ООО КБ "НеваСтройИнвест"

УТВЕРЖДЕНО
Решением Правления № 45/17
от «08» августа 2017 года
Председателя Правления
ООО КБ «НЕВАСТРОЙИНВЕСТ»

_____ /В.Н. Савельев/

ПОЛОЖЕНИЕ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ООО КБ «НЕВАСТРОЙИНВЕСТ»

г. Санкт-Петербург
2017 г

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обеспечении информационной безопасности персональных данных (ПДн) в ООО КБ «НЕВАСТРОЙИНВЕСТ» (далее – Положение) предназначено для применения при организации и непосредственного функционирования процессов обработки персональных данных в Банке, а также при приведении существующих ИСПДн в соответствие требованиям комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и других нормативных документов РФ, в области обработки и обеспечения безопасности ПДн.

1.2. Настоящее Положение разработано ООО КБ «НЕВАСТРОЙИНВЕСТ» (далее – Банк) в целях исполнения требований Федерального закона «О персональных данных» № 152-ФЗ от 27.06.2006, Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России №21 от 18.02.2013г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Модели угроз безопасности ПДн при их обработке в ИСПДн ООО КБ «НЕВАСТРОЙИНВЕСТ» (далее - Модель угроз).

1.3. Требования настоящего Положения распространяются на структурные подразделения и должностные лица Банка, принимающие участие в обеспечении безопасности ПДн.

1.4. Настоящее Положение является общедоступным документом (в соответствии с законодательством Российской Федерации) и определяет содержание и порядок осуществления мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн Банка, представляющие собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку ПДн с использованием средств автоматизации, так и без использования таких средств.

1.5. Настоящее Положение устанавливает требования к сбору, хранению, передаче, использованию, уничтожению и любым другим видам обработки ПДн.

1.6. Настоящее положение не распространяется на ИСПДн, обрабатывающие ПДн, в установленном порядке отнесённые к сведениям, составляющим государственную тайну.

1.7. В соответствии с принятой Моделью угроз в ООО КБ «НЕВАСТРОЙИНВЕСТ» принимается решение о принятии тех или иных организационно-технических мер защиты для безопасности ПДн при их обработке в ИСПДн Банка.

1.8. Обработка ПДн в Банке осуществляется на основе принципов:

- законности целей и способов обработки ПДн – выполнение возложенных на Банк функций, полномочий и обязанностей;

- соответствия целей обработки ПДн целям, заранее определённым и заявленным при сборе ПДн, а также полномочиям Банка;
- соответствия объёма и содержания обрабатываемых ПДн заявленным целям обработки ПДн;
- обеспечение точности, достоверности и актуальности ПДн заявленным целям обработки ПДн, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

1.9. Для обеспечения информационной безопасности ПДн при их обработке в ИСПДн функции мониторинга и контроля защитных мер при обработке ПДн в ИСПДн переданы Службе информационной безопасности Банка.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, И ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Перечень терминов, определений и сокращений представлен в документе «Перечень терминов, определений и сокращений, используемых в ООО КБ «НЕВАСТРОЙИНВЕСТ» при обеспечении информационной безопасности».

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДн

3.1. Основные принципы

Банк, при обработке ПДн в ИСПДн, в соответствие требованиям комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС-1.0-2014, СТО БР ИББС-1.1-2007, СТО БР ИББС-1.2-2014, СТО БР ИББС-1.3-2016) и другими нормативно-правовыми документами, регламентирующими вопросы обеспечения информационной безопасности ПДн, принимает необходимые организационные и технические меры для защиты ПДн от неправомерных действий с ПДн.

Безопасность ПДн при их обработке в ИСПДн достигается путём снижения вероятности осуществления НСД (в том числе случайного) к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иные несанкционированные действия.

При обработке ПДн в ИСПДн должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение НСД к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- непрерывный контроль и анализ уровня защищённости ПДн.

Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты ПДн (СЗПДн), включающей организационные мероприятия и средства защиты информации (СЗИ) (в том числе СКЗИ, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПДн информационные технологии.

Обеспечение безопасности ПДн в Банке осуществляется на основе следующих принципов:

- вовлеченность руководства Банка – деятельность по обеспечению безопасности ПДн инициирована, поддерживается и контролируется руководством Банка;
- соответствие организационных мер и СЗИ актуальным угрозам безопасности ПДн – построение, мониторинг, модернизация СЗПДн в Банке осуществляется на основе анализа угроз безопасности ПДн на текущий момент, с учётом особенностей ИСПДн;
- соответствие организационных мер и СЗИ требованиям нормативно-правовых документов – в Банке используются организационные меры и СЗИ в строгом соответствии с положениями комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и действующими нормативно-правовыми актами РФ в области обработки и защиты ПДн;
- комплексность подхода к безопасности ПДн – с целью обеспечения безопасности ПДн в Банке используется совокупность организационных мер и технических средств защиты;
- патентная чистота – СЗИ, входящие в состав системы защиты ПДн Банка, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей.
- удобство использования – при построении и модернизации системы защиты ПДн в Банке система строится с дружественным к пользователю интерфейсом СЗИ и понятными основными процедурами обеспечения безопасности ПДн;
- постоянное совершенствование – в Банке осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности ПДн, эффективности применяемых организационных мер и технических средств защиты, регулярно анализируется состав актуальных угроз и уровень защищённости ПДн, на основании чего принимаются меры

по устранению выявленных недостатков и совершенствованию системы защиты ПДн.

Достаточность принятых мер по обеспечению безопасности ПДн при их обработке в ИСПДн оценивается при проведении самооценки, аудита и государственного надзора.

Организационные мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн должны включать, в том числе, следующие мероприятия:

- анализ всех АБС для выявления обработки ПДн и отнесение их ИСПДн;
- определение типа ИСПДн и уровня защищённости ПДн в ИСПДн;
- определение типа актуальных угроз безопасности ПДн при их обработке в ИСПДн;
- доработка модели угроз на основе документа «Отраслевая частная модель угроз безопасности ПДн при их обработке в ИСПДн организаций банковской системы Российской Федерации» (СТО БР ИББС-2.4-2010);
- разработку на основе модели угроз системы защиты, обеспечивающей нейтрализацию предполагаемых актуальных угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего уровня защищённости ИСПДн;
- проверку готовности СЗИ, входящих в состав СЗПДн, к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с эксплуатационной и технической документацией к ним;
- обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам эксплуатации СЗИ;
- учёт применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации;
- учёт материальных носителей ПДн, в том числе съёмных носителей ПДн;
- учёт лиц, имеющим допуск к ПДн и лиц, обрабатывающие ПДн в ИСПДн;
- контроль соблюдения условий использования СЗИ, входящих в СЗПДн, предусмотренных эксплуатационной и технической документацией;
- расследование событий, связанных с инцидентами ИБ, таких как несоблюдение условий хранения носителей ПДн, неправильное использование СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищённости ПДн.
- составление заключения по инциденту ИБ и принятие мер по предотвращению подобных нарушений;
- описание состава и режима функционирования компонентов СЗПДн.

Помещения, где размещены компонентов ИСПДн, специальное оборудование, в которых ведётся обработка ПДн, должны быть охраняемыми помещениями, чтобы исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц. В этих помещениях должна обеспечиваться сохранность материальных носителей ПДн и СЗИ, входящих в состав СЗПДн.

Запросы пользователей ПДн на получение ПДн, а также факты предоставления ПДн по этим запросам должны регистрироваться, либо техническими средствами ИСПДн в электронном журнале обращений, либо в журнале обращений субъектов ПДн. Содержание журнала периодически проверяется ответственным сотрудником (администратором безопасности) подразделений информационных технологий или службой ИБ.

Все сотрудники Банка должны быть ознакомлены под подпись с настоящим Положением, а также с изменениями и дополнениями к нему.

3.2. Обеспечение безопасности ПДн по отношению к внутренним нарушителям ИБ

Организационно-технические меры по обеспечению безопасности ПДн от внутренних нарушителей ИБ:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к ПДн;
- строгое избирательное и обоснованное распределение документов и информации, содержащей ПДн, между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключался бы бесконтрольный доступ к ПДн;
- знание сотрудниками требований нормативно-методических документов по обеспечению информационной безопасности в Банке, в том числе по защите ПДн;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- парольный доступ в персональные компьютеры, содержащие ПДн;
- ограничение доступа к сети Интернет с рабочих мест, имеющих доступ к ИСПДн;
- защита доступа к программным средствам ИСПДн паролями доступа;
- установка антивирусного программного обеспечения на рабочие станции и серверы;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором ведётся обработка ПДн в ИСПДн;
- соблюдение порядка уничтожения ПДн;
- своевременное выявление нарушений требований разрешительной системы доступа сотрудниками подразделения;

– разъяснительная работа с сотрудниками по предупреждению распространения, утраты, искажения, изменения, уничтожения ПДн, и ответственности за нарушения правил обработки ПДн.

