В свое время Банк России признал РС БР ИББС-2.0-2007 необязательным, но многие банки продолжают им пользоваться, ведь замены нет. Между тем «бумажная» безопасность в последние годы переросла в организационно-технические меры, и шаблонные документы уже не годятся. Руководствуясь опытом и практикой, в цикле статей авторы опишут примерный «скелет» основных документов, что поможет специалистам ИБ, особенно в небольших банках, правильно регламентировать процессы.

Александр ВИНОГРАДОВ, *ФГУП «ЦНИИХМ», старший научный сотрудник*
Анастасия НИКОЛАЕВА, *независимый эксперт*

Как правильно написать документы по ИБ: шпаргалка от экспертов для небольших банков

При проверках внутренних документов по ИБ регулятор зачастую находит недочеты: например, не создан какой-то журнал либо часть прописанных шагов не реализована — планировали, но забыли или пустили на самотек. Чтобы помочь избежать такой ситуации, мы постарались раскрыть в полном объеме законодательную основу и примерные пункты документов, а при описании законодательной базы учесть комплекс мер, предусмотренных Банком России в области ИБ.

Согласно РС БР ИББС-2.0-2007, в банке необходимо организовать четыре уровня внутренней документации: корпоративная политика ИБ, частные политики ИБ, требования ИБ к процедурам и свидетельства выполнения деятельности по обеспечению ИБ. В этой статье начнем с самых простых и главных документов.

Политика (концепция) ИБ

Законодательная база

1. Федеральные законы[1]: 149-ФЗ, 152-ФЗ, 161-ФЗ, 162-ФЗ, 167-ФЗ.
2. Постановление Правительства РФ: 584.
3. Положения Банка России: 683-П, 716-П, 719-П, 787-П, 802-П.

[1] Ввиду обилия нормативных документов в статье указываются только их номера.

Александр ВИНОГРАДОВ
Анастасия НИКОЛАЕВА

4. Указания Банка России: 2831-У, 3889-У.

5. Указ Президента РФ: 250.

6. Стандарты Банка России (СТО БР ИББС): 1.0-2014, 1.1-2007, 1.2-2014, 1.3-2016, 1.4-2018, СТО БР БФБО: 1.5-2018, рекомендации в области стандартизации (РС БР ИББС): 2.0-2007, 2.1-2007, 2.2-2009, 2.5-2014, 2.6-2014, 2.7-2015, 2.8-2015, 2.9-2016.

7. ГОСТы: ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018.

Примерная структура

1. Описание объектов защиты (структура, состав и размещение основных объектов защиты, информационные связи; категории информационных ресурсов, подлежащих защите, и др.).

2. Цели и задачи информационной безопасности (интересы, затрагивающие субъектов информационных отношений; цели защиты; основные задачи системы обеспечения безопасности информации; основные пути решения задач системы защиты; требования к защите информации в платежной(ых) системе(ах) кредитной организации и др.).

3. Основные угрозы безопасности информации банка (угрозы безопасности информации и их источники; пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации; пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации; пути реализации основных естественных угроз безопасности информации; неформальная модель возможных нарушителей; менеджмент инцидентов ИБ; утечка информации по техническим каналам и др.).

4. Общие принципы оценки рисков нарушения информационной безопасности.

5. Общие принципы обеспечения информационной безопасности банка (специальные принципы обеспечения информационной безопасности; обеспечение формирования службы информационной безопасности; осведомленность в области обеспечения защиты информации и др.).

6. Основные требования по обеспечению информационной безопасности банка:

— требования к защите информации при назначении и распределении функциональных прав и обязанностей (ролей) и обеспечении доверия к персоналу банка;

— требования к защите информации автоматизированных банковских систем на стадиях жизненного цикла;

Как правильно написать документы по ИБ: шпаргалка от экспертов для небольших банков

— требования к защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средств вычислительной техники;

— требования к защите информации при использовании информационно-телекоммуникационной сети «Интернет»;

— требования к защите информации при использовании средств криптографической защиты информации (СКЗИ);

— требования к защите информации при осуществлении переводов денежных средств, применяемые:

✓ при назначении и распределении функциональных прав и обязанностей лиц, связанных с осуществлением переводов денежных средств;

✓ на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации объектов информационной инфраструктуры;

✓ при осуществлении доступа к объектам информационной инфраструктуры, включая требования, применяемые для защиты информации от несанкционированного доступа;

✓ для защиты информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средств вычислительной техники;

✓ при использовании информационно-телекоммуникационной сети «Интернет»;

— безопасность информационных технологических процессов банка;

— защита информации при обработке персональных данных;

— требования к проведению аудита информационной безопасности;

— требования к анализу функционирования системы обеспечения информационной безопасности; требования к анализу системы обеспечения информационной безопасности со стороны руководства банка;

— требования к обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

— организация процесса управления риском информационной безопасности;

— требования к принятию решений по тактическим улучшениям системы обеспечения информационной безопасности; требования к принятию решений по стратегическим улучшениям системы обеспечения информационной безопасности; требования к разработке

Александр ВИНОГРАДОВ
Анастасия НИКОЛАЕВА

и реализации программ по обучению и повышению осведомленности и др.

