УТВЕРЖДЕНО

Протокол Совета Директоров

№22/04/2014 от 22 апреля 2014 г.

Политика обеспечения безопасности персональных данных, обрабатываемых в ЗАО АКБ «РУНА-БАНК»

г. Москва

2014 г.

Оглавление

1. Общие положения

1.1. Политика обеспечения безопасности персональных данных, обрабатываемых в ЗАО АКБ «РУНА-БАНК», определяет требования к обеспечению безопасности персональных данных (ПДн), обрабатываемых в ЗАО АКБ «РУНА-БАНК».

1.2. Настоящая Политика разработана в соответствии с Политикой информационной безопасности ЗАО АКБ «РУНА-БАНК».

1.3. Термины, применяемые в настоящей Политике, трактуются в соответствии с определениями, представленными в Политике информационной безопасности ЗАО АКБ «РУНА-БАНК».

1.4. Настоящая Политика является документом публичного доступа и подлежит опубликованию на информационном сайте Банка.

2. Цели и задачи

2.1. Целями настоящей Политики являются:

- конфиденциальность персональных данных;
- целостность персональных данных;
- доступность персональных данных.

2.2. Задачами настоящей Политики являются:

- принятие правовых и организационных мер по обеспечению безопасности персональных данных (далее - ПДн);
- формулирование требований к применению технических средств, обеспечивающих принятые меры по обеспечению безопасности ПДн;
- осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн действующему законодательству и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике в отношении обработки персональных данных в ЗАО АКБ «РУНА-БАНК», локальным актам Банка;
- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения установленного порядка обработки ПДн, соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральными законами.
- определение требований к процессу управления доступом работников Банка к ПДн;
- определение требований к обеспечению физической безопасности материальных носителей ПДн;
- формирование требований к обеспечению безопасности ПДн для информационных систем персональных данных (далее - ИСПДн) каждого класса;
- определение ролей и распределение обязанностей и полномочий по обеспечению ИБ ПДн.

3. Область действия Политики

3.1. Требования настоящей Политики распространяются на все процессы обработки персональных данных в Банке.

3.2. Процедуры, требования к которым определяются настоящей Политикой, должны быть регламентированы. Структурные подразделения Банка, ответственные за выполнение процедур, требования к которым определяются настоящей Политикой, формируют регламенты процессов обработки ПДн и согласовывают их с лицом, ответственным за организацию обработки ПДн.

3.3. Выполнение процедур, требования к которым определяются настоящей Политикой, должно контролироваться лицом, ответственным за организацию обработки ПДн. Результаты контроля должны документироваться.

4. Принципы защиты персональных данных

4.1. Банк на основе Модели угроз нарушения безопасности персональных данных производит оценку рисков нарушения безопасности ПДн, включающую оценку вреда, который может быть причинен субъектам ПДн в случае реализации угрозы.

На основе принятой оценки рисков нарушения безопасности ПДн Банк формирует перечень организационных и правовых мер, снижающих риски нарушения безопасности ПДн до приемлемого уровня. Банк на основе перечня организационных мер снижения риска нарушения безопасности ПДн применяет технические средства защиты информации.

4.2. Банк обеспечивает безопасность ПДн применением следующих правовых и организационных мер:

1. определение угроз безопасности ПДн при их обработке в ИСПДн;
2. определение и применение организационных мер и технических средств обеспечения безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, устанавливаемых для различных классов ИСПДн;
3. применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
4. оценка эффективности принимаемых мер обеспечения безопасности ПДн до ввода ИСПДн в эксплуатацию;
5. учет машинных носителей персональных данных;
6. обнаружение фактов несанкционированного доступа к ПДн;
7. восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8. установление правил доступа к ПДн при их обработке в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
9. контроль за принимаемыми мерами обеспечения безопасности ПДн и уровня защищенности ИСПДн.

