ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАО «Банк ФИНАМ»

Москва, 2012 г.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Автоматизированная банковская система (АБС)** - комплекс программного и технического обеспечения, реализующий технологию выполнения функций Банка.

1.2. **Администратор информационной безопасности (Администратор ИБ)** - представитель подразделения (лицо), ответственного(ое) за обеспечение информационной безопасности в Банке.

1.3. **Администратор информационной безопасности информационных систем персональных данных (Администратор ИБ ИСПДн)** - представитель подразделения (лицо), ответственного(ое) за обеспечение безопасности персональных данных в информационных системах персональных данных.

1.4. **Банк** – ЗАО «Банк ФИНАМ», включая его обособленные и внутренние структурные подразделения**.**

1.5. **Безопасность персональных данных** – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.

1.6. **Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения ПДн, в том числе их передачи.

1.7. **Информационная безопасность (ИБ)** – безопасность, связанная с угрозами в информационной сфере.

1.8. **Информационная система персональных данных (ИСПДн)**– информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

1.9. **Информационный актив** – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Банка, находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

1.10. **Использование персональных данных** – действия (операции) с ПДн, совершаемые уполномоченными на то сотрудниками Банка в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн либо иным образом затрагивающих его права и свободы или права и свободы других лиц.

1.11. **Конфиденциальность персональных данных** – обязательное для соблюдения Банком или иным получившим доступ к ПДн лицом, требование не допускать их распространения без согласия субъекта ПДн или иного законного основания.

1.12. **Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн.

1.13. **Оператор** - государственный орган, муниципальный орган, юридическое (в том числе Банк) или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

1.14. **Обработка персональных данных** – действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

1.15. **Общедоступные персональные данные** – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.16. **Ответственный за безопасность ПДн** - структурное подразделение или должностное лицо Банка, назначенное ответственным за обеспечение безопасности ПДн приказом Председателя Правления, либо организация - контрагент Банка, имеющая лицензию на деятельность по технической защите конфиденциальной информации, отвечающая за обеспечение безопасности ПДн на договорной основе.

1.17. **Персональные данные (ПДн)** – сведения, перечисленные в разделе 4 настоящего Положения, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также любая

другая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

1.18. **Пользователь информационной системы персональных данных (Пользователь ИСПДн)** – лицо, участвующее в функционировании ИСПДн или использующее результаты ее функционирования.

1.19. **Распространение персональных данных** – действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с ПДн неограниченного круга лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

1.20. **Сеть Интернет** – **Сеть Интернет** – объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

1.21. **Система информационной безопасности (СИБ)** – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

1.22. **Трансграничная передача персональных данных** – передача ПДн Банком через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

1.23. **Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

1.24. **Частная политика информационной безопасности (частная политика ИБ)** - документ, детализирующий положения политики ИБ Банка применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Банка.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящее Положение об обработке персональных данных в ЗАО «Банк ФИНАМ» (далее — Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.06.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон №152-ФЗ), другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой персональных данных, Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2010) и рекомендациями в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» (РС БР ИББС-2.3-2010).

2.2 Положение является частной политикой информационной безопасности и разработано в развитие Политики информационной безопасности Банка на основании задекларированных в ней целей и задач обеспечения информационной безопасности, а также принципов ее реализации.

2.3. Положение определяет требования к порядку сбора, обработки, хранения и защиты (обеспечению безопасности) ПДн субъектов, ПДн которых обрабатываются Банком с использованием средств автоматизации или без использования таких средств, а также требования по обеспечению безопасности ПДн при их обработке.

3. ЦЕЛИ И СФЕРА ДЕЙСТВИЯ ПОЛОЖЕНИЯ

3.1. Целями Положения является определение категорий и состава ПДн, целей и способов обработки ПДн клиентов, сотрудников Банка и иных субъектов, ПДн которых подлежат обработке, установление требований по обеспечению безопасности ПДн при их обработке, а также ответственности сотрудников Банка, имеющих доступ к ПДн.