3.3. Обеспечение безопасности ПДн по отношению к внешним нарушителям ИБ

Организационно-технические меры по обеспечению безопасности ПДн от внешних нарушителей ИБ:

– создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ к ПДн.

– посторонние лица (любое лицо, не имеющее непосредственного отношения к деятельности Банка, посетители, сотрудники других организационных структур) не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в структурных подразделениях, использующих ПДн.

Для защиты ПДн соблюдается ряд мер организационно-технического характера:

– порядок приёма, учёта посетителей;

– технические средства охраны, сигнализации;

– порядок охраны территории, зданий, помещений;

– требования к защите информации при интервьюировании и собеседованиях.

Защита ПДн субъекта от неправомерного их использования или утраты обеспечивается Банком за счёт ее средств в порядке, установленном комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и требованиями нормативных документов РФ.

4. ПОРЯДОК ОБРАБОТКИ ПДн

4.1. Состав и цели обработки ПДн

В ходе анализа процессов обработки ПДн в Банке определяются состав, цели, правовое основание обработки ПДн и сроки хранения обрабатываемых ПДн. В Банке обрабатываются ПДн следующих категорий субъектов ПДн в соответствующих целях:

– Персональные данные сотрудников – в целях обеспечение соответствия требованиям Трудового кодекса и других нормативно-правовых актах РФ, а также ведения учета в кадровом делопроизводстве.

– Персональные данные соискателей на вакантные должности – в целях рассмотрение резюме и отбора кандидатов на вакантную должность для дальнейшего трудоустройства в Банк.

– Персональные данные клиентов – физических лиц – в целях оказания услуг в рамках основной деятельности и исполнения требований законодательства РФ.

- Персональные данные посетителей – в целях принятие решения о допуске на территорию Банка и последующего контроля.
- Персональные данные представителей клиентов – юридических лиц – в целях оказания услуг в рамках основной деятельности и исполнения требований законодательства РФ.
- Персональные данные выгодоприобретателей – физических лиц – в целях исполнения требований законодательства РФ.
- Персональные данные контрагента клиента – в целях исполнения требований законодательства РФ.
- Персональные данные представителей контрагентов – юридических лиц – в целях оказания услуг в рамках хозяйственной деятельности.
- Персональные данные контрагентов физических лиц – в целях оказания услуг в рамках хозяйственной деятельности.

В Банке не допускается и не осуществляется обработка ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и интимной жизни, а также биометрических ПДн.

В Банке допускается обработка ПДн о состоянии здоровья только в рамках предоставления субъектам ПДн услуг по медицинскому страхованию (Банк выступает в роли страхователя), либо другим видам страхования, при которых обработка ПДн о состоянии здоровья является необходимым условием оказания услуги и немедленно прекращается, если устранены причины, вследствие которых они обрабатывались.

Банк получает дополнительное письменное согласие у сотрудников в целях признания ПДн, которыми сотрудника наделяет Банк (должность, рабочие телефоны, рабочий e-mail, стаж работы в Банке) общедоступными.

Данная мера позволяет не получать постоянно дополнительных согласий у сотрудников в случаях необходимости передачи указанных сведений третьим сторонам. Согласие должно содержать Ф. И. О. сотрудника, цель согласия, перечень персональных данных признаваемых общедоступными, а также указано, что данное согласие дает право доступа к указанным персональным данным сотрудника неограниченному кругу лиц, подпись, дата.

4.2. Перечень подразделений допущенных к обработке ПДн

К обработке ПДн допущены сотрудники следующих подразделений Банка:

- Сектор по работе с персоналом – сведения для оформления трудовых отношений;
- Служба экономической безопасности – в соответствии с выполняемыми функциями;
- Отдел бухгалтерского учета, отчетности и расчетов – сведения, используемые при проведении расчетов с сотрудниками;

- Юридический отдел – сведения, необходимые для выдачи доверенностей сотрудникам, для согласования с Банком России назначения сотрудников на должности руководителей, сведения о руководителях Банка, необходимые для предоставления в государственные органы и Банк России в соответствии с федеральными законами и нормативными актами Банка России, сведения о сотрудниках, являющихся аффилированными лицами Банка;
- Служба финансового мониторинга – персональные данные обрабатываемые и передаваемые в рамках законодательства и нормативной документации по противодействию отмыванию доходов и финансовому терроризму;
- Отдел сопровождения некредитных рисков – в рамках хранения и сопровождения юридических дел клиентов;
- Валютный отдел – персональные данные клиентов, необходимые для проведения операций клиентов;
- Отдела анализа кредитных рисков – персональные данные клиентов, указанные в кредитных досье клиентов;
- Отдел кредитного администрирования – персональные данные клиентов, обрабатываемы и передаваемые в бюро кредитных историй в соответствии с требованиями федеральных законов и нормативных актов Банка России;
- Отдел сопровождения ИБС – в рамках настройки технологических процессов обработки и хранения персональных данных;
- Отдел информационных технологий – в рамках настройки технологических процессов обработки и хранения персональных данных;
- Служба информационной безопасности – в рамках контроля за обработкой и хранением персональных данных;
- Отдел по работе с корпоративными клиентами – сведения о персональных данных клиентов, обрабатываемые в ходе их обслуживания;
- Отдел розничного бизнеса – сведения о персональных данных клиентов, обрабатываемые в ходе их обслуживания;
- Подразделения филиала – сведения о сотрудниках, занимающих должности в филиалах в соответствии с компетенцией этих подразделений;
- Сотрудники дополнительных офисов – сведения о персональных данных клиентов, обрабатываемые в ходе их обслуживания;

Указанные подразделения осуществляют обработку ПДн, т.е. осуществляют совокупность любых действий совершаемых с использованием средств автоматизации или без с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение ПДн в объемах и целях, предусмотренных законодательством РФ и внутренними нормативными актами Банка, а также обеспечивают их защиту от неправомерного использования, утраты и несанкционированного уничтожения.

4.3. Требования к обработке ПДн

В целях соблюдения положений комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы РФ» (СТО БР ИББС), а также действующих нормативных документов РФ при обработке ПДн, в Банке установлены следующие обязательные требования:

- обработка ПДн осуществляется с соблюдением Конституции РФ, ФЗ №152 «О персональных данных» и иных нормативно-правовых актов РФ, в целях обеспечения личной безопасности субъекта ПДн и членов его семьи, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- ПДн не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан РФ;
- субъекты ПДн должны быть ознакомлены под подпись с документами Банка, устанавливающими порядок обработки их ПДн, а также их правами и обязанностями в этой области, в соответствии с действующими нормативными документами;
- сбор, хранение, использование, распространение и предоставление ПДн не допускается без письменного согласия субъекта ПДн.

Перед началом обработки ПДн производится обследование информационных систем Банка, определяются все базы данных (хранилища) и отчуждаемые носители информации и содержащиеся в них ПДн. Определяется конфигурация и топология ИСПДн в целом и ее отдельных компонентов, таких как серверное оборудование, автоматизированные рабочие места, общесистемное и прикладное ПО, СЗИ и сетевое оборудование.

С целью определения применения необходимых организационно-технических мер защиты ПДн при их обработке в ИСПДн проводится анализ и оценка вероятности реализации актуальных угроз безопасности и разрабатывается частная модель угроз безопасности ПДн при их обработке в ИСПДн Банка.

4.4. Методы и способы обработки персональных данных

В процессах обработки ПДн в Банке применяются следующие методы:

- автоматизированная обработка;
- обработка без использования средств автоматизации;
- смешанная обработка.

4.4.1. Сбор персональных данных

Банк получает персональные данные из следующих источников:

- непосредственно от субъекта ПДн;

- от третьей стороны, в целях исполнения договорных обязательств или исполнения требований нормативных документов РФ;
- от другого субъекта ПДн, в целях реализации его законных прав.

При получении ПДн не от самого субъекта ПДн, Банк предоставляет субъекту ПДн следующую информацию:

- адрес Банка;
- цели и правовые основания обработки ПДн;
- предполагаемые пользователи ПДн;
- права субъекта ПДн.

В случае получения ПДн не от самого субъекта ПДн и невозможности предоставления ему указанной выше информации, ответственность за уведомление субъекта ПДн, чьи данные передаются, возлагается на лицо, от которого были получены ПДн. Например, при получении ПДн выгодоприобретателей или родственников от сотрудника (страхование сотрудников), ответственность за уведомление выгодоприобретателей или родственников о факте передачи их ПДн возлагается на самого сотрудника.

