

ПТК-120

Приложение к Приказу
от 16.01.2019 №28

ПОЛИТИКА обработки персональных данных

Версия 4.

Москва
2019

Оглавление

Стр.

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	3
1.1. Область применения	3
1.2. Термины и определения.....	4
1.3. Сокращения	5
2. ОСНОВНЫЕ ПОЛОЖЕНИЯ.....	5
2.1. Принципы обработки персональных данных	5
2.2. Цели обработки персональных данных.....	5
2.3. Субъекты персональных данных	6
2.4. Состав персональных данных.....	6
2.5. Согласие на обработку персональных данных	7
2.6. Поручение на обработку персональных данных.....	8
2.7. Обязанности ответственных лиц Банка при обработке персональных данных.....	8
2.8. Способы обработки персональных данных.....	9
2.9. Период обработки и хранения персональных данных.....	11
2.10. Места хранения ПДн (материальные носители).....	12
2.11. Перечень лиц, которые осуществляют обработку ПДн и имеют к ним доступ.....	12
3. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ	13
4. ОСНОВНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН	13
5. ОТВЕТСТВЕННОСТЬ	14
6. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, НА КОТОРЫЕ ДАЮТСЯ ССЫЛКИ	14

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения

1.1.1. Настоящая Политика обработки персональных данных (далее – Политика) регулирует отношения, связанные с обработкой ПДн, осуществляемой Банком с использованием средств автоматизации, в том числе в информационных системах, или без использования таких средств, если обработка ПДн без использования таких средств соответствует характеру действий (операций), совершаемых с ПДн с использованием средств автоматизации, а также вопросы обеспечения безопасности ПДн.

1.1.2. Целью настоящего документа является формирование и проведение единой политики при обработке и обеспечении безопасности ПДн.

1.1.3. Настоящая Политика разработана в соответствии с положениями действующих нормативно-правовых актов Российской Федерации, в том числе:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.1.4. Действие Политики распространяется на все процессы Банка, связанные с обработкой и защитой ПДн, и ее требования обязательны для применения всеми работниками Банка.

1.1.5. Внутренние документы Банка, затрагивающие вопросы обработки и обеспечения безопасности ПДн, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

1.1.6. В целях настоящей Политики понимаются следующие категории персональных данных:

1.1.6.1. категории персональных данных, включающие в себя любую информацию, которая относится прямо или косвенно к субъекту персональных данных;

1.1.6.2. специальные категории персональных данных (расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни);

1.1.6.3. персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (персональные данные, сделанные общедоступными субъектом персональных данных);

1.1.6.4. биометрические персональные данные (сведения, характеризующие физиологические и биологические особенности человека, на основе которых можно установить его личность) (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных). Биометрические персональные данные могут обрабатываться оператором только при наличии письменного согласия субъекта персональных данных (за исключением случаев, установленных в ч.2 ст.11 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

1.1.7. На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Банк включен в реестр операторов, осуществляющих обработку персональных данных.

1.1.8. Настоящая Политика размещена в открытом неограниченном доступе на Интернет-сайте Банка (<https://www.open.ru/about/charter>).

1.1.9. Ответственным за актуализацию документа является Департамент ИТ-эксплуатации.

1.1.10. Настоящий документ относится к направлению деятельности «Информационно-технологическое обеспечение».

1.2. Термины и определения

Ниже приводится список терминов и определений, принятых в рамках данного документа:

Термин	Определение
Автоматизированная обработка персональных данных (ПДн)	Обработка персональных данных с помощью средств вычислительной техники.
Блокирование персональных данных (ПДн)	Временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
Информационная система персональных данных (ИСПДн)	Совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
Обезличивание персональных данных (ПДн)	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.
Обработка персональных данных (ПДн)	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
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.
Персональные данные (ПДн)	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Распространение персональных данных (ПДн)	Действия, направленные на раскрытие ПДн неопределенному кругу лиц.
Территориальное подразделение (ТП)	Территориальная административно-структурная единица филиальной сети Банка. В качестве Территориальных подразделений могут выступать базовый филиал, филиал, дополнительный офис, региональный операционный офис, операционный офис.
Трансграничная передача персональных данных (ПДн)	Передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
Уничтожение	Действия, в результате которых становится невозможным