7. Организация системы управления информационной безопасностью.

8. Оценка и контроль обеспечения требуемого уровня защищенности информации.

Положение о сведениях, содержащих информацию конфиденциального характера, и основных мерах по ее защите

Основное заблуждение при написании данного документа состоит в том, что многие по-прежнему используют устойчивое словосочетание «конфиденциальная информация». Это понятие было введено согласно Федеральному закону от 20.02.1995 № 24-ФЗ, но с учетом принятия в 2006 г. Федерального закона № 149-ФЗ было упразднено.

Законодательная база

1. Федеральные законы: 98-ФЗ, 149-ФЗ, 152-ФЗ, 395-1.
2. Указ Президента РФ: 188.

Примерная структура

1. Описание понятий «банковская тайна», «коммерческая тайна» и «персональные данные».

2. Учет, хранение и использование конфиденциальных документов.

3. Порядок допуска сотрудников банка к сведениям конфиденциального характера.

4. Требования к сотрудникам банка, которые обрабатывают эти сведения.

5. Меры по контролю за обеспечением сохранности документов, содержащих конфиденциальные сведения.

6. Ответственность за утрату документов, содержащих конфиденциальные сведения, их разглашение и неправомерное использование.

7. Перечень конфиденциальных сведений, составляющих банковскую и коммерческую тайну, а также персональные данные (приложение).

8. Инструкция о порядке работы с документами, содержащими сведения конфиденциального характера (приложение).

9. Обязательство о неразглашении банковской и коммерческой тайн, а также персональных данных (приложение).

10. Соглашение о конфиденциальности (приложение).

Как правильно написать документы по ИБ: шпаргалка от экспертов для небольших банков

Политика по обеспечению информационной безопасности средствами антивирусной защиты

Законодательная база

1. Положения Банка России: 683-П, 716-П, 719-П, 787-П, 802-П.
2. Рекомендации Банка России: 49-Т.
3. Стандарты Банка России (СТО БР ИББС): 1.0-2014, 1.1-2007, 1.2-2014, 1.3-2016, 1.4-2018, СТО БР БФБО: 1.5-2018, рекомендации в области стандартизации (РС БР ИББС): 2.0-2007, 2.1-2007, 2.2-2009, 2.5-2014, 2.6-2014, 2.7-2015, 2.8-2015, 2.9-2016.
4. ГОСТы: ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018.
5. Постановление Правительства РФ: 1119.
6. Приказ ФСТЭК России: 21.
7. Формуляры к СКЗИ.
8. Эксплуатационная документация к информационным системам.

Примерная структура

1. Общие положения и принципы.
2. Матрица ответственности.
3. Инструкция по антивирусной защите для пользователей (приложение).
4. Регистрация событий и передача в централизованную систему анализа и сбора логов от программных/программно-аппаратных средств защиты от вредоносного кода.
5. Стандарт настроек эшелонированных программных/программно-аппаратных средств защиты от вредоносного кода.
6. Проведение мероприятий по контролю работоспособности средств защиты от вредоносного кода.
7. Повышение осведомленности пользователей.

На что обратить внимание

1. Эшелонированная система защиты антивирусными решениями разных вендоров.
2. Необходимость в некоторых случаях использовать антивирусные решения, сертифицированные не только ФСТЭК России, но и ФСБ России.
3. Организация процесса мониторинга событий ИБ и анализ данных событий от программных/программно-аппаратных средств защиты от вредоносного кода.

Александр ВИНОГРАДОВ
Анастасия НИКОЛАЕВА

Парольная политика

Законодательная база

1. Положения Банка России: 683-П, 716-П, 719-П, 787-П, 802-П.
2. Стандарты Банка России (СТО БР ИББС): 1.0-2014, 1.1-2007, 1.2-2014, 1.3-2016, 1.4-2018, СТО БР БФБО: 1.5-2018, рекомендации в области стандартизации (РС БР ИББС): 2.0-2007, 2.1-2007, 2.2-2009, 2.5-2014, 2.6-2014, 2.7-2015, 2.8-2015, 2.9-2016.
3. ГОСТы: ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018.
4. Модель угроз и нарушителей.
5. Постановление Правительства РФ: 1119.
6. Приказ ФСТЭК России: 21.
7. Банк данных угроз безопасности информации (https://bdu.fstec.ru/threat).