3.2. Действие Положения распространяется на все подразделения Банка, включая его обособленные и внутренние структурные подразделения.

4. КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1. ПДн классифицируются Банком в следующие категории, указанные в порядке убывания тяжести последствий потери свойств безопасности ПДн субъекта персональных данных:

4.1.1. ПДн, отнесенные в соответствии с Федеральным законом №152-ФЗ к специальным категориям ПДн:

сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

4.1.2. ПДн, отнесенные в соответствии с Федеральным законом №152-ФЗ к биометрическим ПДн:

сведения, которые характеризуют физиологические особенности человека и на основе которых можно однозначно установить его личность (дактилоскопические данные и другие данные в устройствах, использующих для идентификации биометрические данные человека).

4.1.3. ПДн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим ПДн, к общедоступным или обезличенным ПДн, в том числе:

фамилия, имя, отчество (в т.ч. прежние);

дата и место рождения;

паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);

данные водительского удостоверения (серия, номер, дата выдачи, наименование органа, выдавшего документ);

гражданство;

адрес места жительства (по регистрационному документу и фактический);

дата регистрации по месту жительства или по месту пребывания;

номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по регистрационному документу);

сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);

сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения);

сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и ее наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения);

сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;

содержание и реквизиты трудового договора с работником Банка или гражданско-правового договора с гражданином;

сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения);

сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения);

сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения);

сведения об имуществе (имущественном положении):

– автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств),

– недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения),

– банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма, условия вклада и другие сведения),

– кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости, сумма и валюта кредита или займа, цель кредитования, условия кредитования, сведения о залоге, сведения о приобретаемом объекте, данные по ценным бумагам, остатки и суммы движения по счетам, тип банковских карт, лимиты и другие сведения),

сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

сведения об идентификационном номере налогоплательщика;

сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования);

сведения, указанные в оригиналах и копиях приказов по личному составу Банка и материалах к ним;

сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников Банка;

материалы по аттестации и оценке работников Банка;

материалы по внутренним служебным расследованиям в отношении работников Банка;

внутрибанковские материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами;

сведения о временной нетрудоспособности работников Банка;

табельный номер работника Банка;

сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

4.1.4. ПДн, отнесенные в соответствии с Федеральным законом №152-ФЗ к общедоступным или обезличенным ПДн:

сведения, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности, в том числе любые сведения, полученные из средств массовой информации, Сети Интернет, других общедоступных источников получения информации.

4.1.5. Перечень (состав) обрабатываемых ПДн определяются Банком отдельно по каждому субъекту ПДн и утверждаются приказом Председателя Правления.

5. СУБЪЕКТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Банк выделяет следующие субъекты ПДн:

5.1. Клиенты (в том числе заемщики) – физические лица, которым Банк оказывает услуги в соответствии с перечнем банковских операций и иных сделок, указанных в Федеральном законе «О банках и банковской деятельности» и в рамках выданной Банком России лицензии, в том числе владельцы и/или уполномоченные лица юридических лиц – клиентов Банка;

5.2. Сотрудники Банка (в том числе кандидаты на должность) – физические лица, вступившие или намеренные вступить в трудовые отношения с Банком, как с работодателем;

5.3. Физические лица (в том числе индивидуальные предприниматели), с которыми Банк заключил гражданско-правовой договор (подряда, аренды, оказания услуг, и т.д.) или сотрудник юридического лица, с которым у Банка заключен гражданско-правовой договор, действующий от имени Банка на основании доверенности;

5.4. Акционеры Банка;

5.5. Физические лица, ПДн которых поступают в Банк из органов регулирования и надзора в рамках выполнения требований действующего законодательства, в т.ч. надзорных функций.

6. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка Банком ПДн осуществляется Банком в целях:

- осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в том числе: «Об акционерных обществах», «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», нормативными актами Банка России и Федеральной службы по финансовым рынкам, а также Уставом и другими внутренними документами Банка;
- организации учета сотрудников Банка для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия им в обучении, продвижении по службе, пользовании различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и другими внутренними документами Банка.

6.2. Конкретные цели обработки ПДн определяются Банком отдельно по каждому субъекту ПДн и утверждаются приказом Председателя Правления.

При этом для каждой цели обработки ПДн устанавливается объем и содержание ПДН, а также необходимость получения согласия субъектов ПДн.

7. ПРАВОВОЕ ОСНОВАНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Обработка ПДн, осуществляется Банком в рамках лицензий Банка России и Федеральной службы по финансовым рынкам, а также Банка.

7.2. Правовым основанием обработки ПДн являются следующие законодательные и нормативные правовые акты:

- Трудовой кодекс Российской Федерации;
- Федеральный закон №152-ФЗ;
- Федеральный закон Российской Федерации от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 02.12.1990 г. №395-1 «О банках и банковской деятельности»;
- Федеральный закон Российской Федерации от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон №115-ФЗ);
- Федеральный закон от 30.12.2004г. № 218-ФЗ «О кредитных историях»;
- Положение Банка России «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансирования терроризма» от 19.08.2004 №262-П;
- Инструкция Банка России «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам)» (далее – Инструкция №28-И);
- иные законодательные и нормативные правовые документы, регламентирующие банковскую деятельность и трудовые отношения, и касающиеся вопросов сбора, систематизации накопления, хранения, уточнения, использования и распространения ПДн;
- внутренние нормативные документы Банка, регламентирующие указанные вопросы.

7.3. В Банке наряду со специальными документами, также разрабатываются и вводятся в действие внутренние нормативные документы, регламентирующие процессы обеспечения

информационной безопасности активов Банка, действие которых также распространяется и на защиту ПДн.

7.4. Правовое основание обработки ПДн определяются Банком отдельно по каждому субъекту ПДн.

8. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Сроки обработки, в том числе сроки хранения ПДн, определяются в соответствии со сроком действия договора с субъектом ПДн, сроком исковой давности, а также сроками хранения документов, содержащих ПДн, установленными:

- Приказом Минкультуры от 25.08.2010 № 558 «Об утверждении перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения»;
- Постановлением ФКЦБ РФ от 16.07.2003 № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ»,
- иными законодательными и нормативными правовыми актами Российской Федерации, определяющими сроки хранения документов;
- действующей номенклатурой дел Банка.

9. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Банк не осуществляет обработку ПДн, отнесенных в соответствии с Федеральным законом № 152-ФЗ к специальным категориям ПДн и биометрическим ПДн, перечисленных в подпунктах 4.1.1 и 4.1.2 раздела 4 Положения.

9.2. Банк осуществляет обработку Пдн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим ПДн, к общедоступным или обезличенным ПДн, перечисленных в подпункте 4.1.3 раздела 4 Положения, в соответствии с принципами:

- законности целей и способов обработки ПДн и добросовестности;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Банка;
- соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн;
- недопустимости хранения ПДн после достижения цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

9.3. Обработка ПДн должна осуществляться с соблюдением следующих условий:

- сбор, накопление, хранение, изменение, использование и распространение ПДн субъекта ПДн может осуществляться только при условии наличия его письменного согласия, которым признается, включая, но не ограничиваясь этим, анкета, договор, заявление по форме Банка, содержащие его собственноручную подпись, или аналог собственноручной подписи;
- обработка ПДн Банком в целях продвижения банковских услуг на рынке путем осуществления прямых контактов с потенциальным клиентом с помощью средств связи, допускается только при условии предварительного согласия субъекта ПДн:
- при сборе ПДн Банк обязан предоставить субъекту ПДн по его запросу информацию о целях, способах обработки ПДн, сведениях о лицах, имеющих доступ к ПДн, сроках обработки и хранения ПДн, а также об источниках их получения.

10. СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ. ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ.

10.1. Банк осуществляет обработку ПДн с использованием средств автоматизации, а также без использования таких средств.

10.2. Обработка ПДн, содержащихся в ИСПДн, либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как уточнение (обновление, изменение), использование, распространение (в том числе передача), уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

10.3. Банк определяет и документально фиксирует перечень систем, обрабатывающих ПДн (включая ИСПДн) с указанием цели их создания, отдельно по головному офису Банка (включая его ВСП) и по каждому обособленному подразделению Банка (включая его ВСП).

К ИСПДн Банк относит АБС, целью создания и использования которых является обработка ПДн.

АБС, реализующие банковские платежные технологические процессы, не относятся к ИСПДн.

АБС, в которых обрабатываются ПДн, но целью работы которых не является обработка ПДн, включаются в перечень систем, обрабатывающих ПДн, но не классифицируются как ИСПДн.

Перечень систем, обрабатывающих ПДн должен пересматриваться в случае приобретения или создания новой АБС.

10.4. Для каждой ИСПДн Банком определяются и документально фиксируются:

- цель обработки ПДн;
- объем и содержание обрабатываемых ПДн;
- перечень действий с ПДн и способы их обработки.

Объем и содержание ПДн, а также перечень действий и способы обработки ПДн должны соответствовать целям их обработки. В том случае, если для выполнения банковского информационного технологического процесса, реализацию которого поддерживает ИСПДн, нет необходимости в обработке определенных ПДн, эти ПДн должны быть удалены.

11. ОБЩИЕ ТРЕБОВАНИЯ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Конфиденциальность ПДн

Сведения, содержащие персональные данные, относятся Банком к конфиденциальной информации. Перечень конфиденциальной информации утверждается распорядительным документом Председателя Правления.

Банком и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных, за исключением следующих случаев:

1) в случае обезличивания персональных данных;

2) в отношении общедоступных персональных данных.

11.2. Передача ПДн третьему лицу

11.2.1. Передача ПДн субъекта ПДн третьим лицам осуществляется только при наличии письменного согласия субъекта ПДн за исключением случаев, когда ПДн передаются:

- в целях исполнения федерального закона, устанавливающего цель, условия передачи ПДн и круг субъектов ПДн, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- в целях защиты жизни и здоровья субъекта ПДн;
- в случае поступления официальных запросов в соответствии с положениями Федерального закона «Об оперативно-розыскной деятельности»;
- в случае поступления официальных запросов из налоговых органов, органов Пенсионного Фонда России, органов Федерального социального страхования, судебных органов, Банка России;
- в целях исполнения договора.

11.2.2. В случае, когда Банк на основании договора поручает обработку ПДн третьему лицу, указанным договором (в качестве существенного условия) или отдельным соглашением с этим лицом должна быть предусмотрена обязанность обеспечения конфиденциальности ПДн и безопасности ПДн при их обработке.

11.3. Трансграничная передача ПДн

11.3.1. Трансграничная передача ПДн осуществляется Банком только на территории иностранных государств, обеспечивающих адекватную защиту ПДн.

11.3.2. Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты ПДн, может осуществляться только в случаях:

- наличия письменного согласия субъекта ПДн на трансграничную передачу его ПДн;
- исполнения договора, стороной которого является субъект ПДн;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия субъекта ПДн в письменной форме.

11.4. Хранение ПДн

11.4.1. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

11.4.2. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

ПДн, хранящиеся на бумажных носителях, должны находиться в сейфах или в металлических шкафах, обеспечивающих защиту от несанкционированного доступа.

ПДн в электронном виде хранятся в ИСПДн Банка, а также на отчуждаемых машинных носителях (типа CD-, DVD-дисков однократной записи) в порядке, установленном нормативными документами Банка России и внутренними документами Банка.