4.4.2. Накопление персональных данных

Накопление ПДн происходит в результате деятельности Банка.

Банк накапливает ПДн следующими путями:

- копирование оригиналов документов;
- внесение сведений в учетные формы (на бумажные носители и в базы данных автоматизированных систем);
- получение оригиналов документов (трудовая книжка, личный листок по учету кадров, автобиография и пр.).

4.4.3. Хранение персональных данных

Хранение ПДн в Банке осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных документов РФ, связанных с хранением документов, после чего данные могут быть обезличены (при необходимости).

Срок обработки определяется в соответствии с приказом Министерства культуры РФ от 25 августа 2010 г. №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 РФ.

Банк осуществляет хранение ПДн следующими способами:

- на машинных носителях, при автоматизированной обработке ПДн;
- на бумажных носителях, при обработке без использования средств автоматизации.

Порядок учета и хранения носителей ПДн определен во внутренних документах Банка по обеспечению информационной безопасности.

4.4.4. Использование персональных данных

Под использованием ПДн понимаются действия (операции) с ПДн, совершаемые в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта или других лиц либо иным образом затрагивающих права и свободы или других лиц.

В Банке запрещено принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

4.4.5. Распространение и передача персональных данных (взаимодействие с третьими сторонами)

Под передачей ПДн понимаются действия, направленные на передачу ПДн определенному кругу лиц.

Под распространением ПДн понимаются действия, направленные на передачу 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 персональным данным каким-либо иным способом.

При передаче ПДн субъекта Банк обязан соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации;
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;
- не сообщать ПДн сотрудника в коммерческих целях без его письменного согласия;
- персональные данные субъекта могут быть предоставлены родственникам или членам семьи субъекта ПДн по письменному разрешению самого субъекта ПДн;

– не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону.

Банк в ходе своей деятельности осуществляет передачу ПДн третьим лицам в целях исполнения договорных обязательств.

Банк строго определяет круг лиц, допущенных к ПДн. Банк не обнародует персональные данные в средствах массовой информации, и не размещает в информационно-телекоммуникационных сетях.

Доступ третьих сторон к ПДн допускается только с письменного согласия субъекта или без такового в случаях, если такой доступ осуществляется в целях исполнения положений действующих нормативных документов РФ, либо если доступ предоставляется к общедоступным ПДн.

Банком получаются и передаются ПДн в целях исполнения договорных обязательств, а также поручается обрабатывать персональные данные третьей стороне.

Существенным условием договоров о передаче ПДн является обязанность обеспечения сторонами соблюдения конфиденциальности и обеспечение безопасности ПДн при их обработке.

В договорах в обязательном порядке определяется порядок обмена информацией, Банком передаются ПДн только в объеме необходимом для достижения заявленных целей обработки.

Ответственность за соблюдение условий договоров в части обеспечения конфиденциальности и безопасности при обработке ПДн, а также контроля над исполнением этих условий принимающей стороной возложена на руководителя Юридического отдела Банка.

Банк в целях выполнения требований нормативных документов РФ и выполнения условий договорных отношений передает ПДн следующим третьим сторонам:

– Налоговой службе РФ – в целях выполнения требований налогового законодательства, отправки отчетности по сотрудникам Банка. Передаются паспортные данные, финансовая информация (сумма начислений за расчетный период по форме 2-НДФЛ).

– Пенсионному фонду РФ – в целях выполнения требований пенсионного законодательства, отправки отчетности по сотрудникам Банка. Передаются паспортные данные, данные о месте жительства, финансовая информация (сумма начислений за расчетный период, сумма удержанных пенсионных взносов).

– Страховым организациям – в целях получения услуг по страхованию сотрудников Банка. Передаются паспортные данные, данные о месте жительства.

– Кредитным организациям – в целях открытия расчетного счета, оформление банковских карт, перевод денежных средств. Передаются паспортные данные, сведения о банковской карте клиента, данные о месте жительства, контактная информация.

- Центральному Банку РФ – в целях выполнения требований законодательства РФ. Передаются паспортные данные, данные о месте жительства, контактная информация, сведения об ИНН клиента.
- Организациям грузоперевозок – в целях получения курьерских услуг Банком. Передаются контактная информация, данные о месте жительства, контактная информация сотрудника.
- Бюро кредитных историй – в целях получения услуг по формированию, обработке и хранению кредитных историй клиентов Банка. Передаются информация о кредитной истории клиента – сумма кредита, процентная ставка, дата выдачи и погашения, наличие просрочки и т.д.
- Ипотечным агентствам и консалтинговым фирмам – в целях получения услуг по привлечению клиентов. Передаются сведения о клиентах и контрагентах - паспортные данные, информация о кредитной истории, сведения о месте работы, сведения о недвижимости.
- Правоохранительным органам – в целях правоохранительной деятельности Банка.

4.4.6. Обезличивание персональных данных

В Банке может использоваться обезличивание ПДн, в тех процессах, где данную меру возможно осуществить. Обезличивание ПДн организовано таким способом, чтобы не влиять негативным образом на существующие в Банке процессы обработки ПДн.

Обезличивание ПДн освобождает Банк от обеспечения конфиденциальности этих ПДн и сбора дополнительных согласий с субъектов ПДн при совершении различных операций с ПДн.

4.4.7. Блокирование персональных данных

Банк блокирует обрабатываемые ПДн при выявлении недостоверности обрабатываемых сведений или неправомерных действий в отношении субъекта в следующем порядке:

- по требованию субъекта – процедура описана во внутренних документах Банка по обеспечению информационной безопасности;
- по требованию уполномоченного органа по защите прав субъектов (см. раздел 6 «Взаимодействие с органами власти»);
- по результатам внутренних контрольных мероприятий - данная процедура описана во внутренних документах Банка по обеспечению информационной безопасности.

Банк уведомляет субъекта ПДн и (или) уполномоченный орган по защите прав субъектов ПДн о своих действиях по блокированию ПДн.

4.4.8. Уничтожение персональных данных

Банк уничтожает персональные данные в случае:

– достижения целей обработки ПДн или утраты необходимости в их достижении;

– получения соответствующего запроса от субъекта ПДн, при условии, что данный запрос не противоречит требованиям нормативных документов РФ;

– отзыва согласия субъекта на обработку его ПДн (если отзыв согласия влечет за собой уничтожение ПДн);

– получения соответствующего предписания от уполномоченного органа по защите прав субъектов.

Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» БР ИББС и нормативными документами РФ, регламентирующими процесс обработки и обеспечения безопасности ПДн.

Банк может заключать договора с третьими сторонами на оказание услуг по уничтожению материальных носителей. При этом Банк и третья сторона соблюдают все правила для обеспечения конфиденциальности уничтожаемых данных.

Банк сообщает субъекту ПДн и (или) уполномоченному органу по защите прав субъектов об уничтожении соответствующих ПДн в сроки, определенные законодательством РФ.

4.5. Согласие на обработку персональных данных

Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, 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);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

Формы согласий на обработку персональных данных приведены в Приложениях №№ 1-3 настоящего документа.

4.6. Особенности автоматизированной обработки персональных данных

Информационные системы ПДн, позволяющие осуществлять обработку ПДн с использованием средств автоматизации в Банке, выявлены, описаны и классифицированы в порядке, предусмотренном комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и нормативными документами РФ, регламентирующими процесс обработки и обеспечения безопасности ПДн.

В Банке определены критерии отнесения АБС к ИСПДн.

Перечень информационных систем ПДн представлен во внутренних документах Банка по обеспечению информационной безопасности.

4.6.1. Особенности сбора и накопления персональных данных

Банк осуществляет дополнительное накопление ПДн, получаемых по электронной почте или из общедоступных электронных источников (Интернет сайты компаний - рекрутинговых агентств и т. д.).

4.6.2. Особенности использования и распространения персональных данных

При необходимости использования или распространения определенных ПДн отдельно от находящихся на том же машинном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

Распространение и передача ПДн при их обработке в информационных системах осуществляется Банком только по защищенным либо выделенным каналам связи. Банк передает по незащищенным каналам передачи только общедоступные ПДн.

4.6.3. Уничтожение записей, содержащих персональные данные, на машинных носителях

Уничтожение записей, содержащихся на машинных носителях, осуществляется способом, исключающим восстановление уничтоженных ПДн.

Порядок уничтожения носителей, содержащих ПДн, представлен во внутренних документах Банка по обеспечению информационной безопасности.