Термин	Определение
персональных данных (ПДн)	восстановить содержание персональных данных в информационной системе ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

1.3. Сокращения

В данном документе используются следующие сокращения:

Сокращение	Расшифровка сокращения
Банк	ПАО Банк «ФК Открытие»
Архив	Архивное управление Департамента поддержки операционной деятельности Операционного блока
ГО	Месторасположение органов управления Банком, а также его структурных подразделений в г. Москва, за исключением ТП
ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
Политика	«Политика обработки персональных данных» – настоящий документ
Роскомнадзор	Уполномоченный орган по защите прав субъектов ПДн
ФЗ «О персональных данных»	Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»
ЮДК	Юридическое дело клиента - систематизированная подборка информации (документов), содержащее оригиналы и копии документов, предоставленных клиентом (представителем клиента) для открытия/закрытия счета, а также сформированных Банком в процессе обслуживания счета, относящихся к данному клиенту (представителю клиента).

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Принципы обработки персональных данных

2.1.1. Обработка ПДн в Банке осуществляется на основании следующих принципов:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн законным целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Банка;
- соответствия объема и содержания обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- точности 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, содержащих ПДн;
- хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, или устанавливающий срок хранения федеральный закон, договор, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- уничтожения или обезличивание ПДн по достижении целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения ПДн, установленного федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;
- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

2.2. Цели обработки персональных данных

2.2.1. Целями обработки ПДн являются:

- выполнение работ, услуг, функций, полномочий и обязанностей, определенных Уставом, лицензиями и внутренними документами Банка, договорных обязательств Банка перед клиентами, предоставления возможности работникам контрагентов Банка выполнения обязанностей, предусмотренных договорами между Банком и его контрагентами;
- осуществление возложенных на Банк законодательством Российской Федерации функций (в том числе по передаче сведений третьим лицам) в соответствии с законодательством Российской Федерации об исполнительном производстве, Налоговым кодексом Российской Федерации, федеральными законами, в том числе: «Об организации предоставления государственных и муниципальных услуг», «О банках и банковской деятельности», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О несостоятельности (банкротстве)», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О кредитных историях», «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях»;
- организация учета работников Банка для обеспечения соблюдения законов и иных нормативных правовых актов, содействие субъектам ПДн в трудоустройстве, обучении, продвижении по службе, очередности предоставления отпусков, расчета размера заработной платы, использования различных форм страхования, обеспечения пропускного режима Банка, обеспечения личной безопасности работников и сохранности имущества, контроля количества и качества выполняемой работы, пользовании различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, заключенными с субъектами ПДн договорами, а также Уставом и внутренними документами Банка.

2.3. Субъекты персональных данных

2.3.1. Субъектами ПДн в Банке являются:

- соискатели вакантных должностей в Банке;
- действующие и уволенные работники Банка, а также члены их семей;
- физические лица, заключившие или планирующие заключить с Банком гражданско-правовой договор¹;
- представители (работники) клиентов и контрагентов Банка, в том числе представители потенциальных клиентов и контрагентов;
- клиенты-физические лица Банка, в том числе потенциальные;
- аффилированные лица и инсайдеры Банка
- иные физические лица, выразившие согласие на обработку Банком их персональных данных или физические лица, обработка ПД которых необходима Банку для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных на Банк функций, полномочий и обязанностей.

2.4. Состав персональных данных

2.4.1. В процессе своей деятельности Банк осуществляет обработку следующих персональных данных, содержащих любую информацию, которая относится прямо или косвенно к субъекту персональных данных:

- фамилия, имя, отчество (в том числе прежние);
- пол;
- дата и место рождения;

¹ В том числе, физические лица – представители юридических лиц, заключивших или планирующих заключить с Банком гражданско-правовой договор.

