Микрокредитная компания Фонд развития предпринимательства города Глазова

УТВЕРЖДЕНО
приказом директора МК ФРПГ
от 03.02.2017 г. №3

Положение
о защите персональных данных

г. Глазов 2017г.

Оглавление

Определения и принятые сокращения

Персональные данные (ПД) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информационная система персональных данных (ИСПД) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному сотруднику.

Конфиденциальная информация — сведения, связанные с производственной деятельностью, технологической информацией, управлением, финансами, договорными отношениями, информацией о заказчиках, персональными данными сотрудников.

Несанкционированный доступ - доступ к персональным данным без санкции руководителя организации.

1. Общие положения

1.1 Настоящее положение (далее — Положение) является руководящим документом, обязательным для выполнения работниками МК Фонд развития предпринимательства города Глазова (далее Фонд), наделенными полномочиями по работе с персональными данными (далее — ПД), и определяет организационные и организационно-технические мероприятия по обеспечению безопасности ПД.

1.2 Целями Положения являются:

- обеспечение защиты прав и свобод граждан при обработке их ПД, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- установление порядка защиты ПД в процессе их обработки;
- определение прав, обязанностей и ответственности работников Фонда в части защиты ПД.

1.3 Положение распространяется на персональные данные, перечисленные в утвержденном перечне и переданные Фонду физическими лицами на условиях конфиденциальности в целях их обработки в рамках трудовых и гражданско-правовых отношений.

1.4 Положение разработано на основании следующих правовых и нормативных документов:

- Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (далее — Закон);
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 г. № 149-ФЗ;
- Постановление Правительства РФ от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – ПП № 1119);
- Постановление Правительства РФ от 15.09.08 г. № 687 «Об утверждении Положения об особенностях обработки ПД, осуществляемой без использования средств автоматизации» (далее - ПП № 687);
- Приказ ФСТЭК № 21 от 18.02.13. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- «Базовая модель угроз безопасности ПД при их обработке в ИСПД» Утверждена приказом зам. начальника ФСТЭК РФ 15.02.08 г.;

- «Методика определения актуальных угроз безопасности ПД при их обработке в ИСПД». Утверждена приказом зам. начальника ФСТЭК РФ от 14.02.08 г.;

- «Специальные требования и рекомендации по технической защите конфиденциальной информации». Утверждены приказом Гостехкомиссии России от 30.08.2002 г. № 282.

1.5 Разработка мер по защите информации может осуществляться специализированными организациями на договорной основе, имеющими лицензии ФСТЭК и ФСБ РФ на право проведения соответствующих работ.

1.6 Финансирование мероприятий по защите информации предусматривается сметами организации на планируемый год и обеспечивается директором Фонда.

1.7 Порядок ввода в действие и изменения Положения.

1.7.1 Положение вступает в силу с момента его утверждения директором Фонда и действует до замены его новым положением.

1.7.2 Все изменения и дополнения в положение утверждаются распоряжением директора.

1.8 Все служащие Оператора, обрабатывающие ПД, должны быть ознакомлены с Положением под роспись.

1.9 Положение регламентирует:

- структуру управления процессами построения, функционирования и совершенствования системы защиты ПД (далее — СЗПД);
- порядок определения перечня ПД и общедоступных ПД;
- порядок определения перечня носителей ПД;
- разрешительную систему допуска и доступа к ПД;
- классификацию ИСПД и анализ угроз;
- режимы охраны;
- инженерно-техническую защиту;
- программно-аппаратную защиту;
- криптографическую защиту;
- ролевые функции должностных лиц фонда по защите ПД;
- совершенствование и изменение СЗПД;
- обязанности и права персонала по защите ПД;
- обязанности и права Фонда по защите ПД;
- контроль и надзор за исполнением требований законодательных и нормативных документов;
- ответственность за неисполнение требований законодательных актов.

2. Система защиты персональных данных

2.1 СЗПД строится на основе принципов адекватности, комплексности, непрерывности:

2.1.1 Принцип адекватности — СЗПД должна строиться в строгом соответствии с требованиями к защите, которые определяются категорией или необходимым уровнем защищённости ПД, объемом обрабатываемых данных, классом информационной системы ПД (далее — ИСПД), актуальными угрозами и факторами, влияющими на защиту. Уровень защиты должен быть адекватен угрозам.

2.1.2 Принцип комплексности — использование всего арсенала средств защиты для блокирования актуальных угроз защищаемой информации по всем возможным каналам утечки, по всем направлениям деятельности Оператора.

2.1.3 Принцип непрерывности — построение, функционирование и совершенствование СЗПД является непрерывным процессом.

2.2 Методологическим инструментом разработки СЗПД является системный анализ, включающий в себя анализ (моделирование) всех элементов ИСПД, а именно: анализ объекта защиты, анализ потенциальных угроз и моделирование будущей системы защиты.