4.7. Особенности неавтоматизированной обработки (без использования средств автоматизации)

Под обработкой ПДн, осуществляемой без использования средств автоматизации, понимается обработка ПДн, зафиксированных на бумажных носителях.

4.7.1. Особенности сбора персональных данных

В Банк поступают бумажные носители (документы), содержащие ПДн в виде резюме, автобиографий, справок, анкет и пр. Учет и прием документов осуществляется в соответствии с правилами Банка по делопроизводству.

Банк также осуществляет периодический сбор ПДн, путем анкетирования субъектов ПДн, либо запросом дополнительных сведений о субъекте ПДн, в рамках заявленных целей обработки ПДн, не противоречащих положениям действующих нормативных документов РФ в области обработки и защиты ПДн.

4.7.2. Особенности накопления персональных данных

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовая форма), выполняются следующие условия:

- в типовые формы или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы и т. д.) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Банка, фамилия, 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 в Банке способов обработки ПДн;
- в типовую форму включается 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 составляется 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;
- в типовой форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.
- При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Банка или в иных аналогичных целях, соблюдаются следующие условия:
- необходимость ведения журнала (реестра, книги), однократного пропуска, оформляется приказом, содержащим сведения о цели обработки ПДн,

осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию Банка без подтверждения подлинности ПДн, сообщенных субъектом ПДн;

- копирование содержащейся в журналах (реестрах, книгах), однократного пропуска, информации не допускается;
- ПДн каждого субъекта могут заноситься в журнал (книгу, реестр), однократного пропуска, не более одного раза в каждом случае пропуска субъекта ПДн на территорию Банка.

4.7.3. Особенности хранения персональных данных

В Банке обеспечено раздельное хранение ПДн при разных целях обработки и не допускается фиксации на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы. Для обработки каждой категории ПДн используется отдельный бумажный носитель.

4.7.4. Особенности использования и распространения персональных данных

При необходимости использования или распространения определенных ПДн отдельно от находящихся на том же бумажном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

5. ОРГАНИЗАЦИЯ ДОСТУПА СОТРУДНИКОВ К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1. Список сотрудников, имеющих право доступа к работе с ПДн, определен во внутренних документах Банка по обеспечению информационной безопасности.

5.2. Сотрудники Банка получают доступ к ПДн исключительно в объеме, необходимом для выполнения ими конкретных трудовых (должностных) обязанностей.

Сотрудник получает доступ к ПДн после:

- ознакомления и изучения требований настоящего Положения и иных организационно-распорядительных документов на систему обеспечения информационной безопасности в Банке, в том числе по защите ПДн;
- прохождения обучения правилам обеспечения информационной безопасности и обработки ПДн;

- ознакомления с видами ответственности за нарушение/невыполнение требований нормативных документов РФ в области защиты информации, в том числе обработки и защиты ПДн.

5.3. Порядок проведения обучения сотрудников Банка правилам обработки и обеспечения безопасности ПДн в соответствии с внутренними документами Банка по обеспечению информационной безопасности.

5.4. Доступ сотрудников к ПДн осуществляется в соответствии с внутренними документами Банка по обеспечению информационной безопасности, а также перечнем подразделений и сотрудников, допущенных к работе с ПДн в Банке.

5.5. В случае изменений в процессах обработки ПДн, штатной структуре или предоставляемом объеме и правах доступа к ПДн производится пересмотр перечня подразделений и сотрудников, допущенных к работе с ПДн. На СИБ возложена обязанность по поддержанию в актуальном состоянии данного перечня.

5.6. Разовый доступ сотрудника, должность которого не включена в Перечень подразделений и должностных лиц оформляется также в соответствии с документом Банка, определяющим порядок доступа к информации и информационным системам.

5.7. В случае обнаружения нарушений порядка предоставления прав доступа к персональным данным, руководство Банка блокирует предоставленные права доступа к ПДн пользователям до выявления и устранения причин нарушений.

6. ВЗАИМОДЕЙСТВИЕ С ОРГАНАМИ ВЛАСТИ

В целях исполнения законодательства РФ по мотивированному запросу органов власти Банк предоставляет запрашиваемую информацию о субъекте ПДн.

В Банке ответственность за взаимодействие с органами власти по вопросам обработки и защиты ПДн возлагается на СИБ. При необходимости привлекаются и иные подразделения Банка, участвующие в обеспечении ИБ, в том числе ПДн.

6.1. Органы власти, регулирующие область обработки и защиты персональных данных

6.1.1. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как уполномоченный орган по защите прав субъектов ПДн осуществляет федеральный государственный контроль (надзор) за соответствием обработки ПДн требованиям нормативных документов РФ в области обработки и защиты ПДн.

6.1.2. Контроль и надзор за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн, установленных Правительством Российской Федерации, осуществляются Федеральной службой безопасности (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России), в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в ИСПДн.

6.2. Роскомнадзор уполномочен проводить плановые и внеплановые проверки с целью осуществления контроля и надзора выполнения требований нормативных документов РФ в области обработки и защиты ПДн.

6.3. ФСТЭК России уполномочена проводить проверки с целью осуществления контроля и надзора выполнения требований законодательства Российской Федерации в области обеспечения защиты (не криптографическими методами) конфиденциальной информации, предотвращения ее утечки по техническим каналам, и за счет НСД к данной информации.

6.4. ФСБ России уполномочена проводить проверки с целью осуществления контроля и надзора за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности ПДн при их обработке в ИСПДн, в частности за выполнением требований использования шифровальных (криптографических) средств, применяемых для обеспечения безопасности ПДн.

7. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДн

7.1. Стадии создания СЗПДн при их обработке в ИСПДн

Для обеспечения безопасности ПДн при обработке их в ИСПДн создается СЗПДн. СЗПДн включает организационные меры, технические средства защиты информации, а также используемые в ИСПДн информационные технологии, реализующие функции защиты информации. Разработка СЗПДн состоит их следующих стадий:

- предпроектной стадии;
- стадии проектирования;
- стадии приемки и ввода в действие;
- модернизации СЗПДн.

Цели предпроектной стадии:

- определить категории субъектов ПДн, которые обрабатываются в Банке, состав и объем обрабатываемых ПДн, а также цели и правовое основание обработки ПДн и сроки хранения обрабатываемых ПДн;
- определить подразделения и перечень лиц, участвующие в обработке ПДн;
- выделить информационные системы, в которых производится обработка ПДн;
- определить конфигурацию и топологию ИСПДн в целом и ее отдельных компонентов (серверы, АРМ, ПО, СЗИ);
- определить актуальные угрозы безопасности ПДн при их обработке в ИСПДн и разработать частную модель угроз безопасности ПДн при их обработке в ИСПДн Банка;
- определить тип ИСПДн и уровень защищенности ПДн.

По результатам предпроектной стадии определяется степень выполнения требований комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС), в части обеспечения безопасности ПДн, а также разрабатывается план необходимых дальнейших организационных и технических мер по реализации данных требований.

Цели стадии проектирования СЗПДн:

- определить требования по обеспечению безопасности ПДн;
- определить структуру и характеристики создаваемой СЗПДн, состав СЗИ, предполагаемых к использованию в СЗПДн, требования к настройке и эксплуатации этих средств, а также план мероприятий по подготовке СЗПДн к вводу в действие;
- определить требования и регламентировать деятельность сотрудников Банка по организации санкционированной обработки ПДн и обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

Для достижения указанных целей в Банке разрабатывается комплект организационно-распорядительной документации на СЗПДн, описывающей требования и процедуры по управлению и обеспечению безопасности ПДн при их обработке в ИСПДн.

Цели стадии приемки и ввода в действие СЗПДн:

- внедрить технические средства защиты информации;
- проверить работоспособность СЗИ в составе ИСПДн;
- принять организационные меры по обеспечению безопасности ПДн в Банке;
- ознакомить сотрудников Банка с требованиями и обучить порядку обработки и обеспечения безопасности ПДн.

Для достижения перечисленных целей выполняются следующие мероприятия:

- осуществляется закупка, установка и настройка СЗИ, рекомендуется применение сертифицированных СЗИ;
- проводятся предварительные испытания, опытная эксплуатация и приемо-сдаточные испытания СЗИ;
- утверждается и вводится в действие комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности ПДн.
- проводится обучение сотрудников по направлению обеспечения безопасности ПДн: правила автоматизированной обработки ПДн, использования прикладных программ и СЗИ, входящих в состав системы защиты ПДн.

Сотрудники Банка, трудовые обязанности которых предполагают обработку ПДн, в обязательном порядке проходят первичный инструктаж.

Цели модернизации СЗПДн:

- внесение изменений в СЗПДн в связи с выявленными изменениями ИСПДн и устранением недостатков в системе защиты ПДн.