11.5. Уничтожение ПДн

11.5.1. Банк обязан прекратить обработку ПДн и уничтожить (обезличить) их в следующих случаях и в следующие сроки:

1) по достижении целей обработки или при утрате необходимости в их достижении - в срок не превышающий тридцать дней с даты достижения указанной цели или утраты необходимости в ее достижении;

2) при отзыве субъектом ПДн согласия на обработку своих ПДн, если такое согласие требуется в соответствии с законодательством РФ - в срок, не превышающий тридцати дней с даты поступления требования, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо федеральными законами;

3) по требованию субъекта ПДн или Уполномоченного органа по защите прав субъектов ПДн, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки ПДн - в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, тридцати дней с даты получения требования - в остальных случаях;

4) при невозможности устранения Банком допущенных нарушений при обработке персональных данных - в срок, не превышающий десяти рабочих дней с даты выявления нарушений.

В случае отсутствия возможности уничтожения ПДн в течение установленного подпунктами 1-2 срока, Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется третьим лицом, действующим по поручению Банка) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

Об устранении допущенных при обработке ПДн нарушений или об уничтожении ПДн Банк обязан уведомить субъекта ПДн, а также Уполномоченный орган по защите прав субъектов ПДн, если обращение субъекта ПДн либо запрос были направлены указанным органом.

11.5.2. Уничтожение бумажных носителей ПДн производится с помощью средств, гарантирующих невозможность восстановления носителя.

Уничтожение информации с машиночитаемых носителей ПДн должно производиться способом, исключающим возможность использования и восстановления информации.

Обезличивание ПДн должно производиться способом, исключающим возможность идентифицировать субъекта ПД по остаточным данным после проведения соответствующих процедур.

11.6. Внутренние документы, регламентирующие вопросы обработки ПДН

11.6.1.В дополнение к настоящему Положению, Банк разрабатывает и вводит в действие внутренние нормативные документы, регламентирующие отдельные вопросы, связанные с обработкой ПДНн, в том числе:

- особенности обработки ПДн без использования средств автоматизации, в том числе обработки ПДн на бумажных носителях, в частности, при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн,
- порядок уничтожения и обезличивания ПДн;
- порядок обработки обращений субъектов ПДн (или их законных представителей) по вопросам обработки их ПДн;
- порядок действий в случае запросов Уполномоченного органа по защите прав субъектов ПДн или иных надзорных органов, осуществляющих контроль и надзор в области ПДн.

11.6.2. Банком также должны быть документированы все информационные технологические процессы, в рамках которых обрабатываются ПДн в ИСПДн.

12. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

12.1. Общие требования

12.1.1. При обработке ПДн Банк принимает все необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

12.1.2. Организация выполнения требований по обеспечению безопасности ПДн осуществляется Ответственным за безопасность ПДн.

Реализация требований по обеспечению безопасности ПДн должна осуществляться по согласованию и под контролем Администратора ИБ.

12.1.3.В Банке должен быть определен и документально зафиксирован перечень (список) сотрудников, осуществляющих обработку ПДн в ИСПДн либо имеющих доступ к ПДн, отдельно по головному офису Банка (включая его ВСП) и по каждому обособленному подразделению Банка (включая его ВСП).

Допускается указание сотрудников в перечне (списке) на ролевой основе в соответствии с занимаемой должностью.

Доступ сотрудников Банка к ПДн и обработка сотрудниками Банка ПДн должны осуществляться только для выполнения их должностных обязанностей.

Предоставление сотрудникам прав доступа в ИСПДн осуществляется только на основании распорядительного документа Председателя Правления или Управляющего обособленным подразделением Банка. При назначении на должность сотрудников, указанных в перечне (списке) сотрудников, осуществляющих обработку ПДн в ИСПДн либо имеющих доступ к ПДн, на ролевой основе, отдельный распорядительный документ на каждого сотрудника не издается.

