УТВЕРЖДЕНО
Советом директоров АО "РУНА-БАНК"
(протокол №21/09/2017 от «21» сентября 2017 г.)
Председатель Совета Директоров

_____С.А.Борисов

Политика АО «РУНА-БАНК» в отношении обработки персональных данных

г. Москва

2017 г.

Оглавление

1. Общие положения

1.1. Политика АО «РУНА-БАНК» в отношении обработки персональных данных разработана с целью защиты информации, относящейся к личности и личной жизни физических лиц, и определяет порядок получения, обработки, хранения, передачи, защиты и уничтожения персональных данных в АО «РУНА-БАНК».

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

1.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.4. Термины, применяемые в настоящей Политике, трактуются в соответствии с определениями, представленными в Политике информационной безопасности АО «РУНА-БАНК».

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

2. Цели и задачи

2.1. Настоящая Политика разработана с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных (далее - ПДн), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

2.2. Задачами настоящей Политики являются:

- определение принципов, условий и целей обработки ПДн в Банке;
- определение порядка и проведение классификации ПДн;
- определение порядка и проведение классификации информационных систем персональных данных (далее - ИСПДн);
- формулирование требований к материальным носителям ПДн и к типовым формам документов;
- определение требований к процессам обработки ПДн;
- права субъектов ПДн;
- определение порядка работы с обращениями субъектов ПДн;
- определение порядка взаимодействия Банка с третьими лицами и Уполномоченным органом по защите персональных данных.

3. Область действия документа

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.

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

4. Общие принципы, условия и цели обработки ПДн

4.1. Для упорядочения процесса обработки ПДн Банк назначает лицо, ответственное за организацию обработки ПДн.

4.2. В отношении персональных данных Банк руководствуется следующими принципами:

1. обработка ПДн должна осуществляться на законной и справедливой основе;
2. обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей;
3. обработка ПДн должна быть совместима с целями сбора ПДн;
4. обработке подлежат только те ПДн, которые отвечают целям их обработки;
5. содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки;
6. обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;
7. при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн;
8. не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в несовместимых между собой целях;
9. хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
10. обрабатываемые Банком ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не установлено федеральным законом;

11. при обработке ПДн должна быть обеспечена защита ПДн, которая осуществляется в соответствии с Политикой обеспечения безопасности персональных данных, обрабатываемых в АО «РУНА-БАНК».

4.3. Обработка Банком ПДн допускается в следующих случаях:

1. обработка осуществляется с согласия субъекта ПДн;
2. обработка ПДн необходима для достижения целей, предусмотренных законодательством Российской Федерации, для осуществления и выполнения возложенных на Банк функций, полномочий или обязанностей;
3. обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
4. обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
5. обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
6. обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
7. обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн;
8. осуществляется обработка общедоступных ПДн;
9. осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.4. Общими целями обработки ПДн Банком являются:

1. установление трудовых отношений с работниками Банка;
2. осуществление трудовых отношений с работниками Банка, содействие работникам Банка в трудоустройстве, обучении и продвижении по службе;
3. обеспечение личной безопасности работников Банка, контроля количества и качества выполняемой работы, обеспечение сохранности имущества;
4. осуществление банковских операций и иных сделок;
5. осуществление профессиональной деятельности на рынке ценных бумаг;

6. соблюдение норм действующего законодательства, в том числе в области противодействия (легализации) доходов, полученных преступным путем и финансированию терроризма, об акционерных обществах, о рынке ценных бумаг, о кредитных историях, о страховании вкладов физических лиц и т.д.;
7. соблюдение нормативных актов надзорных органов;
8. заключение и исполнение заключенных договоров;
9. продвижение товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи;
10. повышение доверия к Банку и доступности информации о Банке.

4.5. Объем и содержание ПДн, сроки обработки и необходимость получения согласия субъекта ПДн для каждой цели обработки приведены в Перечне персональных данных, обрабатываемых в АО «РУНА-БАНК». Обязанность по актуализации Перечня возлагается на лицо, ответственное за организацию обработки ПДн.