5. Предоставление доступа работников Банка к ПДн

5.1. Доступ к ПДн разрешается только специально уполномоченным лицам. Распределение полномочий ведется лицом, ответственным за организацию обработки ПДн, на ролевой основе. Перечень ролей, ПДн и прав доступа к ПДн оформляется документально.

5.2. Доступ работников Банка к ПДн и обработка ПДн работниками Банка должны осуществляться только для выполнения их должностных обязанностей.

5.3. Предоставление доступа работников Банка к ПДн должно оформляться документально в виде Перечня работников, осуществляющих обработку ПДн в ИСПДн либо имеющих доступ к ПДн. Перечень может быть представлен как в виде бумажного документа, так и в электронном виде.

5.4. Работники Банка, осуществляющие обработку ПДн в ИСПДн, должны быть уведомлены о факте обработки ими ПДн, категориях обрабатываемых ПДн.

5.5. Работники Банка должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

5.6. Все лица, получившие право обработки ПДн, обязаны заключить соглашение о неразглашении персональных данных.

5.7. Работники Банка, которым предоставлен доступ к ПДн и ИСПДн, должны получать и использовать только те ПДн, которые необходимы для выполнения конкретных технологических операций.

6. Обеспечение физической безопасности материальных носителей персональных данных

6.1. Доступ в помещения, в которых ведется обработка ПДн, размещаются технические средства ИСПДн или хранятся носители ПДн, определяется Порядком доступа в помещения ЗАО АКБ «РУНА-БАНК».

6.2. Все материальные носители ПДн подлежат поэкземплярному учету.

6.3. Ввод материального носителя ПДн в эксплуатацию проводится под контролем работника Банка, ответственного за организацию обработки ПДн.

6.4. Снятие с учета материальных носителей ПДн сопровождается стиранием средствами гарантированного стирания информации либо уничтожением носителя. Снятие с учета материального носителя ПДн должно проводиться под контролем Комиссии по уничтожению персональных данных, формируемой работником Банка, ответственным за организацию обработки ПДн. Комиссия по уничтожению персональных данных формируется из администратора безопасности ИСПДн, администратора ИСПДн и начальника службы безопасности.

6.5. Физический доступ к неотчуждаемым материальным носителям ПДн должен быть ограничен и контролироваться. Контроль доступа к несъемным материальным носителям ПДн осуществляет работник Банка, ответственный за организацию обработки ПДн в Банке. Физический доступ к отчуждаемым материальным носителям ПДн контролируется руководителем подразделения, использующего данный носитель.

6.6. При обработке в Банке ПДн на бумажных носителях должны соблюдаться следующие требования:

1. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).
2. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения

данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к этим носителям.

7. Общие требования к обеспечению безопасности персональных данных

7.1. СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2.

8. Информационные системы персональных данных (ИСПДн)

8.1. Общие подходы к защите персональных данных

8.1.1. Согласно п. 5.2.5 Политики в области обработки персональных данных ЗАО АКБ «РУНА-БАНК», выделяются следующие категории ИСПДн:

1. ИСПДн обработки специальных категорий ПДн (ИСПДн-С);
2. ИСПДн обработки биометрических ПДн (ИСПДн-Б);
3. ИСПДн обработки общедоступных и(или) обезличенных ПДн (ИСПДн-Д);
4. ИСПДН обработки ПДн, которые не могут быть отнесены к специальным категориям ПДн, биометрическим ПДн, общедоступным или обезличенным ПДн (ИСПДн-И).

8.1.2. Выбор требований к обеспечению безопасности ПДн в ИСПДн осуществляется в зависимости от результатов классификации ИСПДн.

8.2. Общие требования по обеспечению безопасности ПДн в ИСПДн любого класса

8.2.1. Требования к обеспечению безопасности персональных данных в ИСПДн реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

8.2.2. Организация выполнения требований по обеспечению безопасности персональных данных осуществляется лицом, ответственным за организацию обработки ПДн в Банке.