7.2. Организационные и технические меры по обеспечению безопасности ПДн

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мер, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

7.2.1. Организационные меры по обеспечению безопасности ПДн

Организационные меры по обеспечению безопасности ПДн в Банке включают в себя:

- меры по обеспечению охраны и физической защиты помещений, в которых расположены компоненты ИСПДн, исключающие несанкционированный доступ к ТС ИСПДн, их хищение и нарушение работоспособности;
- обучение сотрудников Банка правилам обработки и защиты ПДн.

1. Обеспечение физической защиты

В целях предотвращения несанкционированного входа (вскрытия) в помещения, а также исключения возможности неконтролируемого проникновения в эти помещения посторонних лиц, в Банке организуется и обеспечивается физическая охрана и техническая защита помещений и прилегающей к ним территория, с использованием централизованной системой видеонаблюдения с записью и хранением видеоинформации, где размещаются ИСПДн, обеспечивающие сохранность технических средств обработки ПДн, носителей ПДн и СЗИ.

Защите подлежат следующие типы помещений:

- производственные помещения, в которых осуществляется непосредственно обработка ПДн пользователями ПДн;
- серверные помещения, в которых установлено серверное, сетевое оборудование и технические средства защиты информации;
- архивные помещения, в которых организовано хранение бумажных документов, содержащих ПДн.
- В целях обеспечения физической защиты помещений применяться следующие средства защиты и контроля за несанкционированным вскрытием:
- система контроля и управления доступом – для физической защиты и разграничения доступа в здании;

- двери помещений оборудуются замками для защиты от несанкционированного проникновения и местами для их опечатывания и сдачи под охрану.
- электронные/механические кодовые замки – для физической защиты и разграничения доступа в помещения;
- устанавливаются металлические двери для защиты от несанкционированного проникновения в серверные и архивные помещения.

Доступ в защищаемые помещения осуществляется согласно списку утвержденному Приказом по Банку о лицах, допущенных в защищаемые помещения. Сотрудники, допущенные в защищаемые помещения, несут персональную ответственность за сохранность выданных им карт доступа, ключей и за неразглашение кодов, используемых для входа в защищаемые помещения. Лица, не указанные в списках о лицах, допущенных в защищаемые помещения, при наличии производственной необходимости могут посещать производственные помещения только в сопровождении допущенных лиц.

Контроль обеспечения безопасности помещений, в которых расположены компоненты ИСПДн, возлагается на Администратора безопасности ПДн.

Пребывание посторонних лиц в серверных помещениях допускается в целях производственной необходимости, только в присутствии Администратора безопасности.

Ответственным подразделением за организацию и/или обеспечение физической охраны и технической защиты Банка возлагается на Службу экономической безопасности.

В случае утраты карты доступа, ключа или компрометации кода к замкам в защищаемые помещения предпринимаются следующие меры:

- оповещается Администратор безопасности, руководитель Службы экономической безопасности служебной запиской;
- производится немедленная блокировка карты, замена запираемых замков или смена кода соответственно.
- назначается служебная проверка защищаемых помещений с составлением акта и принятым мерам, виновные лица привлекаются к административной ответственности.

В целях организации противопожарной безопасности, в Банке устанавливается система пожарной сигнализации и пожаротушения.

7.2.2. Технические меры обеспечения безопасности ПДн

Технические меры обеспечения безопасности ПДн при их обработке в ИСПДн включает в себя:

1. Обеспечение управления доступом

Для организации системы допуска и учета лиц, допущенных к обработке ПДн в ИСПДн Банка, должен быть определен перечень лиц, которым для выполнения трудовых обязанностей необходим доступ к ПДн и реализована разрешительная система допуска

пользователей с разграничением прав доступа пользователей к информационным ресурсам, программным средствам обработки и СЗИ. Доступ пользователям ПДн предоставляется в минимально необходимом объеме, с применением парольной защиты.

Предоставление пользователям прав доступа и изменение их полномочий возлагается на Администратора ИСПДн.

2. Обеспечение регистрации и учета

В целях своевременного обнаружения фактов НСД к ПДн в Банке во всех прикладных системах ИСПДн должно быть организовано ведение электронных журналов содержащих информацию:

- о входе/выходе в систему пользователя, дату, время, идентификатор пользователя, результат попытки входа, адрес компьютера, используемого для входа;
- о запросах пользователей прикладных систем на получение ПДн, а также факты предоставления ПДн по этим запросам;
- о печати материалов пользователями системы, дату, время, номер устройства печати, идентификатор пользователя, объем отпечатанного материала, результат печати;
- о запуске программ и процессов, осуществляющих доступ к защищаемым ПДн, дату, время запуска, идентификатор программы и пользователя, запросившего программу, результат попытки запуска, дата и время попытки доступа к защищаемым ПДн, вид запрашиваемой операции (чтение, запись, удаление), результат попытки доступа;
- о изменениях полномочий пользователей, дату, время изменения, содержание изменения, идентификатор Администратора безопасности, осуществившего изменение.

В ИСПДн полномочия по уничтожению и модификации информации, содержащейся в журналах регистрации событий, принадлежат Администратору безопасности. Архивы журналов регистрации событий уничтожаются только Администратором безопасности и не ранее чем через три года с момента появления последней записи в данном архиве.

В Банке должен быть контроль доступа к коммуникационным портам, устройствам ввода-вывода, съемным машинным носителям и внешним накопителям информации ИСПДн Банка.

Администратор ИСПДн периодически (один раз в месяц) предоставляет данные, накапливаемые в электронных журналах, Администратору безопасности для анализа с целью выявления попыток и фактов НСД к ПДн.

Случаи выявления нарушений порядка предоставления ПДн рассматриваются как инциденты информационной безопасности с блокировкой доступа пользователей к ПДн.

В Банке должен вестись учет как съемных (внешние HDD, CD, DVD, BD, Flash-накопители), так и несъемных (HDD) машинных носителей ПДн и должно быть

организовано хранение и использование этих носителей, исключающее их хищение, подмену и уничтожение.

Ответственность за ведение учета носителей ПДн и организацию надлежащего хранения возлагается на Администратора ИСПДн.

Ответственность за обеспечение безопасного уничтожения носителей ПДн возлагается на Администратора безопасности.

3. Обеспечение целостности

Сохранность и целостность программных средств ИСПДн и ПДн являются обязательными и обеспечиваются, в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы, используемые и создаваемые при эксплуатации ИСПДн.

В Банке должен быть определен и документально зафиксирован состав и назначение ПО, используемого в ИСПДн. Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован. С целью недопущения изменения состава ПО ИСПДн, из него должны быть исключены программные средства, предназначенные для разработки и отладки ПО.

В ИСПДн, комплекс средств автоматизации, который включает одно или несколько АРМ, предназначенных для разработки и отладки ПО либо содержащие средства разработки, отладки и тестирования ПО, должны располагаться в сегментах ЛВС, изолированных от сегментов, задействованных в обработке ПДн.

Средства восстановления функций обеспечения безопасности ПДн в ИСПДн должны предусматривать ведение не менее 2 независимых копий программных средств.

В Банке должны быть реализованы механизмы восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним и/или возникновения форс-мажорных ситуаций или воздействия опасных факторов окружающей среды.

Ответственность за организацию своевременного (периодического) резервного копирования и восстановления информации, а также за хранение резервных носителей, содержащих резервные копии данных, возлагается на Администратора ИСПДн.

4. Обеспечение антивирусной защиты

Для предотвращения возможности внедрения в ИСПДн вредоносного программного кода в Банке должны применяться следующие антивирусные средства:

- антивирусные средства, предназначенные для защиты рабочих станций и серверов;
- пограничные антивирусные средства, предназначенные для использования на сетевых шлюзах (в межсетевых экранах, маршрутизаторах, прокси-серверах).

Администратор ИСПДн осуществляет:

- установку антивирусных средств защиты в соответствии с эксплуатационной и технической документацией к ним;

- настройку параметров антивирусных средств защиты согласно требованиям по обеспечению безопасности ПДн.

На Администратора безопасности возлагается контроль соблюдения условий использования антивирусных средств защиты, предусмотренных эксплуатационной и технической документацией, а также своевременное обновление антивирусных баз.

5. Обеспечение криптографической защиты

В Банке должны применяться сертифицированные средства криптографической защиты информации следующего назначения:

- СКЗИ для обеспечения безопасности ПДн, передаваемых по каналам связи между Банком с одной стороны и внешними организациями с другой;
- средства электронной подписи.

СКЗИ, применяемые для защиты ПДн, должны иметь класс не ниже КС2.

В случае обмена информацией с внешней организацией правила использования СКЗИ должны быть определены условиями договора.