Сотрудники, указанные в перечне (списке) сотрудников, осуществляющих обработку ПДн в ИСПДн либо имеющие доступ к ПДн, на ролевой основе, а также сотрудники, исполняющие обязанности указанных сотрудников на время их отсутствия, считаются допущенными к обработке ПДн в дату их назначения на должность или дату издания приказа об исполнении обязанностей на время отсутствия соответственно. При увольнении сотрудников, указанных в перечне (списке) сотрудников, осуществляющих обработку ПДн в ИСПДн либо имеющие доступ к ПДн, на ролевой основе, а также при прекращении исполнения обязанностей временно отсутствующего сотрудника, занимающего указанную должность, доступ в соответствующие ИС аннулируется.

12.1.4. Сотрудники Банка, осуществляющие обработку ПДн в ИСПДн, должны быть проинформированы о факте обработки ими ПДн, категориях обрабатываемых ПДн, а также должны быть ознакомлены под роспись с Положением и другими внутренними документами Банка, изданными по вопросам обработки и обеспечения безопасности ПДн в части, касающейся их должностных обязанностей.

12.2. Требования по обеспечению информационной безопасности банковских технологических процессов, в рамках которых обрабатываются ПДн

12.2.1. СИБ банковского платежного технологического процесса, в рамках которого обрабатываются ПДн, должна соответствовать требованиям Положения об информационной безопасности банковских платежных технологических процессов, разработанного Банком и утвержденного в установленном порядке.

СИБ банковского информационного технологического процесса, в рамках которого обрабатываются ПДн вне ИСПДн, должна соответствовать требованиям Положения об информационной безопасности банковских информационных технологических процессов, разработанного Банком и утвержденного в установленном порядке.

СИБ банковского информационного технологического процесса, в рамках которого обрабатываются ПДн в ИСПДн, должна соответствовать требованиям Положения об информационной безопасности банковских информационных технологических процессов, разработанного Банком и утвержденного в установленном порядке, и пункту 12.4 Положения.

12.2.2. Все ИСПДн Банка относятся к специальным в соответствии с пунктом 8 Порядка проведения классификации информационных систем персональных данных, утвержденного Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных".

12.2.3. ИСПДн Банка подлежат обязательной классификации. Для проведения классификации ИСПДн распорядительными документами Председателя Правления ~~и~~ (Управляющего обособленным подразделением Банка) назначаются соответствующие комиссии.

Критерии классификации ИСПДн и порядок проведения классификации ИСПДн утверждаются распорядительным документом Председателя Правления Банка.

Классификация ИСПДн должна проводиться в том числе на основе категорий обрабатываемых в ИСПДн ПДн.

Результаты классификации оформляются соответствующим актом, утверждаемым Председателем Правления (Управляющим обособленным подразделением) Банка.

12.3. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн

12.3.1. Требования по обеспечению безопасности ПДн в ИСПДн реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

12.3.2. 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 ПДн.

Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн должны осуществляться по согласованию и под контролем Ответственного за безопасность ПДн и Администратора ИБ Банка.

12.3.3. Все информационные активы, принадлежащие ИСПДн Банка, должны быть защищены от воздействий вредоносного кода.

Обеспечение безопасности ПДн средствами антивирусной защиты производится Банком в соответствии с требованиями, установленными Частной политикой информационной безопасности в области антивирусной защиты для обеспечения защиты АБС Банка от воздействия компьютерных вирусов. Порядок реализации требований по обеспечению безопасности ПДн средствами антивирусной защиты и порядок контроля реализации этих требований определяется внутренними документами Банка, разработанными в целях выполнения указанной Политики.

12.3.4. Система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн организуется в порядке, установленном Политикой информационной безопасности при управлении доступом и регистрации.

12.3.5. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений Банка обязаны обеспечить безопасность ПДн при их обработке в ИСПДн.

Работники, осуществляющие обработку ПДн в ИСПДн, должны действовать в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдать требования Банка по обеспечению ИБ.