- паспортные данные, данные других документов, удостоверяющих личность (серия, номер, дата выдачи, под подразделения, наименование органа, выдавшего документ);
- гражданство;
- статус резидента;
- семейное положение;
- места жительства (адрес регистрации, адрес проживания);
- электронный адрес (e-mail);
- номера контактных телефонов;
- место работы и должность;
- идентификационный номер налогоплательщика;
- номер пенсионного удостоверения;
- информация о счетах, включая информацию об остатках и операциях по ним;
- номера договоров;
- номера кредитных карт;
- иная информация необходимая Банку для осуществления услуг, согласно заключенному договору.

2.4.2. Для лиц, изъявивших желание воспользоваться кредитными продуктами, Банк дополнительно осуществляет обработку следующих персональных данных:

- образование и профессия;
- уровень платежеспособности (уровень дохода);
- данные, содержащиеся в трудовой книжке;
- контактная информация о текущем и предыдущих местах работы;
- информация о составе семьи;
- информация о финансовом состоянии;
- информация об имущественных правах;
- имевшиеся судебные процессы, решения суда об ограничении дееспособности;
- алиментные обязательства;
- иная информация необходимая Банку для осуществления услуг, согласно заключенному договору.

2.4.3. Для лиц, являющихся работниками Банка или проходящих процедуры оформления на работу с целью заключения трудового договора, Банк дополнительно осуществляет обработку следующих персональных данных:

- образование и профессия;
- сведения о воинском учете;
- данные, содержащиеся в трудовой книжке;
- контактная информация о текущем и предыдущих местах работы;
- фотография;
- информация о составе семьи;
- фамилии, имена и отчества, даты и места рождения родственников;
- знание иностранных языков (каких и степень знания);
- другая информация, представленная соискателем в резюме (анкете).

2.4.4. Банк не осуществляет обработку специальных категорий ПДн, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни, судимости физических лиц, если иное не установлено законодательством Российской Федерации. Банк осуществляет обработку специальных персональных данных в части: состояния здоровья, в кадровых системах.

2.4.5. Банк осуществляет обработку сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн).

2.5. Согласие на обработку персональных данных

2.5.1. Получение и обработка ПДн осуществляется Банком с письменного согласия субъекта ПДн.

2.5.2. Письменное согласие субъекта ПДн должно включать:

- фамилию, имя, отчество, адрес субъекта ПДн/представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование и адрес Банка;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка будет поручена такому лицу;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта ПДн;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Банком способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- подпись субъекта ПДн.

2.5.3. 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.

2.5.4. Факт подтверждения согласия путем установки соответствующих флагов/переключателей/нажатия кнопок на экранных веб-формах, подтверждающих согласие субъекта с условиями обработки ПДн при заполнении анкет на официальном сайте Банка в целях получения услуг, предоставляемых Банком, расценивается Банком как согласие на обработку ПДн субъектом, даваемое субъектом в письменном виде.

2.5.5. Согласие на обработку ПДн может быть отозвано субъектом ПДн путем направления в Банк письменного заявления в свободной форме. В этом случае Банк обязуется прекратить обработку, а также уничтожить все имеющиеся в Банке ПДн в сроки, установленные ФЗ «О персональных данных». Банк вправе обрабатывать ПДн без согласия субъекта ПДн (или при отзыве субъектом ПДн указанного согласия) при наличии оснований, указанных в ФЗ «О персональных данных».

2.6. Поручение на обработку персональных данных

2.6.1. Банк вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этой стороной договора (поручения на обработку ПДн). Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О персональных данных».

2.6.2. В поручении Банка должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии с ФЗ «О персональных данных».

2.7. Обязанности ответственных лиц Банка при обработке персональных данных

2.7.1. В целях обеспечения выполнения Банком обязанностей, предусмотренных законодательством Российской Федерации о персональных данных, в банке назначаются:

- должностное лицо, ответственное за организацию обработки ПДн;
- должностное лицо, ответственное за обеспечение безопасности ПДн;
- должностные лица, обслуживающие ИСПДн.

2.7.2. Лицо, ответственное за организацию обработки ПДн, осуществляет общую организацию обработки ПДн, в том числе:

- уведомление уполномоченного органа по защите прав субъектов ПДн об обработке ПДн в соответствии с требованиями ФЗ «О персональных данных»;
- организацию приема и обработки обращений и запросов субъектов ПДн (или их представителей), а также контролирующих органов и контроля за приемом и обработкой таких обращений и запросов;
- организацию процессов повышения уровня осведомленности работников Банка в вопросах обработки ПДн.

