приобщаться аудиторской организацией к другим рабочим документам аудиторской проверки. Однако результаты устного опроса следует проверять, так как опрашиваемый может выражать свое субъективное мнение. Хорошей практикой является проведение перекрестных опросов сотрудников организации (т.е. опрос различных лиц). Наблюдение представляет собой отслеживание аудитором процедур или процессов в проверяемой организации, выполняемых другими лицами (в т.ч. персоналом организации). Информация считается достоверной только в том случае, если она получена непосредственно в момент выполнения проверяемых процедур или функционирования процессов.

7.2.12. Свидетельства аудита ИБ должны быть оценены с точки зрения критериев аудита для формирования выводов аудита ИБ. Выводы аудита ИБ указывают на степень соответствия ИБ организации БС РФ критериям аудита ИБ.

Оценка соответствия ИБ организации БС РФ критериям аудита ИБ осуществляется на основе принятых в организации БС РФ документов и методик.

7.2.13. Выводы аудита ИБ и подтверждающие их свидетельства аудита ИБ должны быть рассмотрены и проанализированы аудиторами совместно с представителем проверяемой организации для получения подтверждения того, что свидетельства аудита ИБ верны и понятны. Нерешенные вопросы должны быть зарегистрированы в протоколах совещаний и отражены в отчете по аудиту ИБ.

7.2.14. По результатам аудита ИБ аудиторской группой должно быть подготовлено аудиторское заключение.

Если ограничение области аудита ИБ настолько существенно и глубоко, что аудитор не в состоянии провести оценку соответствия ИБ проверяемой организации критериям аудита ИБ, то аудиторская группа должна отказаться от формирования заключения.

В результате проведения аудита ИБ умышленно может быть сформулировано заведомо ложное аудиторское заключение. При выявлении любой из заинтересованных в деятельности проверяемой организации БС РФ сторон фактов, подтверждающих умышленное формирование ложного аудиторского заключения, она имеет право добиться отмены такого заключения. Заведомо ложным аудиторское заключение признается только в порядке, установленном органами, контролирующими деятельность аудиторских организаций.

7.2.15. По окончании аудита ИБ должно быть проведено заключительное совещание с участием представителей аудиторской организации, проверяемой организации и заказчика аудита ИБ под председательством руководителя аудиторской группы.

На совещании должны быть представлены выводы аудита ИБ и заключение по результатам аудита ИБ таким образом, чтобы они были понятны и признаны проверяемой организацией. Любые разногласия по выводам и/или заключению по результатам аудита ИБ между аудиторской группой и проверяемой организацией должны быть обсуждены и по возможности разрешены. Если стороны не пришли к единому мнению, то это должно быть зарегистрировано.

На совещании могут быть представлены рекомендации по повышению уровня ИБ проверяемой организации.

7.2.16. По результатам проведения аудита ИБ аудиторская группа должна подготовить отчет. Руководитель аудиторской группы несет ответственность за подготовку и содержание отчета по результатам проведения аудита ИБ.

Отчет должен предоставлять полные, точные, четкие и достаточные записи по аудиту ИБ и должен включать следующее:

- сведения об аудиторской организации;
- сведения о руководителе и членах аудиторской группы;
- сведения о проверяемой организации;
- сведения о заказчике аудита ИБ;
- цель аудита ИБ;
- область аудита ИБ, в частности, сведения о проверенных организационных и функциональных единицах или процессах и охваченном периоде времени;
- сроки проведения аудита ИБ;
- план аудита ИБ на месте;

— документально оформленную совокупность анкет, содержащих критерии аудита ИБ и выводы аудита ИБ, сделанные по каждому из рассмотренных критериев аудита ИБ;
— заключение по результатам аудита ИБ;
— перечень представителей со стороны проверяемой организации, которые сопровождали и опрашивались аудиторской группой при проведении аудита ИБ;
— краткое изложение процесса аудита ИБ, включая элемент неопределенности и/или проблемы, которые могут отразиться на надежности заключения по результатам аудита ИБ;
— подтверждение, что цель аудита ИБ достигнута в области аудита ИБ в соответствии с планом аудита ИБ;
— любые неохваченные области, входящие в область аудита ИБ;
— любые неразрешенные разногласия между аудиторской группой и проверяемой организацией;
— заявление о конфиденциальном характере содержания отчета;
— лист рассылки отчета по результатам аудита ИБ.

Отчет по результатам проведения аудита ИБ должен быть выпущен в согласованные сроки, утвержден руководителем аудиторской организации и разослан получателям, определенным заказчиком аудита ИБ.

Отчет по результатам проведения аудита ИБ является собственностью заказчика аудита ИБ. Члены аудиторской группы и все получатели отчета должны обеспечивать конфиденциальность содержания отчета, за исключением случаев, прямо предусмотренных действующим законодательством Российской Федерации.

8. Проведение самооценки информационной безопасности

8.1. Хорошей практикой проверки уровня ИБ и подготовки к аудиту ИБ организации БС РФ является самооценка ИБ. Самооценка ИБ проводится на основе принятых в организации БС РФ документов и методик.

С помощью самооценки ИБ организации БС РФ могут самостоятельно оценить соответствие ИБ критериям аудита и провести анализ недостатков системы обеспечения ИБ организации БС РФ.

Результаты самооценки ИБ могут служить основанием для устранения выявленных недостатков системы обеспечения ИБ до проведения аудита ИБ в организации БС РФ.

8.2. Самооценка ИБ может проводиться в рамках программы аудита ИБ, разработанной в организации БС РФ.

8.3. Результаты самооценки ИБ не могут служить декларацией о соответствии критериям аудита ИБ.

8.4. Работы по проведению самооценки ИБ организаций БС РФ должны включать следующие этапы:
— формирование группы по организации самооценки ИБ, по сбору и анализу данных самооценки ИБ;
— проведение самооценки ИБ;
— формирование результатов самооценки ИБ и информирование руководства организации БС РФ о результатах проведенной самооценки ИБ.

8.5. Самооценка ИБ должна проводиться сотрудниками организации БС РФ, принимающими непосредственное участие в деятельности по обеспечению ИБ. Как правило, это должны быть сотрудники службы ИБ.

8.6. Результаты самооценки должны быть проанализированы руководством организации БС РФ для понимания существующих в организации БС РФ проблем ИБ и определения мер по их решению.

Библиография

[1] ISO/IEC 27001:2005(E) Information technology — Security techniques — Information security management systems — Requirements

Ключевые слова: банковская система Российской Федерации, информационная безопасность, аудит информационной безопасности, свидетельства аудита информационной безопасности.