Совокупности ПДн, объединенные общими целями обработки (далее — ресурсы ПДн), обрабатываемые в Банке, подлежат учету. Для каждого ресурса ПДн должно быть обеспечено:

- установление цели обработки ПДн;
- установление и соблюдение сроков хранения ПДн и условий прекращения их обработки;
- определение перечня и категорий обрабатываемых ПДн;
- выполнение процедур учета количества субъектов ПДн;
- выполнение ограничения обработки ПДн достижением цели обработки ПДн;
- соответствие содержания и объема обрабатываемых ПДн установленным целям обработки ПДн;
- точность, достаточность и актуальность ПДн, в том числе по отношению к целям обработки ПДн;
- выполнение в случае необходимости установленных процедур получения согласия субъектов ПДн (их законных представителей) на обработку их ПДн;
- прекращение в установленных законом случаях обработки ПДн и уничтожение либо обезличивание ПДн по достижении целей обработки, по требованию субъекта ПДн, в том числе при отзыве субъектом ПДн согласия на обработку его ПДн.

4.6. В случае необходимости обработки ПДн, не указанных в Перечне персональных данных, сотрудник Банка ставит в известность лицо, ответственное за организацию

обработки ПДн. Ответственный сотрудник в течение 5 рабочих дней с момента получения уведомления вносит персональные данные в Перечень и определяет правовые основы для обработки ПДн и необходимость уведомления субъекта ПДн.

4.7. Обработка ПДн осуществляется смешанным образом: неавтоматизированная обработка и обработка с использованием средств автоматизации.

4.8. Обработка ПДн с использованием средств автоматизации осуществляется в ИСПДн .

4.9. Запрещается использовать обрабатываемые ПДн:

- в целях причинения имущественного ущерба и морального вреда гражданам;
- в целях затруднения реализации гражданами РФ своих прав и свобод;
- в целях ограничения прав граждан РФ на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной деятельности.

4.10. Если предоставление ПДн является обязательным в соответствии с федеральным законом, Банк обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

4.11. Если ПДн получены не от субъекта ПДн, Банк, за исключением случаев, указанных в п. 4.12, предоставляет субъекту ПДн следующую информацию:

1. наименование и адрес Банка;
2. цель обработки ПДн и ее правовое основание;
3. предполагаемые пользователи ПДн;
4. права субъекта ПДн;
5. источник получения ПДн.

4.12. Банк не предоставляет субъекту ПДн уведомление о начале обработки его ПДн в следующих случаях:

1. субъект ПДн уведомлен об осуществлении обработки его ПДн;
2. ПДн получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;
3. ПДн сделаны общедоступными субъектом ПДн;
4. Банк осуществляет обработку ПДн для статистических или иных исследовательских целей, научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;
5. предоставление субъекту ПДн информации об обработке его ПДн нарушает права и

законные интересы третьих лиц.

4.13. Работники должны быть ознакомлены под роспись с документами Банка, устанавливающими порядок обработки персональных данных Работников, а также об их правах и обязанностях в этой области.

5. Классификация персональных данных и информационных систем

5.1. Классификация персональных данных

5.1.1. Все обрабатываемые Банке ПДн подразделяются на следующие категории:

- общедоступные или обезличенные;
- биометрические;
- специальные;
- ПДн, которые не могут быть отнесены к специальным, биометрическим или общедоступным.

5.1.2. Классификацию ПДн осуществляет Комиссия по классификации ПДн. Результаты классификации ПДн для каждой цели обработки оформляются в виде Перечня персональных данных, обрабатываемых в АО «РУНА-БАНК».

5.2. Классификация информационных систем

5.2.1. Классификацию автоматизированных информационных систем (далее - АИС), используемых Банком в технологических процессах, осуществляет Комиссия по классификации ПДн. Результаты классификации оформляются в виде Перечня информационных систем персональных данных АО «РУНА-БАНК».

