

ПОЛОЖЕНИЕ

об организации обработки персональных данных в Банке ВТБ (ПАО)

(ВЫПИСКА)

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение об организации обработки персональных данных в Банке ВТБ (ПАО) (далее – Положение) разработано в целях:

- организации обработки персональных данных (далее – ПДн) работников Банка ВТБ (ПАО) (далее – Банк) и иных субъектов ПДн, осуществляемой в рамках полномочий Банка как оператора ПДн, а также в случаях, когда обработка ПДн поручена Банку другим оператором ПДн, в соответствии с требованиями действующего законодательства Российской Федерации, стандартов и руководящих документов регуляторов в области обеспечения безопасности ПДн;
- обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Источниками разработки Положения являются:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07. 2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- иные нормативные акты Российской Федерации и документы регуляторов, регламентирующие вопросы обработки и обеспечения безопасности ПДн в организациях банковской системы Российской Федерации.

1.3. Настоящее Положение определяет цели, условия, требования, правила и процедуры организации правомерной и безопасной обработки ПДн, оператором которых является Банк.

1.4. Данным Положением должны руководствоваться в своей деятельности все работники Банка, допущенные к обработке ПДн и(или) участвующие в процессах обеспечения безопасности ПДн в Банке.

2. ОСНОВНЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем Положении используются следующие термины, определения и сокращения:

- 2.1. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.
- 2.2. **Банк** – Банк ВТБ (ПАО).
- 2.3. **Банк России** – Центральный банк Российской Федерации.
- 2.4. **(Информационная) безопасность персональных данных (далее – ИБ ПДн)** – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.
- 2.5. **Биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.
- 2.6. **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- 2.7. **Информационная система персональных данных (далее – ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- 2.8. **Клиент** – юридическое или физическое лицо, пользующееся услугами Банка.
- 2.9. **Конфиденциальность персональных данных** – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.
- 2.10. **Материальный носитель информации** – материальный объект, используемый для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в том числе в преобразованном виде.
- 2.11. **Модель угроз** – описание источников угроз; методов реализации угроз; объектов, пригодных для реализации угроз; уязвимостей, используемых источниками угроз; типов возможных потерь; масштабов потенциального ущерба от реализации угроз.
- 2.12. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- 2.13. **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.
- 2.14. **Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных или по его просьбе, или подлежащие опубликованию или обязательному раскрытию в соответствии с действующим законодательством Российской Федерации.
- 2.15. **Объект доступа** – объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящие в состав автоматизированной системы.

2.16. **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.

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

Примечание. К ПДн субъекта относятся в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, биометрические характеристики (индивидуальные биометрические характеристики лица, отпечаток пальца, слепок голоса).

2.18. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.19. **Работник** – физическое лицо, вступившее в трудовые отношения с Банком.

2.20. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц

2.21. **Субъект доступа** – работник или иное лицо, осуществляющий физический и(или) логический доступ, или программный сервис, осуществляющий логический доступ.

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

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

2.24. **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор)** – уполномоченный орган по защите прав субъектов ПДн в Российской Федерации.

2.25. **Федеральная служба безопасности Российской Федерации (далее – ФСБ России)** – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

2.26. **Федеральная служба по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России)** – федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Правовыми основаниями обработки ПДн в Банке являются:

- Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности», иные федеральные законы и принятые на их основе нормативные правовые акты, регулирующие отношения, связанные с деятельностью Банка;
- уставные документы Банка;
- договоры, заключаемые между Банком и клиентами – физическими лицами, физическими лицами, выступающими представителями клиентов – юридических лиц, физическими лицами – работниками Банка;

- согласия на обработку ПДн (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора).

3.2. На основании п. 3.1 и полномочий Банка как оператора ПДн, Банк обрабатывает ПДн субъектов следующих категорий:

- физических лиц, являющихся или намеревающихся стать клиентами Банка, а также их представителей¹;
- работников Банка²;
- кандидатов на работу в Банке;
- стажеров, направляемых в подразделения Банка для прохождения производственной практики;
- физических лиц, которым оформляются разовые и временные пропуска при посещении ими офисов Банка;
- акционеров Банка;
- иных субъектов, вступивших или намеревающихся вступить в договорные отношения с Банком;
- иных субъектов обращающихся в Банк (при необходимости обработки их ПДн для целей выполнения их запросов).

3.3. «Перечень ПДн, обрабатываемых в Банке ВТБ (ПАО)» сформирован в соответствии с технологической потребностью реализации бизнес-процессов в Банке и утвержден Заместителем Президента – Председателя Правления Банка 07.02.2011г.