В Банке должен вестись учет всех применяемых СКЗИ, эксплуатационной и технической документации к ним, а также учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности ПДн.

На Администратора безопасности возлагается ответственность за обеспечение функционирования и безопасности СКЗИ согласно требованиям руководящих документов ФСБ России.

8. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ПДн

8.1. Контроль состояния защищенности ПДн в Банке осуществляется с целью своевременного выявления и предотвращения утечки ПДн, вследствие НСД к ним, преднамеренных программно-технических воздействий на ПДн и оценки уровня защищенности ПДн (далее - Контроль).

8.2. Контроль эффективности внедренных мер и СЗИ, входящих в состав СЗПДн, должен проводиться в соответствии с требованиями эксплуатационной документации на СЗИ и требованиями других нормативных документов не реже одного раза в год.

8.3. Обязательным является контроль СЗИ, входящих в состав СЗПДн, при вводе их в эксплуатацию после проведения ремонта таких средств, а также при изменении условий и расположения их эксплуатации. Контроль состояния уровня защищенности ПДн в Банке организовывается Администратором безопасности.

8.4. Контроль состояния и эффективности СЗПДн осуществляется в соответствии с планом основных мероприятий по защите информации на текущий год. Результаты периодического контроля оформляются отдельными протоколами или актами.

8.5. По всем выявленным нарушениям требований по защите ПДн Администратор безопасности в пределах своих прав и функциональных обязанностей обязан добиваться их немедленного устранения.

8.6. Руководители структурных подразделений, в чьих компетенциях находятся процессы обработки ПДн, и ответственные за эксплуатацию компонентов ИСПДн обязаны принять все необходимые меры по немедленному устранению выявленных нарушений. При невозможности их немедленного устранения они обязаны прекратить работы с ПДн и организовать работы по устранению выявленных нарушений.

8.7. Сотрудники, осуществляющие обработку ПДн в ИСПДн, обязаны выполнять требования Администратора ИСПДн по устранению допущенных ими нарушений норм и требований по обработке и/или обеспечении безопасности ПДн. Также сотрудники несут персональную ответственность за соблюдение требований по обеспечению безопасности ПДн в ходе проведения работ.

8.8. Учет, хранение и выдача сотрудникам паролей и ключей для системы защиты ПДн от НСД, оперативный контроль действий сотрудников, осуществляющих обработку ПДн, осуществляет Администратор безопасности.

9. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. К инцидентам информационной безопасности, связанным с нарушением требований по обработке и обеспечению безопасности ПДн при их обработке в ИСПДн, относятся любые нарушения, приводящие к снижению уровня защищенности ИСПДн, в том числе несоблюдение условий хранения носителей ПДн и использования СЗИ, которые могут привести к нарушению конфиденциальности, целостности или доступности ПДн.

9.2. В Банке в случаях возникновения подобных инцидентов информационной безопасности осуществляется своевременное устранение нарушений требований по обработке и обеспечению безопасности ПДн, проводятся разбирательства, составляются заключения по фактам возникновения инцидентов, разрабатываются и принимаются меры по предотвращению возможных последствий инцидентов.

9.3. Организация и контроль процесса реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн, возлагается на Администратора безопасности.

9.4. Процедура управления инцидентами информационной безопасности, связанными с нарушением требований по обработке и обеспечению безопасности ПДн, определяет порядок проведения следующих мероприятий:

- определение инцидента информационной безопасности;
- оповещение ответственного лица о возникновении инцидента;
- устранение последствий и причин инцидента;

- расследование инцидента;
- реализация необходимых корректирующих и превентивных мер.

По итогам расследования инцидента информационной безопасности составляется заключение и принимаются административные меры к виновным.

10. МОДЕРНИЗАЦИЯ СЗПДн

10.1. Для определения необходимости модернизации СЗПДн не реже одного раза в год Комиссией по защите ПДн проводится проверка состава и структуры СЗПДн, состава актуальных угроз, типа ИСПДн и уровня защищенности ПДн.

10.2. Модернизация СЗПДн в обязательном порядке проводится в случаях, если:

- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав ПДн, состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- изменился состав актуальных угроз безопасности ПДн в ИСПДн;
- изменился тип ИСПДн или уровень защищенности ПДн.

10.3. Комиссия по защите ПДн ежегодно разрабатывает план работ по обеспечению безопасности ПДн, в котором определяется перечень необходимых мероприятий по обеспечению безопасности ПДн с учетом уже выполненных в Банке мероприятий. В план работ по обеспечению безопасности ПДн включаются организационные и технические меры, направленные на выполнение требований комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и на совершенствование СЗПДн, а также контрольные мероприятия и мероприятия по проведению обучения в Банке. В плане указываются дата, сроки проведения мероприятий, их периодичность (разовые или регулярные) и назначаются ответственные лица за их организацию и выполнение.

10.4. Сотрудники, участвующие в обеспечении безопасности ПДн в Банке вправе формировать предложения по совершенствованию СЗПДн и направлять их на рассмотрение Комиссии по защите ПДн. Комиссия формирует отчет о выполнении плана работ по обеспечению безопасности ПДн.

10.5. Ежегодный отчет по выполнению плана работ включает в себя:

- результаты проведенной проверки состава и структуры, состава актуальных угроз, типа ИСПДн и уровня защищенности ПДн;
- результаты проведенных контрольных мероприятий по защите ПДн;
- результаты проверок регулирующими органами;
- результаты анализа инцидентов информационной безопасности;
- результаты плановых мероприятий по обеспечению безопасности ПДн;

- предложения по совершенствованию СЗПДн на основе полученных результатов.

10.6. На основании решения, принятого руководством, по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн Комиссия по защите ПДн составляет план работ по обеспечению безопасности ПДн на следующий год.

11. ПРИВЛЕЧЕНИЕ СТОРОННИХ ОРГАНИЗАЦИЙ ДЛЯ ПРОВЕДЕНИЯ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

11.1. Банк может привлекаться сторонние организации для проведения следующих мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн:

- разработка нормативно-методических материалов по вопросам обеспечения безопасности ПДн;
- обеспечение сертифицированными СЗИ;
- выполнение организационных и технических мероприятий в области защиты ПДн, на проведение которых у Банка отсутствует соответствующее разрешение, либо отсутствуют технические средства и подготовленные специалисты, либо это экономически нецелесообразно;
- контроль и аудит эффективности проводимых мер по защите ПДн.

Привлекаемая для оказания услуг в области защиты ПДн сторонняя организация должна иметь лицензию на соответствующий вид деятельности.

11.2. Администратор безопасности является ответственным за выбор организации, привлекаемой для проведения мероприятий по созданию или модернизации СЗПДн, проведению контрольных мероприятий, проведению обучения сотрудников Банка по направлению обеспечения безопасности ПДн и формирует предложения для согласования с руководством.

11.3. В заключаемом договоре на проведение сторонней организацией мероприятий по обеспечению безопасности ПДн, на проведение контрольных мероприятий в Банке или на обучение сотрудников по направлению обеспечения безопасности ПДн, существенным условием договора является обязательство привлекаемой организации обеспечить конфиденциальность получаемой информации, ставшей известной в ходе выполнения работ по обеспечению безопасности ПДн в Банке.

11.4. В случае привлечения сторонней организации для проведения мероприятий по созданию или модернизации СЗПДн в договоре прописываются обязательства привлекаемой организации по проведению необходимых организационно-технических мер, включающих в себя:

- организацию и проведение работ по созданию СЗПДн;

- реализацию требований комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и нормативных документов РФ в области обработки и защиты ПДн;
- своевременное совершенствование СЗПДн;
- поддержание работоспособности и сопровождение СЗПДн.

11.5. В случае привлечения сторонней организации для проведения контрольных мероприятий (аудит обеспечения безопасности ПДн) в договоре прописываются обязанности привлекаемой организации по выполнению необходимых работ, включающих в себя:

- проверку выполнения требований комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС) и нормативных документов РФ в области обработки и защиты ПДн;
- оценку обоснованности и эффективности принятых в Банке мер по обеспечению безопасности ПДн.

11.6. В случае привлечения сторонней организации для обучения сотрудников Банка по направлению обеспечения безопасности ПДн, предъявляются следующие требования:

- организация должна иметь лицензию на осуществление образовательной деятельности;
- предлагаемые организацией программы и курсы обучения должны быть согласованы с регулирующими и надзорными органами;
- организация должна иметь возможность проводить обучение на территории Банка или на собственной территории;
- по результатам проведенного обучения организация должна проводить итоговую аттестацию сотрудников;
- организация должна предоставлять отчет для руководства Банка о результатах проведенного обучения.