5.2.2. Отнесение АИС к ИСПДн, критерии классификации ИСПДн и порядок проведения классификации ИСПДн определяются Порядком проведения классификации автоматизированных банковских систем АО «РУНА-БАНК», содержащих персональные данные. Результаты классификации документально фиксируются и утверждаются руководством Банка.

5.2.3. Состав и назначение программного обеспечения ИСПДн документально фиксируются в реестре информационных активов АО «РУНА-БАНК».

5.2.4. Классификация ИСПДн Банка проводятся на основании результатов моделирования угроз безопасности ПДн

5.2.6.

6. Требования к обработке отдельных типов и категорий ПДн

6.1. Специальные категории персональных данных

6.1.1. Обработка специальных категорий ПДн допускается в следующих случаях:

1. субъект ПДн дал согласие на обработку своих ПДн;
2. субъект ПДн сделал свои ПДн общедоступными;
3. обработка ПДн осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;
4. обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;
5. обработка ПДн необходима для установления или осуществления прав субъекта ПДн или третьих лиц, а равно и в связи с осуществлением правосудия;
6. обработка ПДн осуществляется в соответствии с законодательством Российской Федерации;
7. обработка ПДн осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

6.1.2. Обработка ПДн о судимости обрабатывается Банком в случаях и в порядке, которые определяются в соответствии с федеральными законами.

6.1.3. Обработка специальных категорий ПДн должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

6.2. Биометрические персональные данные

6.2.1. Биометрические ПДн, используемые Банком для установления личности субъекта ПДн, могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн.

6.3. Персональные данные работников Банка

6.3.1. Банк не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Банк вправе получать и обрабатывать данные о частной

жизни Работника только с его письменного согласия.

6.3.2. Банк не имеет права получать и обрабатывать персональные данные Работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

6.3.3. Принятие решений, затрагивающих интересы работников, не может быть основано на ПДн работника, полученных в результате их автоматизированной обработки или электронного получения.

6.3.4. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

6.3.5. Банк не должен запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

6.3.6. Не допускается обработка Банком информации о частной жизни работников Банка.

6.3.7. Общедоступные источники ПДн (в том числе справочники, адресные книги) создаются и публикуются Банком только для цели выполнения требования законодательства РФ. Для включения ПДн работников Банка в эти источники необходимо получение от таких работников письменного согласия на распространение ПДн. Создаваемые источники ПДн могут содержать:

1. фамилию, имя, отчество;
2. адрес корпоративной электронной почты;
3. внутренний телефонный номер;
4. должность и структурное подразделение.

7. Особенности обработки ПДн в ИСПДн

7.1. Банковские информационные технологические процессы, в рамках которых обрабатываются ПДн в ИСПДн, должны быть документированы.

8. Трансграничная передача персональных данных

8.1. Трансграничная передача ПДн на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн, осуществляется в соответствии с настоящей Политикой.

8.2. Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватную защиту прав субъектов ПДн, может осуществляться в следующих случаях:

1. наличие согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;
2. исполнение договора, стороной которого является субъект ПДн;
3. необходимость защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

9. Требования к материальным носителям ПДн

9.1. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

9.2. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10. Требования к типовым формам документов

10.1.1. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование Банка, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Банком способов обработки персональных данных.
2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных.
3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.
4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

11. Прекращение обработки ПДн

11.1. Банк уничтожает ПДн в следующих случаях:

1. при невозможности устранения нарушения, выраженного в совершении неправомерных действий с ПДн – в срок, не превышающий десяти рабочих дней, с даты выявления факта совершения неправомерных действий (в том числе и по требованию субъекта или Уполномоченного органа о том, что ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а устранение нарушения невозможно);
2. по достижении цели обработки в срок, не превышающий тридцати рабочих дней с даты достижения целей обработки, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн,

иным соглашением между Банком и субъектом ПДн, или федеральными законами;

3. при отзыве субъектом согласия на обработку ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами;
4. по требованию субъекта ПДн или Уполномоченного органа по защите прав субъектов ПДн - если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

11.2. Уничтожение или обезличивание ПДн организуется лицом, ответственным за организацию обработки ПДн, и документально фиксируется Комиссией по уничтожению персональных данных.

