УТВЕРЖДЕНО
решением Правления
ПАО АКБ «Связь-Банк»
Протокол № 113
от 23 декабря 2014 г.

Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных в ПАО АКБ «Связь-Банк»

город Москва
2014

Оглавление

1. Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных в ПАО АКБ «Связь-Банк» (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных, обрабатываемых с использованием средств автоматизации, в ПАО АКБ «Связь-Банк» (далее – Банк).

1.2. Настоящее Положение не распространяется на отношения, возникающие при:

- организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну

1.3. Настоящее Положение разработано в соответствии со следующими нормативными документами:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС-1.0.2014.

2. Термины и определения

Банк – ПАО АКБ «Связь-Банк».

Персональные данные (ПДн) – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и(или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Источник угрозы безопасности персональных данных – объект или субъект, реализующий угрозы безопасности персональных данных путем воздействия на объекты среды обработки персональных данных Банка.

Объект среды обработки персональных данных – материальный объект среды хранения, передачи, обработки, уничтожения и т.д. персональных данных.

Оценка риска нарушения безопасности персональных данных – систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения безопасности персональных данных, обрабатываемых в Банке.

Риск нарушения безопасности персональных данных – риск, связанный с угрозой безопасности персональных данных.

Угроза безопасности персональных данных – угроза нарушения свойств безопасности персональных данных – доступности, целостности или конфиденциальности персональных данных.

3. Цель Положения

3.1. Целью данного Положения является организация мероприятий по защите персональных данных (далее – ПДн) и приведение существующих информационных систем персональных данных (далее – ИСПДн) Банка в соответствие с предъявляемыми требованиями по информационной безопасности.

3.2. Мероприятия по защите ПДн, отнесенных к конфиденциальной информации Банка, являются неотъемлемой составной частью деятельности Банка.

3.3. Требования положений настоящего документа должны учитываться разработчиком на всех стадиях жизненного цикла (техническое задание, проектирование, создание и тестирование, приемка и ввод в действие, эксплуатация, модернизация, снятие с эксплуатации) автоматизированных банковских систем (далее – АБС), отнесенных к ИСПДн Банка, путем прямого включения требований в соответствующие проектные и рабочие документы.

3.4. Требования по обеспечению безопасности персональных данных при их обработке в ИСПДн и перечень необходимых мер защиты определяются дифференцированно по результатам классификации ИСПДн в Банке, а также по результатам оценки рисков нарушения безопасности персональных данных.

4. Объекты защиты

4.1. В Банке подлежат защите автоматизированные системы (далее – АС), локальные вычислительные сети (ЛВС), средства и системы связи и передачи информации, другие технические средства, используемые в рамках банковского платежного технологического процесса, в которых обрабатываются персональные данные.

4.2. Защита ПДн в Банке обеспечивается выполнением комплекса организационных, технологических, технических и программных мер, средств, и механизмов защиты информации от несанкционированного доступа, программно-технических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также обеспечения работоспособности

технических средств.

4.3. Угрозы утечки персональных данных по техническим каналам[1] являются для Банка неактуальными.

5. Ответственные за защиту ПДн в Банке

5.1. Организация выполнения и (или) реализации требований по обеспечению безопасности персональных данных возлагается на Департамент безопасности ПАО АКБ «Связь-Банк».

5.2. Должностные лица подразделений Банка, в обязанность которых входит обработка ПДн, обязаны обеспечить каждому субъекту ПДн возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законодательством Российской Федерации.

5.3. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению информационной безопасности (далее – ИБ) ИСПДн Банка, возлагаются приказами (распоряжениями) на администраторов информационной безопасности ИСПДн.

5.4. Настоящее Положение является обязательным для исполнения всеми работниками, ответственными за защиту ПДн.

6. Нормативно-методическая документация

При организации и проведении работ по обеспечению безопасности ПДн необходимо руководствоваться следующими нормативными и методическими документами:

- Конституцией Российской Федерации;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС-1.0.2014.
- Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622).