11.7. Организацией обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн, занимается Администратор ИСПДн. В случае необходимости, ремонт технических средств может быть произведен с привлечением специалистов сторонних организаций на договорной основе с составлением актов выполненных работ.

11.8. Администратором безопасности определяется порядок привлечения сторонних организаций для обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн.

11.9. Обязательным условием при передаче технических средств обработки ПДн и машинных носителей ПДн для осуществления ремонтных работ сторонней организацией является удаление ПДн с носителей, установленных на передаваемых

устройствах, либо извлечение носителей ПДн. Контроль исполнения данного требования возлагается на Администратора безопасности.

11.10. После проведения ремонта средств защиты или средств обработки ПДн, при изменении условий их расположения или эксплуатации обязательно осуществляется проверка готовности этих средств к использованию с составлением заключений о возможности их эксплуатации.

12. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПДн

12.1. Планирование мероприятий по защите ПДн при их обработке в ИСПДн, требования к содержанию плана, порядок разработки, согласования, утверждения и оформления плана, порядок отчетности и контроля над его выполнением определяются действующими нормативными документами РФ.

12.2. План на очередной календарный год разрабатывается Администратором безопасности и определяет перечень основных проводимых организационно-технических мер по защите ПДн с указанием:

- сроков выполнения мероприятий;
- ответственных сотрудников за выполнение соответствующих пунктов Плана.

В План включаются:

- мероприятия по контролю состояния уровня защищенности ПДн;
- мероприятия по обучению и повышению квалификации сотрудников, допущенных к обработке ПДн.

Отчет о результатах выполнения запланированных мероприятий по защите ПДн за текущий год формируется Администратором безопасности и представляется руководству Банка.

13. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

13.1. Права субъекта персональных данных

Субъект ПДн имеет право:

- на полную информацию о своих ПДн и о порядке их обработки;
- требовать исключения, исправления или уточнения своих ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или если они не являются необходимыми для заявленной цели обработки, а также данных, обработанных с нарушением требований нормативных документов РФ;

- при отказе Банка исключить или исправить персональные данные субъекта, он имеет право заявить в письменном виде о своем несогласии с соответствующим обоснованием такого несогласия;
- требовать об извещении Банком всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- определять своих представителей для защиты своих ПДн;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами.

Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.

Банк в целях исполнения положений действующих нормативных документов РФ в области обработки и защиты ПДн, предоставляет доступ субъекту ПДн или его законному представителю к ПДн на основании соответствующего запроса.

Запрос субъекта ПДн должен быть удостоверен одним из следующих способов:

- общегражданским паспортом (заграничным паспортом), с указанием сведений о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя в случае непосредственного обращения субъекта ПДн с запросом;
- электронной подписью - в случае направления электронного запроса.

При предоставлении информации необходимо руководствоваться документом Банка, определяющим порядок реагирования на запросы субъектов ПДн.

Банк предоставляет субъекту информацию:

- о месте нахождения (адрес);
- о факте обработки ПДн;
- цели обработки ПДн;
- способах обработки ПДн;
- о лицах, осуществляющих обработку;
- перечень обрабатываемых ПДн и источник получения ПДн.

Сведения о наличии ПДн должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

Если Банк принимает решения на основании исключительно автоматизированной обработки ПДн, субъект имеет право требовать разъяснений принимаемых решений, о возможных юридических последствиях таких решений, а также заявлять возражения против принимаемых решений.

Ограничение прав субъекта ПДн:

- Банк не предоставляет доступ субъекту ПДн, если предоставление ПДн нарушает конституционные права и свободы других лиц.

13.2. Обязанности субъекта персональных данных

- Субъект ПДн обязан предоставлять Банку достоверные ПДн и своевременно сообщать о произошедших в них изменениях.

14. ПРАВА И ОБЯЗАННОСТИ БАНКА

14.1. Права Банка

Банк имеет право:

- требовать от субъекта ПДн предоставления достоверных сведений о себе в порядке и объеме, предусмотренном законодательством Российской Федерации, а в случае их изменений своевременно уведомлять об этом Банк;
- отказать субъекту или его законному представителю, уполномоченному органу по защите прав субъектов предоставление доступа к информации по формальным признакам в случае несоответствия порядка предоставления запросов от субъектов и (или) уполномоченного органа по защите прав субъектов;
- осуществлять трансграничную передачу ПДн без дополнительного согласия субъекта ПДн в случае, если передаваемые ПДн являются общедоступными или в случае обезличивания ПДн.
- поручать обработку ПДн третьим лицам на договорной основе.

Банк не имеет право:

- получать и обрабатывать ПДн субъекта ПДн о его политических, религиозных и иных убеждениях и частной жизни;
- получать и обрабатывать ПДн субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

14.2. Обязанности Банка

Для защиты ПДн субъектов, Банк обязан:

- обеспечить защиту ПДн субъекта от неправомерного их использования или утраты в порядке, установленном действующим законодательством;
- возложить персональную ответственность за обработку ПДн на сотрудников, допущенных к ПДн и осуществляющих эту обработку, через должностные инструкции сотрудников;
- ознакомить сотрудника с настоящим Положением и его правами в области защиты ПДн под подпись;
- осуществлять передачу ПДн субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

- обеспечить субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий документов, содержащих его персональные данные, за исключением случаев, предусмотренных законодательством;
- по требованию субъекта предоставить ему полную информацию о его ПДн и обработке этих данных;
- разъяснить субъекту ПДн юридические последствия отказа предоставить свои персональные данные, если обязанность предоставления ПДн субъектом установлена федеральным законом (включая налоговое, трудовое право).

В случае выявления недостоверных ПДн или неправомерных действий с ними Банк обязан осуществить блокирование ПДн, относящихся к соответствующему субъекту, или обеспечить их блокирование, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности ПДн Банк на основании соответствующих документов обязан уточнить персональные данные в течение семи рабочих дней и снять их блокирование.

В случае выявления неправомерных действий с персональными данными Банк в срок, не превышающий трех рабочих дней с дня такого выявления, обязан устранить допущенные нарушения или обеспечит их устранение. В случае невозможности устранения допущенных нарушений Банк в срок, не превышающий 10 рабочих дней со дня выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные или обеспечит их уничтожение.

Об устранении допущенных нарушений или об уничтожении ПДн Банк обязан уведомить субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, то и указанный орган.

В случае достижения цели обработки ПДн Банк обязан незамедлительно прекратить обработку ПДн или обеспечить ее прекращение и уничтожить соответствующие персональные данные или обеспечить их уничтожение в срок, не превышающий двадцати рабочих дней со дня достижения цели обработки ПДн, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта ПДн.

В случае отзыва субъектом согласия на обработку своих ПДн Банк обязан прекратить обработку ПДн или обеспечить ее прекращение и уничтожить персональные данные или обеспечить их уничтожение в срок, не превышающий двадцати рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) федеральным законом. Об уничтожении ПДн Банк обязан уведомить субъекта ПДн.

До начала обработки ПДн Банк обязан уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн.

Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной подписью в соответствии с законодательством РФ.

В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных в данном Разделе, Банк осуществляет блокирование таких ПДн или обеспечивает их

блокирование и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

15. ОБЯЗАННОСТИ, ПРАВА И ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ БАНКА ПРИ ОБРАБОТКЕ ПДн

Общее руководство и контроль над выполнением требований данного Положения возложены на СИБ.

Общая организация процессов обработки ПДн сотрудников, членов семьи сотрудников и кандидатов на вакантные должности в соответствии с установленными требованиями и непосредственное руководство указанными процессами в Банке возлагается на руководителя подразделения, обрабатывающего ПДн.

Общая организация прочих процессов обработки ПДн (клиентов, представителей клиентов, контрагентов клиентов, выгодоприобретателей, посетителей и т. д.) в соответствии с установленными требованиями и непосредственное руководство указанными процессами в Банке также возлагается на руководителя подразделения, обрабатывающего ПДн.

15.1. Руководители структурных подразделений Банка

15.1.1. Обязанности

В рамках процессов обработки ПДн, руководители структурных подразделений обязаны:

- обеспечивать выполнение требований по обработке и защите ПДн в соответствии с настоящим Положением и иными руководящими нормативными правовыми актами по обеспечению информационной безопасности, в том числе по защите ПДн;
- осуществлять постоянный контроль над подчиненными, разъяснять и требовать от подчиненных выполнения требований нормативных правовых актов по вопросам обработки и защиты ПДн;
- участвовать в процессе разработки и согласования организационно-распорядительных документов СЗ Банка;
- взаимодействовать с регулирующими органами по вопросам обработки и обеспечения безопасности ПДн;
- определять необходимость и направлять на обучение Пользователей ПДн;
- предоставлять консультации Пользователям ПДн по вопросам автоматизированной и неавтоматизированной обработки ПДн в рамках своих компетенций;
- организовывать и контролировать своевременное предоставление сотрудникам доступа к ПДн и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;

- определять права доступа к ПДн и автоматизированным средствам обработки ПДн в рамках своих компетенций;
- предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности ПДн;
- сообщать о выявленных нарушениях требований настоящего Положения СИБ.