2.7.3. Лицо, ответственное за обеспечение безопасности ПДн, осуществляет организацию работ по обеспечению безопасности ПДн и внутренний контроль за соблюдением Банком и его работникам законодательства Российской Федерации в области ПДн.

2.7.4. Должностные лица, обслуживающие ИСПДн, включают работников ДИТ (администраторы системного и прикладного ПО, сетевые администраторы), которые обеспечивают функционирование ИСПДн, а также управление сетевым оборудованием, участвующим в передаче ПДн.

2.7.5. В Банке должен быть утвержден приказом Перечень обособленных подразделений, работники которых имеют доступ к ПДн. Дополнительно ДИБ имеет возможность получить актуальный список работников Банка, имеющих доступ к ПДн.

2.8. Способы обработки персональных данных

2.8.1. Обработка ПДн Банком осуществляется путем их сбора, записи, систематизации, накопления, хранения, уточнения (обновление, изменение), извлечения, использования, передачи (распространение, предоставление, доступ), обезличивания, блокирования, удаления, уничтожения.

2.8.2. Банк осуществляет обработку персональных данных следующими способами:

- автоматизированная обработка (производится при помощи средств вычислительной техники);
- неавтоматизированная обработка (производится без участия средств вычислительной техники);
- смешанная обработка (производится как при помощи средств вычислительной техники, так и без них).

2.8.3. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных законодательством Российской Федерации.

2.8.4. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

2.8.5. В случае необходимости осуществления трансграничной передачи персональных данных Банк, перед совершением такой передачи, обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, а также отсутствии установленных законодательством запретов или ограничений на передачу персональных данных на территорию данного иностранного государства.

2.8.6. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться Банком в случаях:

- наличия согласия в письменной форме субъекта персональных данных;
- исполнения договора, стороной которого является субъект персональных данных;
- в иных случаях, установленных законодательством Российской Федерации.

2.8.7. ПДн при их обработке, осуществляемой без использования средств автоматизации, ПДн обособляются от иной информации, в частности, путем фиксации их на отдельных носителях.

2.8.8. Обработка ПДн, осуществляемая без использования средств автоматизации, проводится таким образом, чтобы обеспечивать раздельное хранение ПДн разных целей обработки.

2.8.9. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы. Для обработки каждой категории ПДн используется отдельный бумажный носитель.

2.8.10. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, в Банке соблюдаются следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации; имя (наименование) и адрес Банка; фамилию, имя, отчество и адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о выдаче указанного документа и выдавшем его органе; фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о выдаче указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя; перечень ПДн, на обработку которых дается согласие субъекта ПДн; наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка; источник получения ПДн; сроки обработки ПДн; перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;
- типовая форма предусматривает поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПДн;
- типовая форма 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;
- типовая форма исключает объединение полей, предназначенных для внесения ПДн, цели, обработки которых заведомо не совместимы.

2.8.11. Уточнение ПДн, обрабатываемых в Банке осуществляется по запросам субъектов ПДн, их законных представителей или в случае обращения уполномоченного органа по защите прав субъектов ПДн.

2.8.12. Основанием для уничтожения ПДн, обрабатываемых в Банке, является:

- достижение цели обработки ПДн;
- прекращение необходимости в достижении цели обработки ПДн;
- отзыв субъектом ПДн согласия на обработку своих ПДн, за исключением случаев, когда обработка указанных ПДн является обязательной в соответствии с законодательством Российской Федерации или договором, либо обработка может осуществляться без согласия субъекта ПДн;
- выявление неправомерных действий с ПДн и невозможности устранения

допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления;

- истечение срока хранения ПДн, установленного законодательством Российской Федерации и нормативными документами Банка;
- предписание уполномоченного органа по защите прав субъектов ПДн (Роскомнадзор) или иного уполномоченного органа.