7. Организация работ по обеспечению безопасности ПДн

7.1. Организационные меры по защите ПДн в Банке включают в себя следующие мероприятия:

- Определение лиц, подразделений, ответственных за защиту информации в Банке;
- Определение перечня ПДн, обрабатываемых в Банке;
- Определение целей обработки ПДн;
- Определение сроков обработки и хранения ПДн;

[1] Технический канал утечки информации – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

- Определение круга лиц, допущенных к обработке ПДн;
- Организация доступа в помещения, где осуществляется обработка ПДн;
- Обучение и повышение осведомленности работников, допущенных к обработке ПДн, в области обеспечения информационной безопасности в Банке;
- Учет применяемых технических средств защиты ПДн;
- Учет носителей ПДн;
- Разработка нормативных и организационно-распорядительных документов (далее — ОРД).

7.2. Ответственность за организацию работ по обеспечению безопасности и защиты ПДн, внесение соответствующих изменений в существующие положения о структурных подразделениях, разработку и утверждение должностных инструкций работников, отвечающих за защиту ПДн, возлагается на Департамент безопасности.

7.3. В рамках настоящего Положения к защищаемой информации относится документированная конфиденциальная информация, обрабатываемая в Банке, созданная в Банке или полученная от юридических или физических лиц на законных основаниях.

7.4. В Банке обрабатываются персональные данные, определяемые в соответствии с Перечнем сведений ограниченного распространения, составляющих конфиденциальную информацию ПАО АКБ «Связь-Банк».

7.5. Цели обработки персональных данных в Банке определяются на основании Положения об обработке персональных данных в ПАО АКБ «Связь-Банк».

7.6. Сроки хранения и обработки информации, содержащей ПДн субъектов, определяются в соответствии с Положением об обработке персональных данных в ПАО АКБ «Связь-Банк» в действующей редакции.

7.7. По истечении срока хранения и обработки информации, содержащей ПДн субъектов, данная информация должна быть уничтожена (обезличена).

7.8. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются.

8. Определение круга лиц, допущенных к обработке ПДн

8.1. Круг лиц, допущенных к обработке ПДн, определяется каждым руководителем самостоятельного (структурного) подразделения (либо руководителем филиала Банка), в котором обрабатываются ПДн. Перечень подразделений и работников, допущенных к работе с персональными данными, обрабатываемыми в Банке, ведется в виде электронного реестра согласованных заявок «На доступ к ПДн» в базе данных «Заявки 2.0» в системе Lotus Notes / Domino на основании пп. 6.1.6 Положения об обработке персональных данных в ПАО АКБ «Связь-Банк» в действующей редакции.

8.2. Ответственность за определение круга лиц, допущенных к обработке ПДн, а также за формирование перечня категорий ПДн, к которым оформляется допуск, полностью несет руководитель самостоятельного (структурного) подразделения (в филиалах Банка – руководитель филиала либо лицо, его замещающее в соответствии с установленным порядком). С целью недопущения предоставления избыточного доступа к ПДн Перечень категорий ПДн, доступных каждому работнику в отдельности, формируется исходя из принципа минимума полномочий, необходимых для выполнения работником непосредственных трудовых обязанностей.

8.3. Все лица, допущенные к обработке ПДн, должны быть ознакомлены с нормативной и организационно-распорядительной документацией по обработке и защите ПДн в Банке.

8.4. В должностные инструкции работников, принимающих участие в обработке ПДн, включается раздел об ответственности за обеспечение информационной безопасности ПДн[2].

[2] Требования к содержанию раздела должностной инструкции об ответственности за обеспечение информационной безопасности ПДн приведены в Приложении №1 к настоящему Положению

9. Организация доступа в помещения, где осуществляется обработка ПДн

9.1. В соответствии с действующими нормативными и организационно-распорядительными документами Банка определяется порядок доступа в помещения, в которых размещаются технические средства ИСПДн и хранятся носители персональных данных, предусматривающий контроль доступа в помещения и наличие препятствий для несанкционированного проникновения в помещения.

9.2. Указанный в п. 9.1 настоящего Положения порядок определен в Инструкции о пропускном и внутриобъектовом режимах на объектах ОАО АКБ «Связь-Банк» в г. Москве. В филиалах Банка разрабатывается аналогичный внутренний порядок в соответствии с указанной Инструкцией и настоящим Положением, согласовывается с Отделом защиты объектов Банка Департамента безопасности и Отделом защиты информации Департамента безопасности и утверждается управляющим филиала.

9.3. Перечень лиц, допущенных в помещение (серверную комнату), где располагаются серверы и телекоммуникационное оборудование, согласовывается в обязательном порядке с Департаментом безопасности.