В случае отсутствия возможности уничтожения ПДн либо обезличивания ПДн в течение срока, установленного Федеральным законом «О персональных данных», Банк обеспечивает их блокирование с последующим уничтожением ПДн. Уничтожение ПДн должно быть произведено не позднее шести месяцев со дня их блокирования.

12. Права субъекта персональных данных

12.1. Субъект ПДн имеет право на получение в доступной форме информации, касающейся обработки его персональных данных, в том числе содержащей:

1. подтверждение факта обработки Банком ПДн;
2. правовые основания и цели обработки ПДн;
3. цели и применяемые Банком способы обработки ПДн;
4. наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Банком или на основании федерального закона;
5. обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6. любую запись, содержащую его ПДн;

7. сроки обработки ПДн, в том числе сроки их хранения;
8. порядок осуществления субъектом ПДн прав, предусмотренных федеральным законом;
9. информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
10. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;
11. иные сведения, предусмотренные федеральными законами.

12.2. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, если:

1. обработка Банком ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
2. доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

12.3. Субъект ПДн имеет право потребовать от Банка уточнение или изменение его ПДн.

12.4. Субъект ПДн имеет право потребовать от Банка уничтожить его ПДн в случае, если эти ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

12.5. Субъект ПДн имеет право определять своих представителей для защиты своих персональных данных.

13. Взаимодействие Банка с субъектами ПДн и с третьими лицами

13.1. Согласие субъекта ПДн на обработку его ПДн

13.1.1. Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Банком.

13.1.2. Согласие может быть отозвано субъектом ПДн. В случае отзыва субъектом

ПДн согласия на обработку ПДн Банк вправе продолжить обработку без согласия субъекта ПДн при наличии иных оснований.

13.1.3. Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн возлагается на Банк.

13.1.4. Согласие субъекта ПДн на обработку его ПДн, направленное в Банк в электронном виде, считается равнозначным согласию, представленному на бумажном носителе и подписанном собственноручной подписью субъекта ПДн, если оно подписано электронной подписью в соответствии с федеральным законом.

13.2. Обработка обращений субъектов ПДн

13.2.1. Субъекты ПДн либо их представители вправе обращаться в Банк с запросами на предоставление, уточнение, изменение или уничтожение их ПДн. Запросы должны направляться в Банк в письменном виде. Бланки запросов подлежат опубликованию на официальном сайте Банка. Запрос может быть представлен в форме электронного документа, подписанного электронной подписью в соответствии с законодательством РФ.

13.2.2. Запрос субъекта ПДн на получение информации об обработке его ПДн должен содержать следующие сведения:

1. номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
2. сведения, подтверждающие участие субъекта ПДн в отношениях с Банком;
3. подпись субъекта ПДн или его представителя.

13.2.3. Сведения, предоставляемые субъекту ПДн по его запросу, не должны содержать ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

13.2.4. Запрос субъекта ПДн на уточнение/изменение его ПДн должен содержать следующие сведения:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с Банком;
- подпись субъекта ПДн или его представителя.
- документы, подтверждающие изменение персональных данных.

13.2.5. Уточняемые или изменяемые ПДн подлежат немедленному блокированию на период проведения проверки обращения, если это не нарушает права и законные интересы субъекта ПДн или третьих лиц. Банк в срок, не превышающий 7 рабочих дней, вносит

необходимые изменения и уведомляет об этом субъекта ПДн.

13.2.6. Запрос субъекта ПДн на уничтожение его ПДн в случае, если эти ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, должен содержать:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с Банком;
- подпись субъекта ПДн или его представителя.
- документы, подтверждающие изменение персональных данных.