15.1.2. Права

Руководители структурных подразделений, участвующих в процессах обработки ПДн, имеют право:

- формировать предложения по совершенствованию СЗ Банка;
- формировать предложения о необходимости проведения контрольных мероприятий по защите ПДн для СИБ;
- формировать предложения по внесению изменений в организационно-распорядительные документы СЗ Банка;
- запрашивать у сотрудников, участвующих в обработке и обеспечении безопасности ПДн, информацию и документы, необходимые Руководителю в рамках обязанностей, указанных в настоящем Положении;
- участвовать в проведении проверок по обеспечению безопасности ПДн вверенного ему подразделения.

15.2. Сотрудники Банка

15.2.1. Обязанности

Сотрудники Банка, участвующие в процессах обработки ПДн обязаны:

- соблюдать требования организационно-распорядительных документов СЗ Банка по обработке и обеспечению безопасности ПДн;
- проходить обучения и инструктажи по вопросам обработки и обеспечения безопасности ПДн;
- предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении внутренних контрольных мероприятий по защите ПДн;
- сообщать о выявленных нарушениях требований настоящего Положения своему непосредственному руководителю, СИБ.

15.2.2. Права

Сотрудники Банка, участвующие в процессах обработки ПДн имеют право:

- получать доступ к ПДн в рамках выполнения своих трудовых обязанностей;

- получать консультации и рекомендации, по вопросам обработки и обеспечения безопасности ПДн от должностных лиц, ответственных за обеспечение безопасности ПДн в Банке.

15.3. Ответственность должностных лиц

Должностные лица, указанные выше, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением, в пределах, определенных действующим законодательством РФ.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

За несоблюдение требований настоящего Положение законодательством РФ в области ПДн предусмотрена дисциплинарная, административная, гражданская и уголовная ответственность.

Руководство Банка вправе применять предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания.

16. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Настоящее Положение должно пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн, а также требований комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС);
- изменения основных направлений Политики информационной безопасности Банка;
- изменением организационной и технологической инфраструктуры ИСПДн;
- выявления снижения общего уровня ИБ при выполнении банковского информационного технологического процесса, в рамках которого обрабатываются ПДн;
- не реже одного раза в два года (по результатам аудита).

Ответственным за пересмотр настоящего Положения и составление рекомендаций по его изменению является Администратор безопасности.

17. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПДн

Сотрудники Банка, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой и административной

ответственности (ст. 13.11 Кодекса об административных правонарушениях Российской Федерации) в соответствии с федеральными законами.

За нарушение норм, регулирующих получение, обработку и защиту ПДн, должностные лица Банка несут административную ответственность согласно ст. 13.11 Кодекса об административных правонарушениях Российской Федерации, а также возмещают субъекту ПДн ущерб, причиненный неправомерным использованием информации, содержащей его ПДн.

Приложение № 1

ФОРМА

СОГЛАСИЕ
работника на обработку персональных данных

Я, _____
(ф.и.о. работника)

зарегистрированный (ая) по адресу: _____

_____

паспорт серия _____ № _____, выдан _____

_____ в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О защите персональных данных» даю согласие на обработку своих персональных данных ООО КБ «НЕВАСТРОЙИНВЕСТ», расположенному по адресу: 192102, г. Санкт-Петербург, ул. Фучика, дом 4, литер К, пом. 3,4 18Н, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона № 152-ФЗ со всеми данными, которые находятся в распоряжении ООО КБ «НЕВАСТРОЙИНВЕСТ» с целью начисления заработной платы, исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование, представления организацией-работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС РФ, сведений в ФСС РФ, предоставлять сведения в банк для оформления банковской карты и перечисления заработной платы на карты, и третьим лицам для оформления полиса ДМС, а также предоставлять сведения в случаях, предусмотренных федеральными законами и иными нормативно-правовыми актами, следующих моих персональных данных:

1. Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя, отчество (в т.ч. предыдущие),
паспортные данные или данные документа, удостоверяющего личность,
дата рождения, место рождения,
гражданство,
отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения,
данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке,
данные документов о подтверждении специальных знаний,
данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях,
знание иностранных языков,
семейное положение и данные о составе и членах семьи,
сведения о социальных льготах, пенсионном обеспечении и страховании,
данные документов об инвалидности (при наличии),
данные медицинского заключения (при необходимости),
стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
должность, квалификационный уровень,
сведения о заработной плате (доходах), банковских счетах, картах,
адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства,
номер телефона (стационарный домашний, мобильный),
данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ (ИНН),
данные страхового свидетельства государственного пенсионного страхования,
данные страхового медицинского полиса обязательного страхования граждан.

2. Перечень действий, на совершение которых дается согласие:

Разрешаю Оператору (организации-работодателю) производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ, а именно: сбор,

систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных. Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

3. Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данных между Оператором (организацией-работодателем) и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

4. Сроки обработки и хранения персональных данных:

Обработка персональных данных, прекращается по истечении семи лет после окончания трудового договора работника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении (постоянно или 75 лет), а персональные данные работников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

Настоящее согласие действует с «____» _____ 201__г.

_____ /_____/ «____» _____201__г.
(подпись) (Ф.И.О) (дата подписи)

Приложение № 2

ФОРМА

СОГЛАСИЕ НА ПРИЗНАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕДОСТУПНЫМИ[1]

Я,

_____

,

даю согласие ООО КБ «НЕВАСТРОЙИНВЕСТ» на признание указанных ниже персональных данных общедоступными.

1) Перечень общедоступных персональных данных:
- фамилия, имя, отчество;
- дата рождения
- должность (текущая и прежние) в ООО КБ «НЕВАСТРОЙИНВЕСТ»;
- стаж работы в ООО КБ «НЕВАСТРОЙИНВЕСТ»;
- рабочие телефоны;
- рабочий e-mail.

2) Я оповещен о том, что в соответствии с п. 1 ст. 8 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» обеспечение конфиденциальности общедоступных персональных данных не требуется и осознаю, что данное согласие дает право доступа к указанным персональным данным неограниченному кругу лиц.

_____	_____	_____	_____
должность	дата	подпись	расшифровка подписи

[1] Данное согласие составлено в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Приложение № 3

ФОРМА

СОГЛАСИЕ
на обработку персональных данных

Настоящим заявлением я, _____,
(Фамилия, Имя, Отчество клиента полностью)

паспорт _____,
(номер, серия, дата выдачи, орган, выдавший документ)

в целях реализации Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.06.2006 *(далее – Закон о персональных данных)* и в целях рассмотрения Банком вопроса о предоставлении мне кредита, ДАЮ СВОЁ СОГЛАСИЕ на осуществление Банком или его представителями в любое время любых действий, которые необходимы или желаемы для целей рассмотрения Банком вопроса о предоставлении мне кредита (включая, без ограничения: сбор, систематизацию, накопление, хранение, уточнение/обновление/изменение, использование, распространение (в т.ч., передачу), обезличивание, блокирование, уничтожение, трансграничную передачу, а также осуществление любых иных действий с учетом положений Закона о персональных данных) в отношении всех моих персональных данных, а именно: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, и любая иная информация, доступная либо известная в любой конкретный момент времени Банку (далее – Персональные данные). Обработка моих Персональных данных осуществляется Банком с применением следующих основных способов обработки Персональных данных (но не ограничиваясь ими): хранение, запись на электронные носители и их хранение, составление перечней, маркировка.

Я согласен(-на) и уведомлен(-а) о том, что в помещениях Банка ведётся видеонаблюдение и данное изображение используется в целях обеспечения общественной безопасности.

Я подтверждаю, что, давая такое согласие, я действую свободно, по своей воле и в своем интересе.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме. В случае принятия Банком положительного решения по вопросу предоставления мне кредита, настоящее согласие действует до момента заключения между мною и Банком соответствующего кредитного договора.

Я предупрежден(-а), что в случае досрочного отзыва данного согласия до окончания рассмотрения Банком вопроса о предоставлении мне кредита, в предоставление мне кредита Банком будет отказано.

_____ _____
(подпись Заёмщика) *(Фамилия, инициалы Заёмщика)*

«____» _____ 20___г