Примерная структура

1. Общие положения и принципы (создание, изменение, защита паролей).
2. Контроль соблюдения политики, ответственность.
3. Регистрация событий ИБ и передача в централизованную систему анализа и сбора логов.

На что обратить внимание

Для объектов информационной инфраструктуры необходимо обратить внимание на реализацию ряда параметров парольной политики:

— длина пароля не менее 8 символов для пользователей и не менее 16 символов для эксплуатационного персонала;

— параметры сложности пароля и частота его смены;

— двухфакторная авторизация эксплуатационного персонала для доступа к объектам информационной инфраструктуры;

— процесс резервного копирования аутентификационных данных эксплуатационного персонала, техники и технологические учетные записи.

Положение о повышении осведомленности и проверке знаний по вопросам ИБ

Законодательная база

1. Положения Банка России: 683-П, 716-П, 719-П, 787-П, 802-П.
2. Стандарты Банка России (СТО БР ИББС): 1.0-2014, 1.1-2007, 1.2-2014, 1.3-2016, 1.4-2018, СТО БР БФБО: 1.5-2018, рекомендации в области

стандартизации (РС БР ИББС): 2.0-2007, 2.1-2007, 2.2-2009, 2.5-2014, 2.6-2014, 2.7-2015, 2.8-2015, 2.9-2016.

3. ГОСТы: ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018.

Примерная структура

1. Формы повышения осведомленности: вводный (первичный) инструктаж, целевой (внеплановый) инструктаж, специальное обучение.

2. Формы проведения: индивидуальное, групповое, внутреннее и внешнее.

3. Организация повышения осведомленности и проверки знаний.

4. Макет теста для проверки знаний по вопросам ИБ (приложение).

5. Личная карточка (приложение).

На что обратить внимание

Необходимо:

1. Разрабатывать и утверждать годовые планы по всем формам проведения: в какое время (число, месяц) проводить повышение осведомленности для каждого структурного подразделения банка.

2. Разрабатывать/изменять планы повышения осведомленности по всем формам проведения (список внутренних документов и др.).

3. Разрабатывать и утверждать годовые планы проверок знаний по информационной безопасности (период проведения и др.).

Положение об организации и обеспечении информационной безопасности хранения, обработки и передачи по каналам связи информации с использованием СКЗИ

Законодательная база

1. Федеральные законы: 63-ФЗ, 161-ФЗ.

2. Постановление Правительства РФ: 313.

3. Приказ ФАПСИ России: 152.

4. Приказ ФСБ России: 66 (Положение ПКЗ-2005).

5. Положения Банка России: 683-П, 716-П, 719-П, 787-П, 802-П.

6. Стандарты Банка России (СТО БР ИББС): 1.0-2014, 1.1-2007, 1.2-2014, 1.3-2016, 1.4-2018, СТО БР БФБО: 1.5-2018, рекомендации в области стандартизации (РС БР ИББС): 2.0-2007, 2.1-2007, 2.2-2009, 2.5-2014, 2.6-2014, 2.7-2015, 2.8-2015, 2.9-2016.

7. ГОСТы: ГОСТ Р 57580.1-2017, ГОСТ Р 57580.2-2018.

Александр ВИНОГРАДОВ
Анастасия НИКОЛАЕВА

Примерная структура

1. Виды и принципы использования электронной подписи.
2. Порядок работы с СКЗИ (генерация и регистрация, смена криптографических ключей при компрометации или подозрении на компрометацию, проведение технической экспертизы при разрешении конфликтных ситуаций и др.).
3. Требования к обеспечению информационной безопасности при использовании СКЗИ: организационному обеспечению безопасности СКЗИ, размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ; требования к сотрудникам, осуществляющим эксплуатацию и установку (инсталляцию) СКЗИ, и др.
4. Организация эксплуатации СКЗИ в банке: ввод в эксплуатацию, эксплуатация, вывод из эксплуатации, контроль за эксплуатацией и др.
5. Права и обязанности участников эксплуатации СКЗИ (описываются все структурные подразделения, которые участвуют в процессе).
6. Акт (макет) ввода СКЗИ в эксплуатацию (приложение).
7. Формуляр (макет) рабочего места СКЗИ (приложение).
8. Журнал (макет) поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложение).
9. Лицевой счет (макет) сотрудника (приложение).
10. Акт (макет) вывода СКЗИ из эксплуатации (приложение).
11. Акт (макет) об уничтожении ключевой информации (приложение).
12. Инструкция по работе на рабочих местах, на которых эксплуатируются СКЗИ (приложение).

В следующих номерах мы рассмотрим документы более низкого уровня, касающиеся доступа, инцидентов, сети (средства защиты, выделение контуров, доступные сайты и др.).