13.2.7. Такие ПДн подлежат немедленному блокированию на период проведения проверки обращения. В случае принятия положительного решения по обращению Банк в срок, не превышающий 7 рабочих дней, уничтожает такие ПДн и уведомляет об этом субъекта ПДн.

13.2.8. Субъект ПДн имеет право направить повторный запрос на предоставление информации об обработке его ПДн в следующих случаях:

1. если предоставленные сведения были предоставлены не в полном объеме (с обязательным обоснованием направления повторного запроса);
2. если с момента получения Банком предыдущего запроса прошло не менее тридцати дней.

13.2.9. Банк имеет право отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям. Такой отказ должен быть мотивированным.

13.3. Передача ПДн третьим лицам

13.3.1. Банк вправе поручить обработку ПДн другому лицу на основании заключаемого с этим лицом договора.

13.3.2. Договор, заключаемый с лицом, осуществляющим обработку ПДн по поручению Банка, должен содержать:

1. обязательство лица соблюдать принципы и правила обработки ПДн, предусмотренные настоящей Политикой;
2. обязательство лица выполнять требования, предусмотренные Политикой обеспечения безопасности персональных данных, обрабатываемых в АО «РУНА-БАНК»;
3. перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки;
4. ответственность лица перед Банком за действия, связанные с обработкой лицом ПДн.

13.3.3. Передача ПДн, в том числе обрабатываемых без согласия субъекта ПДн, третьим лицам осуществляется Банком только на основании письменного согласия субъекта ПДн на передачу, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных действующим законодательством.

13.3.4. Персональные данные работников Банка могут предоставляться:

1. уполномоченным органам в порядке, установленном разделом 15 настоящей Политики;
2. государственным и негосударственным структурам;
3. организациям, в которые работник Банка может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения);
4. другой организации - сведения о работающем или уволенном работнике Банка;
5. родственникам или членам семьи работника Банка.

13.3.5. Основанием для предоставления ПДн лицам, перечисленным в п. 11.2, является письменный запрос и письменное согласие работника на передачу персональных данных.

13.3.6. Третьи лица, получающие от Банка ПДн, должны использовать ПДн только в тех целях, для которых они сообщены, обеспечивать защиту полученных ПДн. Банк вправе требовать от третьих лиц подтверждение выполнения требований к защите ПДн. В том случае, если Банк поручает обработку ПДн третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности ПДн и безопасности ПДн при их обработке.

13.3.7. Персональные данные работника Банка, передаваемые представителям работников Банка, должны быть ограничены теми данными, которые необходимы для выполнения указанных представителем функций.

13.4. Взаимодействие с Уполномоченным органом по защите прав субъектов ПДн

13.4.1. Банк зарегистрирован в качестве оператора персональных данных. Регистрационный номер в «Реестре операторов, осуществляющих обработку персональных данных» - 11-0170731.

13.4.2. В случае изменения сведений, указанных в уведомлении об обработке персональных данных, Банк извещает Уполномоченный орган в течение десяти рабочих дней

с даты возникновения таких изменений.

13.4.3. Уполномоченный орган имеет право:

- запрашивать у Банка, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
- требовать от Банка уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований Закона о персональных данных;
- обращаться в суд с исковыми заявлениями в защиту прав субъектов ПДн, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов ПДн в суде;
- направлять в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, применительно к сфере их деятельности, сведения, указанные в пункте 7 части 3 статьи 22 Закона о персональных данных;
- направлять заявление в орган, осуществляющий лицензирование деятельности Банка, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу ПДн третьим лицам без согласия в письменной форме субъекта ПДн;
- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн, в соответствии с подведомственностью;
- привлекать к административной ответственности лиц, виновных в нарушении Закона о персональных данных.

13.4.4. Банк обязан сообщить в Уполномоченный орган или иные надзорных органы, осуществляющие контроль и надзор в области ПДн по их запросу необходимую информацию

в течение тридцати дней с даты получения такого запроса.

13.4.5. Банк по запросу обязан предоставить Уполномоченному органу документы и локальные акты, определяющие политику Банка в отношении обработки персональных данных.