9.4. В целях обеспечения ограниченного доступа в серверную комнату входная дверь должна быть снабжена функцией автоматической системы контроля доступа. В случае если установка данной системы невозможна, необходимо регистрировать вход/выход работников в соответствии с перечнем лиц, допущенных в серверное помещение.

9.5. Должна осуществляться физическая охрана помещений информационных систем персональных данных. В случае размещения объектов информационной инфраструктуры Банка на арендованных площадях физическая охрана помещений может обеспечиваться как на уровне только помещений Банка[3], так и на уровне всего объекта силами управляющего объектом.

9.6. Доступ в помещения, где обрабатываются ПДн, лицам, не допущенным к обработке ПДн, запрещен. В случае необходимости обеспечения доступа в помещения лицам, не допущенным к обработке ПДн (например, для уборки, технического обслуживания помещения), доступ осуществляется в присутствии работников, размещающихся в указанном помещении, а также необходимо исключить возможность несанкционированного доступа к техническим средствам обработки ПДн и носителям информации, содержащим ПДн.

10. Обучение работников Банка

10.1. Подразделение, ответственное за защиту ПДн, проводит обучение работников, использующих средства защиты информации, применяемые в ИСПДн, правилам работы с данными средствами не реже одного раза в год. Также проводится инструктаж работников Банка, допущенных к обработке ПДн, по правилам обработки ПДн в соответствии с утвержденными требованиями законодательства Российской Федерации, нормативных документов Банка России и Положения об обработке персональных данных в ПАО АКБ «Связь-Банк».

10.2. Ответственным подразделением за подготовку материалов обучения в области обеспечения безопасности ПДн и за сбор необходимых для этого данных является Департамент безопасности.

10.3. Ответственность за организацию обучения работников Банка возлагается на Департамент персонала.

[3] Отдельно регламентированный Банком пропускной режим, обеспечиваемый силами подрядного охранного предприятия.

11. Общие требования по обеспечению безопасности банковских технологических процессов, в рамках которых обрабатываются ПДн

11.1. Обеспечение требуемых функций и мер системы информационной безопасности банковского платежного и информационного технологических процессов, в рамках которых обрабатываются персональные данные (а также персональные данные вне ИСПДн), должно соответствовать всем требованиям Политики информационной безопасности ПАО АКБ «Связь-Банк» и требованиям настоящего Положения.

12. Общие требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн

12.1. Создание ИСПДн Банка включает разработку и согласование (утверждение) предусмотренной техническим заданием организационно-распорядительной, проектной и эксплуатационной документации на создаваемую систему. В документации должны быть отражены вопросы обеспечения безопасности обрабатываемых персональных данных.

12.2. Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн осуществляется по согласованию и под контролем Департамента безопасности в соответствии с Положением по использованию информационных ресурсов ОАО АКБ «Связь-Банк» в действующей редакции.

12.3. Все информационные активы, принадлежащие ИСПДн, защищаются от воздействий вредоносного кода (компьютерных вирусов, троянских коней, червей и т.д.) средствами антивирусной защиты в соответствии с Положением об организации антивирусной защиты в автоматизированной системе ПАО АКБ «Связь-Банк» в действующей редакции.

12.4. Департаментом безопасности определяется система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн.

12.5. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений Банка обеспечивают безопасность персональных данных при их обработке в ИСПДн.

12.6. Работники, осуществляющие обработку персональных данных в ИСПДн, действуют в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдают требования внутренних нормативных и организационно-распорядительных документов Банка по обеспечению информационной безопасности.

12.7. Порядок действий администратора информационной безопасности ИСПДн и персонала, занятого в процессе обработки персональных данных, определяется инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн.

Указанные инструкции (руководства):

- Устанавливают требования к квалификации администратора информационной безопасности и персонала в области защиты информации, а также актуальный перечень защищаемых объектов и правила его обновления;
- Содержат в полном объеме актуальные (по времени) данные о возможных полномочиях пользователей в системе;
- Содержат данные о технологии обработки информации в объеме, необходимом для администратора информационной безопасности;
- Устанавливают порядок и периодичность анализа журналов регистрации событий (архивов журналов);
- Регламентируют другие действия администратора информационной безопасности и персонала, предусмотренные настоящим Положением.