12.3.6. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению ИБ ИСПДн Банка, возлагаются приказом Председателя Правления (Управляющего обособленным подразделением) на Администратора ИБ ИСПДН.

12.3.7. Порядок действий Администратора ИБ ИСПДн и персонала, занятых в процессе обработки ПДн, должен быть определен инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн.

12.3.8. Пользователи ИСПДн и обслуживающий персонал ИСПДн не должны осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование ПДн. Запрещается несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование ПДн, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки.

12.4. Внутренние документы, регламентирующие вопросы обеспечения безопасности ПДн при их обработке

12.4.1.В дополнение к настоящему Положению, Банк разрабатывает и вводит в действие внутренние нормативные документы, регламентирующие отдельные вопросы, связанные с безопасностью ПДНн при их обработке, в том числе:

- порядок ведения перечня сотрудников, имеющих доступ к ПДн и предоставления доступа в информационные системы, в которых обрабатываются ПДн;
- порядок доступа сотрудников Банка и иных лиц в помещения, в которых размещаются технические средства ИСПДн, ведется обработка ПДн и хранятся материальные носители ПДн, предусматривающий контроль доступа в помещения посторонних лиц и наличие препятствий для несанкционированного проникновения в помещения;
- порядок хранения материальных носителей ПДн, устанавливающий: места хранения материальных носителей ПДн; требования по обеспечению безопасности ПДн при хранении их носителей; должностных лиц, ответственных за реализацию требований по обеспечению безопасности ПДн; порядок контроля выполнения требований по обеспечению безопасности ПДн при хранении материальных носителей ПДн.
- мероприятия по обеспечению безопасности ПДн при их обработке без использования средств автоматизации
- модель угроз безопасности ПДн, содержащую актуальные для Банка угрозы ИБ.

13. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОЛОЖЕНИЯ И УСЛОВИЯ ЕГО ПЕРЕСМОТРА

13.1. Контроль реализации требований Положения осуществляется путем:

- контроля за соблюдением требований по обеспечению безопасности ПДн при их обработке со стороны Администратора ИБ;
- проведения самооценки ИБ при обработке ПДн;
- проведения аудита ИБ при обработке ПДн;
- анализа функционирования системы информационной безопасности при обработке ПДн (в том числе со стороны руководства Банка).

13.2. Пересмотр Положения производится по мере необходимости (при внесении изменений в законодательные акты, нормативные документы Российской Федерации в области обеспечения информационной безопасности и нормативные акты Банка России, а также при изменении концептуальных подходов руководства Банка к вопросам обработки ПДн, установленных Положением.

13.3. Должностные лица, ответственные за пересмотр Положения, устанавливаются приказом по Банку.

14. ОТВЕТСТВЕННОСТЬ ЗА РЕАЛИЗАЦИЮ ПОЛОЖЕНИЯ

14.1. Ответственность за выполнение требований по обеспечению безопасности ПДн при их обработке, установленных Положением и другими внутренними документами Банка, издаваемыми

по вопросам обработки ПДн, несут Ответственный за безопасность ПДн и Администратор ИБ ИСПДн.

14.2. Обязанность по выполнению мер защиты ПДн, предписанных Положением и другими внутренними документами Банка, издаваемыми по вопросам антивирусной защиты, возлагается на пользователей банковских технологических процессов, в рамках которых обрабатываются ПДн, в том числе пользователей ИСПДн.

14.3. Контроль за соблюдением Политики лицами, перечисленными в пунктах 8.1 и 8.2 Политики, возлагается на Администратора ИБ Банка.

14.4. Любое грубое нарушение работниками Банка требований Положения, иных внутренних документов Банка по вопросам обработки ПДн, расследуется Банком. К виновным лицам должны применяться адекватные меры воздействия.

14.5. За нарушение установленных Банком требований и правил по обеспечению ИБ при обработке ПДн работники Банка несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную действующим законодательством Российской Федерации.