3.4. Банк не обрабатывает специальных категорий ПДн, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни. Для целей идентификации и пропуска субъектов на территорию Банка обрабатываются биометрические ПДн (фотографии субъектов ПДн)³.

4. ПОЛИТИКА БАНКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Основными принципами обработки ПДн в Банке являются:

- **законность:** любая деятельность в отношении ПДн осуществляется в соответствии с требованиями действующего законодательства Российской Федерации и требованиями уполномоченных органов (ФСТЭК, ФСБ России, Роскомнадзор, Центральный Банк Российской Федерации);
- **целесообразность и целенаправленность:** ПДн в Банке обрабатываются в том и только в том объеме, который необходим для достижения заранее определенных целей обработки ПДн. В Банке обеспечивается соответствие порядка и способов обработки ПДн целям обработки ПДн. По достижении указанных целей обработка соответствующих ПДн прекращается;
- **безопасность:** все действия в отношении ПДн в Банке осуществляются таким образом, чтобы минимизировать возможность нанесения ущерба субъекту ПДн. Для этого в Банке

¹ Детальный порядок работы с ПДн клиентов Банка описывается в соответствующих нормативных актах и(или) распорядительных документах Банка, регламентирующих технологические и бизнес-процессы Банка, в рамках которых производится обработка ПДн.

² Обработка ПДн работников Банка осуществляется в соответствии с Положением «О защите персональных данных работников Банка ВТБ», введенным в действие Приказом Банка от 11.09.2017г. №1249.

³ В данном случае фотография субъекта ПДн отнесена к биометрическим ПДн на основании официально опубликованных Разъяснений Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.08.2013г. «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки».

реализуется комплекс мер, направленных на обеспечение безопасности конфиденциальной информации (включая ПДн и иные виды защищаемой законом информации), а также специальных мер и средств обеспечения информационной безопасности (далее – ИБ) ПДн.

4.2. Целями обработки ПДн в Банке являются:

- осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в том числе, но не ограничиваясь: Федеральным законом от 02.12.1990 № 395-1 «О банках и банковской деятельности», Федеральным законом от 30.12.2004 № 218-ФЗ «О кредитных историях», Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральным законом от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», Федеральным законом от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг», Федеральным законом от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)», Федеральным законом от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», нормативными актами Банка России, а также Уставом и нормативными актами Банка;
- обслуживание клиентов Банка;
- организация учета работников Банка для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, продвижении по работе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: Федеральным законом от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также Уставом и нормативными актами Банка;
- обеспечение доступа субъектов ПДн на территорию Банка при необходимости, обеспечение безопасности Банка при осуществлении такого доступа.

4.3. Указанные выше цели обуславливают необходимость обработки ПДн для выполнения следующих основных задач:

- заключения договоров/сделок с субъектами ПДн (их законными представителями)⁴ и их исполнения;
- продвижения продуктов Банка, включая оповещение субъектов ПДн об изменениях в продуктовой линейке, направление адресных продуктовых предложений, проведение маркетинговых исследований с использованием информационно-телекоммуникационных сетей и статистическую обработку информации;
- обеспечения юридической значимости документов, образующихся в процессе исполнения договоров с клиентами, работниками, партнерами, контрагентами и прочими сторонними по отношению к Банку лицами и организациями;
- обеспечения возможности защиты имущественных и иных интересов Банка, его работников и клиентов;
- организации кадровой работы и учета работников Банка для содействия в трудоустройстве, обучении, продвижении по работе, пользования различного вида льготами;
- осуществления управленческой деятельности;
- контроля количества и качества предоставляемых Банком услуг;
- осуществления административно-хозяйственной деятельности;
- формирования отчетности, в том числе для предоставления регуляторам и государственным органам.

⁴ В том числе оценка кредитоспособности/платежеспособности при рассмотрении заявок субъекта ПДн на предоставление банковских услуг.

4.4. Общий порядок обработки ПДн

4.4.1 Обработка ПДн в Банке осуществляется только с согласия субъекта ПДн (его законного представителя⁵ после проверки его полномочий) кроме случаев, указанных в статье 6 Федерального закона № 152-ФЗ.

4.4.2 Формы письменного согласия на обработку ПДн устанавливаются нормативными и(или) методическими документами Банка, регламентирующими обработку ПДн в Банке.

4.4.3 Банк осуществляет передачу ПДн государственным органам и уполномоченным юридическим и физическим лицам⁶ в рамках их полномочий и компетенции в соответствии с Федеральным законом № 152-ФЗ.