8.2.3. Выполнение требований по обеспечению безопасности ПДн осуществляется администратором безопасности ИСПДн либо на договорной основе организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации. Реализация требований к обеспечению безопасности ПДн в ИСПДн осуществляется по согласованию и под контролем лица, ответственного за организацию обработки ПДн в Банке.

8.2.4. Создание ИСПДн Банка должно включать 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. Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн должны осуществляться по согласованию и под контролем работника Банка, ответственного за организацию обработки ПДн.

8.2.5. Объекты информационной инфраструктуры, задействованные в функционировании ИСПДн Банка, должны быть защищены средствами обнаружения и предотвращения воздействия вредоносного кода.

8.2.6. Доступ к коммуникационным портам (COM, LPT, Firewire, USB, PCMCIA, eSATA, SCSI и другие, рассчитанные на подключение съемных носителей информации) и к накопителям на сменных носителях (floppy-дисководы, пишущие оптические приводы и др.) в системных блоках АРМ, участвующих в обработке ПДн при помощи ИСПДн, согласовывается с лицом, ответственным за организацию обработки ПДн, и контролируется.

8.2.7. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений Банка обеспечивают безопасность персональных данных при их обработке в ИСПДн. Работники, осуществляющие обработку персональных данных в ИСПДн, должны действовать в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдать требования настоящей Политики.

8.2.8. Обязанности по администрированию ИСПДн на всех стадиях жизненного цикла возлагаются на администратора ИСПДн.

8.2.9. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению безопасности ИСПДн, возлагаются на администратора безопасности ИСПДн.

8.2.10. ИСПДн должны быть снабжены эксплуатационной документацией, включающей в себя:

1. требования к квалификации администратора ИСПДн и администратора безопасности ИСПДн;
2. актуальный перечень защищаемых объектов и правила его обновления;
3. актуальные данные о полномочиях пользователей
4. данные о технологии обработки информации в объеме, необходимом для администратора безопасности ИСПДн;
5. порядок и периодичность анализа журналов регистрации событий (архивов журналов);
6. параметры конфигурации средств защиты и механизмов защиты информации от несанкционированного доступа;
7. порядок и периодичность проверок установленных параметров конфигурации средств защиты и механизмов защиты;
8. регламенты действий администраторов ИСПДн, администраторов безопасности ИСПДн и работников Банка, предусмотренные настоящей Политикой.

8.2.11. Пользователям и обслуживающему персоналу ИСПДн не разрешается осуществлять несанкционированное и(или) нерегистрируемое копирование, в том числе с использованием устройств фото- и видеосъемки.

8.3. Требования по обеспечению безопасности ПДн в ИСПДн-Д

8.3.1. ИСПДн-Д должны быть снабжены эксплуатационной документацией, включающей в себя:

1. процессы обработки ПДн
2. порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств
3. порядок формирования и смены паролей, а также контроля исполнения этих процедур

8.3.2. Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечиваются по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов.

8.3.3. При наличии технической возможности количество последовательных неудачных вводов пароля должно быть ограничено 5 попытками. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора безопасности ИСПДн.

8.3.4. Передача персональных данных должна осуществляться только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию с работником Банка, ответственным за организацию обработки ПДн.

8.4. Требования по обеспечению безопасности ПДн в ИСПДн-И

8.4.1. К обеспечению безопасности ПДн в ИСПДн-И применяются все требования, определенные в разделе 8.3, и дополнительные требования, предусмотренные настоящим разделом.

8.4.2. Выполнение функций обеспечения безопасности персональных данных в ИСПДн-И должно обеспечиваться специализированными средствами защиты информации, а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО).

8.4.3. На стадии ввода в действие разработчиком ИСПДн должны быть выполнены настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий.

8.4.4. ИСПДн-И должны быть снабжены эксплуатационной документацией, включающей в себя:

1. Порядок постоянного контроля фактического состояния настроек средств и механизмов защиты правилам, указанным в п. 8.4.3. Указанный порядок должен быть согласован с администратором безопасности ИСПДн.
2. Периодичность и порядок очистки журналов регистрации событий ИСПДн. Перед очисткой журналов событий должно выполняться архивирование журналов. Операция архивирования журнала должна регистрироваться в качестве первой записи в новом журнале регистрации событий.