2.8.13. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае прекращения необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.8.14. Обезличивание ПДн должно осуществляться следующими методами:

- введения идентификаторов, путем замены части сведений идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;
- изменения состава или семантики данных путем их замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;
- декомпозиции, путем разделения множества (массива) данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;
- перемешивания, путем перестановки отдельных значений или групп значений атрибутов данных в массиве данных.

2.8.15. При обработке ПДн в ИСПДн с целью обеспечения безопасности ПДн при наличии технической возможности Банк стремится:

- исключать фиксацию на одном материальном носителе ПДн и иных видов информации, а также ПДн, цели, обработки которых заведомо несовместимы;
- для каждой категории ПДн использовать отдельный материальный носитель.

2.9. Период обработки и хранения персональных данных

2.9.1. Сроки обработки ПДн определяются в соответствии со сроком действия договора с субъектом ПДн, сроком исковой давности, Приказом Министерства культуры Российской Федерации 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», а также иными требованиями законодательства Российской Федерации.

2.9.2. Обработка ПДн начинается – с момента поступления в Банк и прекращается:

- в случае выявления неправомерной обработки ПДн Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты такого выявления, Банк обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Банка. В случае невозможности устранения допущенных нарушений Банк в срок, не превышающий десять рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Банк уведомляет субъекта ПДн или его представителя, а в случае, если обращение или запрос были направлены Роскомнадзором - также этот орган;
- в случае достижения цели обработки ПДн Банк незамедлительно прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн Банк

прекращает обработку ПДн и уничтожает (за исключением ПДн, которые хранятся в соответствии с действующим законодательством) ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва. Об уничтожении ПДн Банк уведомляет субъекта ПДн.

2.9.3. Уничтожение ПДн производится в случаях и в сроки, указанные выше, за исключением ПДн бухгалтерского и кадрового учета, которые хранятся в соответствии с действующим законодательством Российской Федерации.

2.9.4. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в п.2.9.2. настоящей Политики, Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

2.10. Места хранения ПДн (материальные носители)

2.10.1. Хранение персональных данных (материальных носителей) осуществляется в специально отведённых в Банке и Территориальных подразделениях Банка местах хранения персональных данных (материальных носителей) в специальном помещении (специальных сейфах/шкафах), доступ к которому(-ым) ограничен.

2.10.2. Требования к местам хранения ЮДК в Территориальном подразделении установлены в соответствии с «Банковскими правилами по открытию и закрытию банковских счетов, счетов по вкладам (депозитам) физическим лицам - клиентам ПАО Банк «ФК Открытие» [5] и «Банковскими правилами по открытию и закрытию банковских счетов, счетов по вкладам (депозитам), депозитных счетов клиентам ПАО Банка «ФК Открытие» – юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством порядке частной практикой [6].

2.10.3. Требования к местам хранения ЮДК, дел постоянного хранения и дел по личному составу в Архиве Банка, а также требования к архивохранилищам установлены в соответствии с «Порядком формирования, хранения и передачи досье клиентов физических лиц на централизованное хранение в ПАО Банк «ФК Открытие» (ПДК-1161) [8] и «Порядком формирования, оформления дел и передачи их на архивное хранение в ПАО Банке «ФК Открытие» (ПДК-642) [7].

2.11. Перечень лиц, которые осуществляют обработку ПДн и имеют к ним доступ

2.11.1. В состав перечня работников, осуществляющих обработку персональных данных без использования средств автоматизации либо имеющих к ним доступ, входят работники в обязанности которых включено взаимодействие с клиентами и получение от клиентов документов, содержащих персональные данные клиентов, работники, оформляющие личные дела, приказы по личному составу, работники Архива, а также работники структурных подразделений, осуществляющие запрос на предоставление копий документов из ЮДК в Архив Банка, работники в обязанности которых входит проверка корректности клиентских данных.

2.11.2. Запрос и выдача дел и документов во временное пользование осуществляется в соответствии с «Порядком формирования, оформления дел и передачи их на архивное хранение в ПАО Банке «ФК Открытие» [7], «Порядком формирования, хранения и передачи досье клиентов физических лиц на централизованное хранение в ПАО Банк «ФК Открытие» (ПДК-1161) [8].