4.4.4 Банк может осуществлять передачу ПДн для обработки третьему лицу в соответствии со статьей 6 Федерального закона № 152-ФЗ. При этом:

- обработка третьим лицом ПДн, предоставленных Банку субъектом ПДн (его законным представителем), может осуществляться только с согласия субъекта ПДн (его законного представителя), если получение такого согласия необходимо в соответствии с требованиями Федерального закона № 152-ФЗ;
- обработка ПДн третьим лицом может осуществляться только на основании договора, в котором определены перечень действий (операций), которые будут осуществляться с ПДн, а также положения по обеспечению ИБ ПДн, в том числе требования не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации⁷.

4.4.5 Банк может осуществлять трансграничную передачу ПДн в случаях, предусмотренных статьей 12 Федерального закона № 152-ФЗ, договорами и соглашениями с международными организациями. При этом в указанные договоры и соглашения должны быть включены положения по обеспечению адекватной защиты прав субъектов ПДн (в том числе положения по обеспечению ИБ ПДн).

4.4.6 Банк осуществляет деятельность по своевременному выявлению и внесению изменений в обрабатываемые ПДн с целью обеспечения их достоверности и актуальности, в том числе по отношению к целям обработки ПДн. Соответствующие процедуры и инструкции устанавливаются нормативными и(или) методическими документами Банка, регламентирующими обработку ПДн в Банке.

4.4.7 Хранение ПДн в форме, позволяющей идентифицировать субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки, если иное не установлено законодательством Российской Федерации или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

⁵ В случае получения ПДн субъекта через его законного представителя, Банк уведомляет о данном факте субъекта ПДн и сообщает ему его права в отношении обрабатываемых ПДн, наименование и адрес Банка, цели обработки ПДн, предполагаемых пользователей ПДн. Исключение составляют случаи, когда:

- ПДн переданы в Банк на основании требований федерального закона;
- ПДн являются общедоступными;
- Банк осуществляет обработку ПДн по поручению третьего лица – оператора на основании договора, заключенного между Банком и таким третьим лицом.

⁶ Представителю субъекта ПДн (в том числе адвокату) ПДн передаются в порядке, регламентированном действующим законодательством Российской Федерации и объеме, установленном распоряжением субъекта ПДн, при наличии одного из следующих надлежащим образом оформленных документов:

- оригинала нотариально удостоверенной доверенности представителя субъекта ПДн;
- заявления субъекта ПДн, написанного в присутствии работника Банка и заверенного работником Банка, принявшим заявление (или заверенного нотариально, если оно составлялось не в присутствии работника Банка).

В случае если лицо, обратившееся в Банк с запросом на предоставление ПДн, не уполномочено на получение информации, относящейся к ПДн, Банк обязан отказать лицу в выдаче такой информации с соответствующим уведомлением указанного лица об отказе.

⁷ В том числе Федеральным законом от 30.12.2004 № 218-ФЗ «О кредитных историях», в соответствии с которым Банком заключаются договоры с бюро кредитных историй об оказании информационных услуг.

4.4.8 Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

4.4.9 Хранение ПДн при обработке с использованием средств автоматизации осуществляется обособленно от иной информации, в частности путем фиксации на отдельных материальных носителях (при наличии технической возможности), а при обработке ПДн на бумажных носителях – в специальных разделах или в полях форм документов⁸.

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

4.4.11 По достижении целей обработки ПДн или по требованию субъекта ПДн (его законного представителя) ПДн уничтожаются или обезличиваются в соответствии с Федеральным законом № 152-ФЗ.

4.4.12 Ответственность за организацию процесса обработки ПДн возлагается на выделенного работника Банка приказом Банка. В его обязанности входит:

- внутренний контроль соблюдения Банком и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;
- обеспечение доведения до сведения работников Банка положений законодательства о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;
- организация приема и обработки обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

4.4.13 Для выполнения своих обязанностей указанное в пункте 4.4.12 лицо, ответственное за организацию обработки ПДн в Банке, наделяется правами:

- принимать решения в пределах своей компетенции в части организации процесса обработки ПДн;
- получать имеющиеся в Банке сведения, указанные в части 3 статьи 22 Федеральным законом № 152-ФЗ;
- требовать от работников Банка соблюдения действующего законодательства Российской Федерации, а также локальных нормативных актов Банка.
- контролировать осуществление мер, направленных на обеспечение выполнения обязанностей по защите прав субъектов ПДн и обеспечения ИБ их ПДн, предусмотренных законодательством Российской Федерации, и принятыми в соответствии с ним нормативными правовыми актами.