3. Порядок внесения изменений в ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО.

4. Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий.

5. Порядок восстановления функций обеспечения безопасности ПДн в ИСПДн.

8.4.5. Регистрация входа в ИСПДн-И (выхода из ИСПДн) является обязательной. В журнале регистрации событий ИСПДн указываются следующие данные:

- дата и время входа в систему (выхода из системы) субъекта доступа;
- идентификатор субъекта, предъявленный при запросе доступа;
- результат попытки входа: успешная/неуспешная;
- IP-адрес компьютера, используемого для входа в систему.

8.4.6. Пользователи, разработчики и администраторы ИСПДн не должны иметь полномочий по уничтожению или модификации журнала регистрации событий ИСПДн.

8.4.7. Архивы журналов регистрации ИСПДн-И хранятся не менее 3 лет с даты создания архива.

8.4.8. Эталонные копии ПО ИСПДн-И подлежат учету. Учет ведется лицом, ответственным за организацию обработки персональных данных, в журнале, содержащем следующие данные:

- регистрационный номер
- дата постановки на учет

8.5.9. Хранение эталонных копий ПО ИСПДн осуществляется администратором ИСПДн на носителе однократной записи.

8.5.10. Резервному копированию подлежат все программные средства, архивы, журналы и данные, используемые и создаваемые в процессе эксплуатации ИСПДн. Резервное копирование производится администратором ИСПДн ежедневно. Резервные копии размещаются не менее чем в двух экземплярах на разных физических носителях информации.

8.5.11. Восстановление функций обеспечения безопасности ПДн в ИСПДн в случае нештатной ситуации осуществляется администратором безопасности ИСПДн под контролем лица, ответственного за организацию обработки ПДн. Процедура восстановления должна быть регламентирована разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

8.5.12. Подключение ИСПДн-И 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 и номеров портов, без учета состояния соединения);
- 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).

8.6. Требования по обеспечению безопасности ПДн в ИСПДн-Б

8.6.1. К обеспечению безопасности ПДн в ИСПДн-Б применяются все требования, определенные в разделе 8.4.

8.6.2. К обеспечению физической безопасности материальных носителей биометрических ПДн применяются все требования, определенные в разделе 6, и дополнительные требования, определенные настоящим разделом.

8.6.3. Материальный носитель ПДн должен обеспечивать:

1. защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;
2. возможность доступа уполномоченных сотрудников Банка к записанным на материальный носитель биометрическим персональным данным;
3. возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;
4. невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе

8.6.4. Материальный носитель ПДн должен использоваться не более срока эксплуатации, установленного изготовителем материального носителя.

8.6.5. Технологии хранения биометрических ПДн вне ИСПДн должны обеспечивать:

1. Применение криптографических средств или иных информационных технологий, позволяющих сохранить конфиденциальность, целостность и неизменность биометрических персональных данных, записанных на материальный носитель.
2. Проверку наличия письменного согласия субъекта ПДн на обработку его ПДн или наличия иных оснований обработки ПДн.

8.6.6. В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана электронной подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

8.6.7. При хранении биометрических ПДн вне ИСПДн должна обеспечиваться

регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из ИСПДн.

8.7. Требования по обеспечению безопасности ПДн в ИСПДн-С

8.7.1. К обеспечению безопасности ПДн в ИСПДн-С применяются все требования, определенные в разделе 8.4, и дополнительные требования, определенные настоящим разделом.

8.7.2. ИСПДн-С должны быть снабжены эксплуатационной документацией, включающей в себя параметры настроек технических и программных средств, обеспечивающих изоляцию сегментов локальной вычислительной сети (далее - ЛВС), задействованных в обработке ПДн, от других сегментов ЛВС и сети Интернет.