2.11.3. Перечень работников ГО и Территориальных подразделений Банка, осуществляющих обработку персональных данных клиентов-физических лиц без использования средств автоматизации либо имеющих к ним доступ, определяется в соответствии с «Банковскими правилами по открытию и закрытию банковских счетов, счетов по вкладам (депозитам) физическим лицам - клиентам ПАО Банк «ФК Открытие» (ПДК-1054) [5].

2.11.4. Перечень лиц работников ГО и Территориальных подразделений Банка, осуществляющих обработку персональных данных клиентов-юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой (их представителей), без использования средств автоматизации либо имеющих к ним доступ, определяется в соответствии с Приложением №1 к Приложению №2 к «Банковским правилам по открытию и закрытию банковских счетов, счетов по вкладам (депозитам), депозитных счетов клиентам ПАО Банка «ФК Открытие» – юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством порядке частной практикой [6].

3. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Субъект ПДн имеет право на получение информации, касающейся обработки Банком его ПДн.

3.2 Субъект ПДн вправе 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.

3.3 Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами Российской Федерации, в том числе если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

3.4 Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта ПДн.

3.5 Банк принимает и обрабатывает запросы субъектов персональных данных и предоставляет сведения, подтверждающие факты обработки персональных данных, правовые основания, цели, сроки и способы обработки персональных данных, виды обрабатываемых персональных данных, свое наименование и местонахождение.

4. ОСНОВНЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

4.1 В Банке принимаются следующие меры по обеспечению выполнения обязанностей, предусмотренных ФЗ «О персональных данных»:

- Назначение ответственных за организацию обработки и защиты ПДн;
- издание документов, определяющих политику Банка в отношении обработки ПДн, локальных актов по вопросам обработки и защиты ПДн; Применение правовых, организационных и технических мер по обеспечению безопасности ПДн;
- Осуществление внутреннего контроля и аудита соответствия обработки ПДн требованиям законодательства РФ, настоящей Политике, иным локальным актам Банка;
- Оценка возможного вреда субъектам ПДн, причиненного в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;
- Ознакомление работников, непосредственно осуществляющих обработку ПДн с положениями законодательства РФ о персональных данных, в том числе требованиями к защите ПДн, настоящей Политикой и иными локальными актами Банка по вопросам обработки персональных данных и (или) обучение указанных

работников;

- Обеспечение обработки ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в ФЗ «О персональных данных».

4.2 Обеспечение безопасности ПДн в Банке достигается:

- определением угроз безопасности ПДн при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- обеспечением учета и сохранности носителей ПДн;
- обнаружением фактов несанкционированного доступа к ПДн и принятием мер;
- восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПДн, обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн.

4.3 Меры по обеспечению безопасности ПДн принимаются 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 и направлены на нейтрализацию актуальных угроз безопасности ПДн.

4.4 Состав и содержание организационных и технических мер безопасности ПДн устанавливается в соответствии с внутренними нормативными документами Банка.

5. ОТВЕТСТВЕННОСТЬ

Работники Банка, виновные в нарушении норм, регулирующих обработку и защиту ПДн, установленных в Банке, могут быть привлечены к дисциплинарной, гражданско-правовой, административной или уголовной ответственности в соответствии с законодательством Российской Федерации.

6. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, НА КОТОРЫЕ ДАЮТСЯ ССЫЛКИ

1. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».
2. Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
3. Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. «Банковские правила по открытию и закрытию банковских счетов, счетов по вкладам (депозитам) физическим лицам – клиентам ПАО Банк «ФК Открытие» (ПДК-1054).
6. «Банковские правила по открытию и закрытию банковских счетов, счетов по вкладам

(депозитам), депозитных счетов клиентам ПАО Банка «ФК Открытие» – юридическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством порядке частной практикой» (ПДК-1048).

7. «Порядок формирования, оформления дел и передачи их на архивное хранение в ПАО Банке «ФК Открытие» (ПДК-642).
8. «Порядок формирования, хранения и передачи досье клиентов физических лиц на централизованное хранение в ПАО Банк «ФК Открытие» (ПДК-1161).