12.8. Параметры конфигурации средств защиты и механизмов защиты информации от

несанкционированного доступа, используемых в зоне ответственности администратора информационной безопасности, определяются в эксплуатационной документации на ИСПДн. Порядок и периодичность проверок установленных параметров конфигурации устанавливаются в эксплуатационной документации, при условии, что проверки должны проводиться не реже чем раз в год.

12.9. Организационно-техническими мерами должно быть запрещено несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки.

13. Требования по обеспечению безопасности ПДн, обрабатываемых в информационных системах обработки общедоступных и (или) обезличенных персональных данных

13.1. Для информационных систем обработки общедоступных и (или) обезличенных персональных данных применяются все требования по обеспечению безопасности, определенные в разделе 5 настоящего Положения, а также следующие требования.

- Процессы обработки персональных данных, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются разработчиком ИСПДн в проектной и эксплуатационной документации.
- Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечивается по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов.
- При наличии технической возможности количество последовательных неудачных попыток ввода пароля должно быть ограничено – не более 5 попыток. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности.
- Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком ИСПДн в эксплуатационной документации в инструкциях (руководствах) администраторов информационной безопасности.
- Передача персональных данных осуществляется только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию с Департаментом безопасности.

14. Требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн

14.1. Для информационных систем обработки персональных данных применяются все требования по обеспечению безопасности, определенные в разделах 12 и 13 настоящего Положения, а также выполнение функций обеспечения безопасности персональных данных в ИСПДн обеспечивается средствами защиты информации, прошедшими в установленном порядке процедуру оценки соответствия (сертификации на соответствие требованиям по безопасности информации), а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО).

14.2. На стадии ввода в действие разработчиком ИСПДн выполняются настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий.

Разработчиком ИСПДн определяется порядок постоянного контроля фактического

состояния указанных настроек на предмет их соответствия установленным правилам.

Указанный порядок должен согласовывается с Департаментом безопасности.

14.3. Регистрация входа в ИСПДн (выхода из ИСПДн) субъекта доступа является обязательной.

В журнале регистрации событий, который ведется в электронном виде в ИСПДн, указываются следующие параметры:

- Дата и время входа в систему (выхода из системы) субъекта доступа;
- Идентификатор субъекта, предъявленный при запросе доступа;
- Результат попытки входа: успешная или неуспешная (несанкционированная);
- Идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

14.4. В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журнале регистрации событий, указанном в пункте 14.4 настоящего Положения.

14.5. Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив.

14.6. Операция по архивированию журнала регистрации событий, в свою очередь, регистрируется с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

14.7. Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

14.8. В Банке определяется и документально фиксируется порядок постановки на учет и снятия с учета машинных носителей, предназначенных для размещения персональных данных.

14.9. Снятие с учета машинных носителей, на которых были размещены персональные данные, производится по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения.

14.10. Процедура стирания информации регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн в зависимости от применяемого средства гарантированного стирания.

14.11. При наличии технической возможности осуществляется очистка освобождаемых областей памяти на носителях, ранее использованных для хранения персональных данных.

14.12. Состав и назначение программного обеспечения ИСПДн определяются и утверждаются документально в соответствии с Положением по использованию информационных ресурсов ОАО АКБ «Связь-Банк».

14.13. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, регламентируется и утверждается документально.

14.14. Эталонные копии ПО учитываются, доступ к ним регламентируется. Соответствующие регламенты в виде инструкций, руководств готовятся разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

14.15. Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

14.16. Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий, регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

14.17. Восстановление функций обеспечения безопасности персональных данных в ИСПДн в случае нештатной ситуации осуществляется администратором ИСПДн с обязательным привлечением администратора информационной безопасности ИСПДн. Процедура восстановления регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

14.18. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые обеспечивают выполнение следующих функций:

- Фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- Идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- Регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
- Возможность проверки (контроля) целостности программной и информационной частей средства межсетевого экранирования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);
- Фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- Восстановление свойств межсетевого экрана после сбоев и отказов оборудования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);
- Возможность проведения регламентного тестирования реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования).

15. Контроль за соблюдением информационной безопасности ПДн

15.1. Контроль за состоянием защиты информации и ПДн (далее — контроль) осуществляется с целью своевременного выявления и предотвращения утечки информации и ПДн, несанкционированного доступа к информации и ПДн, преднамеренных программно-технических воздействий на информацию и ПДн, а также хищения ПДн.