4.4.14 Банк осуществляет уведомление Роскомнадзора об обработке ПДн (в т.ч. о намерениях осуществлять обработку ПДн), о прекращении обработки ПДн, об изменении сведений об обработке ПДн, ранее направленных Банком в Роскомнадзор в сроки, установленные Федеральным законом № 152-ФЗ.

⁸ Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должна:

- содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации; наименование и адрес подразделения Банка, обрабатывающего ПДн; фамилию, имя, отчество и адрес субъекта ПДн; источник получения ПДн; сроки обработки ПДн; перечень действий с ПДн, которые будут совершаться в процессе их обработки; общее описание используемых оператором способов обработки ПДн.
- предусматривать поле или приложение, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;
- быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

4.5. Права субъектов персональных данных

4.5.1 В целях обеспечения защиты ПДн, обрабатываемых в Банке, субъект ПДн или его законный представитель (здесь и далее по тексту под субъектами ПДн понимаются сам субъект ПДн, его законный представитель) имеет право:

- свободного бесплатного доступа к своим ПДн, включая право на получение копии любой записи, содержащей ПДн субъекта ПДн, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих ПДн возможно при личном обращении субъекта ПДн в Банк;
- получения информации, касающейся обработки его ПДн, в том числе содержащей:
 - подтверждение факта обработки ПДн Банком;
 - правовые основания и цели обработки ПДн;
 - цели и применяемые Банком способы обработки ПДн;
 - 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;
 - обрабатываемые ПДн, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
 - сроки обработки ПДн, в том числе сроки их хранения;
 - порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;
 - информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;
 - иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами;
- требовать от Банка уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- запрашивать (в том числе повторно, но не ранее чем через тридцать дней⁹ после первоначального обращения или направления первоначального запроса, кроме случая, когда запрашиваемые сведения не были предоставлены) свои ПДн, обрабатываемые в Банке, и получать их в доступной форме;
- требовать извещения Банком всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать действия или бездействие Банка в Роскомнадзоре или в судебном порядке;
- отозвать свое согласие на обработку ПДн.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В Банке определены угрозы ИБ и реализован комплекс организационно-технических мер защиты конфиденциальной информации, к которой относятся ПДн, а также специальных мер и средств обеспечения ИБ ПДн, направленных на предотвращение несанкционированного или

⁹ Если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

случайного доступа к ПДн, их уничтожения, искажения, блокирования, распространения и иных неправомерных действий.

5.2. К мерам защиты ПДн в Банке относятся в том числе:

- учет ПДн и их носителей;
- учет и классификация информационных систем персональных данных (далее – ИСПДн);
- назначение лица, ответственного за организацию обработки ПДн;
- назначение лица, ответственного за обеспечение безопасности ПДн;
- формализация и контроль выполнения порядка обработки ПДн в ИСПДн;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, обеспечение регистрации и учёта действий, совершаемых с ПДн в ИСПДн;
- формализация и контроль выполнения требований по уничтожению (обезличиванию) ПДн и носителей ПДн;
- регулярный внутренний контроль соответствия обработки ПДн требованиям действующего законодательства;
- оценка вреда, который может быть причинен субъектам ПДн в случае нарушения действующего законодательства;
- применение организационных и технических мер по обеспечению безопасности ПДн при обработке их в ИСПДн, необходимых для выполнения требований к защите ПДн в соответствии с установленным уровнем защищённости;
- применение организационных и технических мер по обеспечению безопасности ПДн при передаче ПДн по телекоммуникационным каналам связи;
- применение технических средств защиты информации, прошедших в установленном в соответствии с Федеральным законом от 27.12.2002 №184-ФЗ «О техническом регулировании» порядке процедуру оценки соответствия;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- контроль доступа работников Банка и иных лиц к обрабатываемым в Банке ПДн и средствам их обработки;
- ознакомление работников Банка, осуществляющих обработку ПДн с требованиями действующего законодательства и требованиями внутренних локальных нормативных актов;
- контроль соблюдения работниками Банка, осуществляющими обработку ПДн, правил, требований и процедур обработки ПДн;
- раздельное хранение ПДн, обработка которых осуществляется с различными целями;
- обеспечение процедур резервного копирования и восстановления ПДн;
- включение положений по обеспечению ИБ ПДн в договоры с третьими лицами, которым передаются ПДн, в том числе требований не раскрывать и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищённости ИСПДн.

5.3. Определение, фиксация и выполнение требований по обеспечению ИБ ПДн выполняется в том же порядке, что и определение, фиксация и выполнение требований по обеспечению ИБ иной конфиденциальной информации в Банке.

Президент - Председатель Правления
Банка ВТБ (ПАО)

А.Л. Костин