8.7.3. Идентификация информационных ресурсов (например, информационных массивов, баз данных, файлов, обрабатывающих их программ), содержащих персональные данные, должна осуществляться по логическим именам.

8.7.4. Контроль доступа субъектов к защищаемым информационным ресурсам в соответствии с правами доступа указанных субъектов является обязательным.

8.7.5. Регистрация печати материалов, содержащих персональные данные, является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

- дата и время печати;
- спецификация устройства печати (логическое имя (номер) внешнего устройства);
- полное наименование (вид, шифр, код) материала;
- идентификатор субъекта доступа, запросившего печать материала;
- объем фактически отпечатанного материала (количество страниц, листов, копий) и результат печати: успешная (весь объем) или неуспешная.

8.7.6. Регистрация запуска программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам, является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат попытки запуска: успешная или неуспешная (несанкционированная);
- дата и время попытки доступа к защищаемому информационному ресурсу;
- имя (идентификатор) защищаемого информационного ресурса;
- вид запрашиваемой операции (например, чтение, запись, модификация, удаление);
- результат попытки доступа: успешная или неуспешная (несанкционированная).

8.7.7. Регистрация изменений полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов) является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

- дата и время изменения;
- содержание изменения с указанием идентификатора субъекта доступа, чьи

полномочия подверглись изменению, или логического имени защищаемого информационного ресурса, чей статус изменился;

- идентификатор администратора информационной безопасности, осуществившего изменение.

8.7.8. Пользователи, разработчики и администраторы ИСПДн не должны иметь полномочий по уничтожению или модификации журналов регистрации событий ИСПДн, указанных в пп. 8.7.5, 8.7.6 и 8.7.7.

8.7.9. С целью недопущения изменения состава ПО ИСПДн, комплекс средств автоматизации которой представляет собой автономное, изолированное на физическом уровне в соответствии с эталонной моделью взаимодействия открытых систем — моделью OSI, автоматизированное рабочее место (АРМ) работника или работников, из ПО должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно аппаратного обеспечения). Если стандартные программные средства общего назначения не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО, допускается использование этих программных средств при условии, что документально введен запрет использования отдельных их компонент (средств разработки и отладки ПО).

8.7.10. В ИСПДн, комплекс средств автоматизации которой включает одно или несколько сетевых АРМ, сетевого оборудования и серверов, технические и программные средства, предназначенные для разработки и отладки ПО либо содержащие средства разработки, отладки и тестирования программно аппаратного обеспечения, должны располагаться в сегментах ЛВС, изолированных (на уровне не выше сетевого в соответствии с эталонной моделью взаимодействия открытых систем — моделью OSI) от сегментов, задействованных в обработке персональных данных. Стандартные программные средства общего назначения (например, MS Office), которые не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО, могут быть использованы в сегментах, задействованных в обработке персональных данных, при условии, что документально введен запрет использования отдельных их компонент (средств разработки и отладки ПО).

8.7.11. Передача ПДн между подразделениями Банка по телекоммуникационным каналам и линиям связи, не принадлежащим Банку или не пролегающим только по территории Банка, должна осуществляться только при обеспечении их защиты с помощью организации виртуальных частных сетей (Virtual Private Network — VPN) или иных защитных мер, механизмов и средств, применение которых согласовывается с администратором безопасности ИСПДн.

8.7.12. Передача ПДн по телекоммуникационным каналам и линиям связи между подразделениями Банка, с одной стороны, и внешними организациями, с другой стороны, должна осуществляться с использованием сертифицированных средств криптографической защиты или иных защитных механизмов, применение которых определяется администратором безопасности ИСПДн. В случае использования СКЗИ должны быть выполнены требования нормативных правовых актов ФСБ России. В случае обмена информацией с другой организацией правила использования СКЗИ должны быть определены соглашением сторон, в частности, условиями договора. При отсутствии указанной технической возможности передача персональных данных в электронном виде осуществляется на магнитных и других съемных носителях. Порядок такой передачи должен быть согласован с работником Банка, ответственным за организацию обработки ПДн.