15.2. Контроль заключается в проверке выполнения требований законодательства Российской Федерации по вопросам защиты информации, решений Федеральной службы по техническому и экспортному контролю (ФСТЭК России), нормативных документов Банка России и внутренних нормативных и организационно-распорядительных документов Банка, а также в проведении регулярных самооценок и аудитов информационной безопасности, осуществляемых в соответствии с методическими рекомендациями Банка России.

15.3. Постоянный контроль за состоянием защиты информации и ПДн в Банке осуществляет Департамент безопасности.

15.4. Периодический контроль за деятельностью по защите информации и ПДн в Банке осуществляется Службой внутреннего контроля.

15.5. Контроль за эффективностью применяемых в Банке мер и средств защиты информации проводится в соответствии с требованиями эксплуатационной документации, других нормативных документов, но не реже одного раза в год.

16. Определение нарушений

16.1. Процесс обеспечения безопасности и защиты ПДн считается эффективным, если принимаемые меры соответствуют установленным в данном Положении и в других нормативных документах Банка требованиям или нормам.

16.2. Несоответствие мер установленным требованиям или нормам по обеспечению безопасности и защиты ПДн является нарушением.

16.3. При обнаружении нарушений руководители самостоятельных (структурных) подразделений в рамках своей компетенции обязаны принять необходимые меры по их устранению в соответствии с нормативной и организационно-распорядительной документацией Банка.

16.4. Контроль за устранением этих нарушений осуществляется Департаментом безопасности.

16.5. Разбирательство и составление заключений в обязательном порядке проводится Департаментом безопасности в случае выявления следующих фактов:

- Несоблюдение условий хранения носителей ПДн;
- Использование средств защиты информации, применение которых может привести к нарушению заданного уровня безопасности (конфиденциальность, целостность, доступность) ПДн или к снижению уровня защищенности ПДн;
- Нарушение заданного уровня безопасности ПДн (конфиденциальность, целостность, доступность).

16.6. По окончании разбирательства проводятся необходимые мероприятия по предотвращению повторения подобных нарушений.

17. Заключительные положения

17.1. Настоящее Положение вступает в силу с момента его утверждения Правлением Банка и действует до его отмены.

17.2. Изменения к настоящему Положению утверждаются Правлением Банка.

17.3. Разработчиком и структурным подразделением, отвечающим за актуализацию настоящего Положения, является Департамент безопасности.

17.4. Если при изменении законодательства Российской Федерации отдельные статьи настоящего Положения вступают в противоречие с ним, то эти статьи утрачивают силу, и до момента внесения изменений в Положение работники Банка руководствуются действующим законодательством Российской Федерации. Факт прекращения действия одного или нескольких пунктов не влияет на действие настоящего Положения в целом.

17.5. С момента вступления в силу настоящего Положения считать утратившим силу Положение о порядке организации и проведения работ по обеспечению безопасности персональных данных в ОАО АКБ «Связь-Банк», утвержденное решением Правления Банка от 28.03.2011 (протокол № 20).

Приложение

Требования к разделу должностной инструкции об ответственности за обеспечение информационной безопасности ПДн

В содержание должностных инструкций работников Банка, имеющие доступ к сбору, обработке и хранению персональных данных работников, клиентов и посетителей Банка, в связи с осуществлением своих непосредственных функциональных обязанностей, должны быть включены следующие требования по обеспечению информационной безопасности ПДн:

- Не разглашать, не передавать и не раскрывать третьим лицам персональные данные работников Банка, а также персональные данные, содержащиеся в документах, в обращениях граждан и иных субъектов персональных данных, которые могут быть доверены (будут доверены) или стали (станут известными) в связи с выполнением должностных обязанностей.
- В случае попытки третьих лиц получить персональные данные работников, клиентов или посетителей Банка, а также персональные данные, содержащиеся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных, сообщать непосредственному руководителю. О фактах утраты или недостачи носителей персональных данных, удостоверений, пропусков, ключей от защищённых помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможной утечки сведений, немедленно сообщать своему непосредственному руководителю, а также работникам Отдела защиты информации Департамента безопасности, в филиале – Помощнику управляющего филиалом по безопасности (руководителю подразделения безопасности филиала).