14. Обязанности и полномочия

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

1. Лицо, ответственное за организацию обработки персональных данных — работник Банка, на которого приказом Председателя Правления Банка возложена обязанность по организации обработки персональных данных.
2. Комиссия по классификации персональных данных - работники Банка, на которых приказом Председателя Правления Банка возложена обязанность по классификации персональных данных.
3. Комиссия по уничтожению персональных данных — работники Банка, на которых решением работника Банка, ответственного за организацию обработки персональных данных, возложена обязанность подтверждения уничтожения персональных данных.
4. Лицо, ответственное за защиту персональных данных в ИСПДн — работник Банка, на которого приказом Председателя Правления Банка возложена обязанность по обеспечению защиты персональных данных в ИСПДн

14.2. Лицо, ответственное за организацию обработки персональных данных:

- контролирует выполнение требований настоящей Политики;
- производит пересмотр и актуализацию настоящей Политики;
- ведет Перечни ПДн и ИСПДн;
- ведет перечень работников, осуществляющих обработку ПДн в ИСПДн, либо имеющих доступ к ПДн;
- информирует работников Банка о факте обработки ими ПДн, категориях обрабатываемых ПДн;
- уведомляет субъектов ПДн о начале обработки их ПДн;
- производит ознакомление работников Банка под роспись со всей совокупностью требований по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей;
- формирует Комиссию по уничтожению персональных данных;
- организует уничтожение персональных данных и материальных носителей ПДн;

- обрабатывает обращения субъектов ПДн и Уполномоченных органов;
- опубликовывает настоящую Политику на официальном сайте Банка.

14.3. Комиссия по классификации персональных данных:

- проводит классификацию персональных данных;
- проводит классификацию АИС и отнесение их к ИСПДн.

14.4. Комиссия по уничтожению персональных данных:

- удостоверяет уничтожение персональных данных.

14.5. Ответственный за защиту персональных данных в ИСПДн:

- осуществляет применение организационных, организационно-технических и технических мер защиты персональных данных в ИСПДн.

Все работники Банка обязаны информировать работника Банка, ответственного за организацию обработки ПДн, и подразделения, обрабатывающие ПДн, о фактах разглашения и (или) неправомерного использования ПДн.

15. Обеспечение безопасности персональных данных

15.1. Принципы защиты персональных данных

Угрозы утечки персональных данных по техническим каналам, а также угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн, признаются неактуальными для Банка.

15.1.1 Банк оценивает угрозы нарушения безопасности персональных данных производит оценку рисков нарушения безопасности ПДн, включающую оценку вреда, который может быть причинен субъектам ПДн в случае реализации угрозы, и формирует Модель угроз безопасности персональных данных.

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.

15.1.2. 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;
10. установление порядка передачи ПДн между пользователями ресурса ПДн, предусматривающего передачу ПДн только между работниками Банка, имеющими доступ к ПДн.

Для выполнения требований к защите персональных данных для второго уровня защищенности ПДн при их обработке в ИСПДн должны применяться следующие меры:

1. в части обеспечения ИБ на стадиях жизненного цикла:
    1. определение, выполнение и регистрация процедур контроля целостности и обеспечения доверенной загрузки программного обеспечения;
    2. определение, выполнение, регистрация и контроль процедур доступа к эксплуатационной документации и архивным файлам, содержащим параметры настройки ИСПДн;
    3. определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления ПДн;
    4. определение, выполнение, регистрация и контроль процедур резервного копирования и обеспечения возможности восстановления программного обеспечения, входящего в состав ИСПДн;
2. в части обеспечения ИБ при управлении доступом и регистрации:
    1. идентификация и аутентификация устройств, используемых для осуществления доступа;
    2. размещение технических устройств, предназначенных для администрирования ИСПДн, автоматизированных мест пользователей и серверных компонент ИСПДн в отдельных выделенных сегментах вычислительной сети;
    3. мониторинг сетевого трафика, выявление вторжений и сетевых атак и реагирование на них;
    4. определение, выполнение, регистрация и контроль процедур обновления сигнатурных баз технических защитных мер;
3. в части обеспечения ИБ банковских информационных технологических процессов:
    1. определение, выполнение, регистрация и контроль процедур использования коммуникационных портов, устройств ввода-вывода информации, съемных машинных носителей и внешних накопителей информации;
    2. определение, выполнение, регистрация и контроль процедур доступа к архивам ПДн.