8.7.13. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов),

которые должны иметь подтвержденный сертификатом класс защиты не ниже четвертого при возможности информационного обмена между всеми компонентами защищаемой ИСПДн без использования компонентов других автоматизированных банковских систем организации БС РФ (в иных случаях — не ниже третьего класса). Указанные классы защиты устанавливаются в соответствии с руководящим документом “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”, утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 года.

9. Обязанности и полномочия

9.1. В целях выполнения требований настоящей Политики выделяются следующие роли:

1. Разработчик ИСПДн - физические или юридические лица, создавшие программы, входящие в состав ИСПДн, а также сотрудники Банка, осуществляющие внедрение ИСПДн.

2. Комиссия по уничтожению персональных данных - сотрудники Банка, на которых решением работника Банка, ответственного за организацию обработки ПДн, возложена обязанность подтверждения уничтожения персональных данных.

3. Администратор ИСПДн — работник Банка, ответственный за техническую реализацию ИСПДн.

4. Администратор безопасности ИСПДн — работник Банка, ответственный за техническую реализацию средств обеспечения безопасности ИСПДн.

9.2. Разработчик ИСПДн:

- разрабатывает эксплуатационную документацию ИСПДн согласно п. 8.2.10 (подпункты 1,4,5,7), 8.3.1, 8.4.4

9.3. Работник Банка, ответственный за организацию обработки ПДн:

- ведет поэкземплярный учет материальных носителей ПДн;
- ведет поэкземплярный учет эталонных копий ПО ИСПДн;
- контролирует ввод в эксплуатацию материального носителя ПДн и снятие его с эксплуатации;
- организует уничтожение материальных носителей ПДн;
- контролирует выполнение требований настоящей Политики.

9.4. Администратор ИСПДн

- при недостаточном уровне документирования со стороны разработчика ИСПДн - разрабатывает (дополняет) эксплуатационную документацию согласно п. 8.2.10 (подпункты 1,4), 8.3.1, 8.4.4;
- формирует концепции и технические задания на ИСПДн;
- осуществляет проектирование, создание и тестирование внедряемой ИСПДн;
- администрирует ИСПДн на всех стадиях жизненного цикла;
- осуществляет ввод в эксплуатацию материального носителя ПДн и снятие его с эксплуатации;
- хранит эталонные копии ПО ИСПДн на носителе однократной записи;
- организует и проводит регулярное резервное копирование в соответствии с п.

8.5.10;

- производит восстановление функций обеспечения безопасности ПДн в ИСПДн.

9.5. Администратор безопасности ИСПДн

- производит архивирование и хранение архивов журналов регистрации событий ИСПДн;
- контролирует физический доступ к коммуникационным портам АРМ, обрабатывающих ПДн при помощи ИСПДн;
- контролирует физический доступ к неотчуждаемым материальным носителям ПДн;
- администрирует средства защиты и механизмы защиты, реализующие требования по обеспечению ИБ ИСПДн;
- разрабатывает эксплуатационную документацию ИСПДн согласно п. 8.2.10 (подпункты 2,3,5,6,7,8).

9.6. Служба безопасности:

- осуществляет контроль доступа в помещения, в которых ведется обработка ПДн и(или) хранятся носители ПДн.

9.7. Комиссия по уничтожению персональных данных:

- документально фиксирует факт уничтожения материального носителя ПДн.

9.8. Руководители структурных подразделений, эксплуатирующих или обслуживающих ИСПДн:

- обеспечивают безопасность персональных данных при их обработке в ИСПДн.

10. Пересмотр Политики

10.1. Настоящая Политика подлежит пересмотру по решению работника Банка, ответственного за организацию обработки ПДн, а также при изменении:

- законодательства РФ;
- нормативных актов Банка России;
- Политики информационной безопасности ЗАО АКБ «РУНА-БАНК»;
- Порядка проведения классификации автоматизированных банковских систем ЗАО АКБ «РУНА-БАНК», содержащих персональные данные.