16. Предоставление доступа работников Банка к ПДн

16.1. 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.

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

16.3. 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.

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

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

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

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

17. Обеспечение физической безопасности материальных носителей персональных данных

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

17.2. Все материальные носители ПДн подлежат поэкземплярному учету.

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

17.4. 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.

17.5. 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.

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

- 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).
- 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.
- 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.
- Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
- При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к этим носителям.

18. Общие требования к обеспечению безопасности персональных данных

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

19. Информационные системы персональных данных (ИСПДн)

19.1. Общие подходы к защите персональных данных

19.1.1. Категорирование ИСПДн осуществляется по результатам определения перечня актуальных угроз безопасности ПДн и объема обрабатываемых данных.

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

19.2. Общие требования по обеспечению безопасности ПДн в ИСПДн

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

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

19.2.3. 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.

19.2.4. 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.

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

19.2.6. 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.

19.2.7. 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.

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

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

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

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

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

19.2.12. На стадии сопровождения (модернизации) ИСПДн должны быть определены, выполняться и регистрироваться процедуры:

- фиксации внесенных изменений;
- проверки функциональности ИСПДн, в том числе применяемых мер защиты информации.

Процедуры информационного взаимодействия ИСПДн с иными АБС должны быть регламентированы.

Для каждой ИСПДн должен быть назначен работник Банка, ответственный за обеспечение безопасности ПДн в ИСПДн.

19.2.13. ИСПДн 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

19.2.14. 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.

19.2.15. 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.

19.2.16. 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.

19.2.17. Выполнение функций обеспечения безопасности персональных данных в ИСПДн может обеспечиваться специализированными средствами защиты информации или комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО). Приоритет имеют встроенные механизмы защиты

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

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

- Порядок постоянного контроля фактического состояния настроек средств и механизмов защиты правилам, указанным в п. 8.2.18. Указанный порядок должен быть согласован с администратором безопасности ИСПДн.
- 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.

- Порядок внесения изменений в ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО.
- Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий.
- Порядок восстановления функций обеспечения безопасности ПДн в ИСПДн.

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

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

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

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

- регистрационный номер
- дата постановки на учет

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

19.2.24. 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.

19.2.25. 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.

19.2.26. Подключение ИСПДн 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).

20. Обязанности и полномочия

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

1. Разработчик ИСПДн - физические или юридические лица, создавшие ПО, входящее 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.

20.2. Разработчик ИСПДн:

- разрабатывает эксплуатационную документацию ИСПДн

20.3. 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.

20.4. Администратор ИСПДн

- при недостаточном уровне документирования со стороны разработчика ИСПДн - разрабатывает (дополняет) эксплуатационную документацию
- 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
- производит восстановление функций обеспечения безопасности ПДн в ИСПДн.

20.5. 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

20.6. Служба безопасности:

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

20.7. Комиссия по уничтожению персональных данных:

- документально фиксирует факт уничтожения материального носителя ПДн.

20.8. Руководители структурных подразделений, эксплуатирующих или обслуживающих ИСПДн:

- обеспечивают безопасность персональных данных при их обработке в ИСПДн.

21. Порядок пересмотра Политики

21.1. Настоящая Политика подлежит пересмотру в следующих случаях:

- при изменении законодательных актов РФ, регулирующих отношения в области персональных данных;
- трудового законодательства;
- при пересмотре положений Политики информационной безопасности Банка;
- по решению руководства Банка или работника Банка, ответственного за организацию обработки ПДн.