2.3 Система защиты информации состоит из следующих компонентов: организационно-правовая, техническая, программно-аппаратная, криптографическая (шифрование).

2.3.1 Организационно-правовая защита — комплекс организационных мероприятий по постановке режима защиты, включающий в себя разработку пакета организационно-распорядительной и нормативной документации, для обеспечения управления процессами обработки и защиты ПД и охрану прав субъектов ПД. Организационная защита включает в себя:

- управление процессами создания и функционирования СЗПД.
- организацию охраны территорий, зданий, помещений, ресурсов;
- разрешительную систему как основу защиты информации;
- организацию защиты ПД при работе с персоналом и клиентами;
- организацию аналитической работы;
- организацию защиты ПД при осуществлении публикаций в открытой печати и рекламной деятельности.

2.3.2 Техническая защита включает в себя:

- инженерно-технические средства защиты — физические барьеры и технические средства охраны (охранная сигнализация периметра объекта и помещений, пожарная сигнализация, системы контроля и управления доступом, системы охранного теленаблюдения);

- технические средства защиты информации от утечки по оптическому, акустическому и электромагнитному каналам утечки информации.

2.3.3 Программно-аппаратная защита от НСД в информационную систему:

- управление доступом, регистрация и учет;
- антивирусные средства;
- межсетевые экраны;
- обнаружение вторжений;
- анализ защищенности информационных систем (сканеры безопасности);

2.3.4 Криптографическая защита включает в себя защиту информации при ее передаче по каналам связи, если необходимость такой защиты будет определена Оператором.

3. Организация работы по исполнению требований закона

3.1 Для управления процессами построения, функционирования и совершенствования СЗПД приказом директора Фонда создана структура управления СЗПД в составе:

- ответственный за обеспечение безопасности персональных данных при их обработке с применением средств автоматизации (администратор безопасности);
- ответственный за обеспечение безопасности при их обработке без использования средств автоматизации;
- постоянно действующая экспертная комиссия по защите персональных данных (далее — ПДЭК);
- комиссии по проведению проверочных мероприятий, формируемые в соответствии с целями и задачами проверок.

3.1.1 Основные функции лиц, ответственных за обеспечение безопасности ПД:

- разработка планов работ по внедрению, поддержке функционирования и совершенствованию системы защиты ПД в соответствии с законодательством РФ в области ПД и нормативными документами уполномоченных органов;
- организация работ в соответствии с утвержденными планами;
- организация внутреннего контроля над соблюдением работниками Фонда требований Закона по защите ПД;

- доведение до сведения персонала Фонда положений законодательства РФ в области ПД, локальных нормативных актов по вопросам защиты ПД (обучение, инструктаж);

3.1.2 Функции лица, ответственного за обеспечение безопасности ПД при их обработке с использованием средств автоматизации (администратор безопасности):

- контроль над соблюдением работниками Фонда требований по защите ПД, при их обработке с использованием средств автоматизации;
- поддержка подсистемы управления доступом, регистрации и учета действий пользователей в ИСПД, контроль над правомерностью их действий;
- администрирование учетных записей пользователей: создание, удаление, разграничение прав доступа, в соответствии с разрешительной системой доступа;
- поддержка подсистемы обеспечения целостности информации в ИСПД;
- поддержка подсистемы антивирусного контроля;
- контроль межсетевого взаимодействия при подключении к сетям общего доступа и международного обмена и при отправке конфиденциальной информации по каналам связи;
- контроль и проведение регулярной смены личных идентификаторов (паролей) доступа пользователей в ИСПД;
- иные функции согласно утвержденной инструкции администратора ИСПД.

3.1.3 Функции лица, ответственного за обеспечение безопасности ПД при их обработке без использования средств автоматизации:

- контроль над соблюдением работниками Фонда требований по защите ПД при их обработке без использования средств автоматизации;
- обеспечение и поддержка конфиденциального документооборота, в части обработки бумажных носителей ПД;
- обеспечение раздельного и защищенного хранения бумажных носителей, содержащих ПД.

3.1.4 ПДЭК является коллегиальным органом Фонда, состав комиссии утверждается распоряжением директора. ПДЭК в своей деятельности руководствуется утвержденным положением о ПДЭК в части защиты персональных данных. Основные функции ПДЭК в части защиты персональных данных:

- разработка планов мероприятий по защите ПД;
- проведение аналитической работы по созданию и совершенствованию СЗПД;
- рассмотрение сведений, вносимых в перечень ПД, и изменение состава сведений;

- организация и проведение работ по контролю эффективности принимаемых мер по защите ПД и подготовка предложений по совершенствованию действующей СЗПД;

- рассмотрение документов выделенных для архивного хранения или уничтожения.

3.1.5 Комиссии по проведению проверочных мероприятий создаются в соответствии с утверждаемым директором Фонда планом проверочных мероприятий по защите ПД. Основными целями проверок является выполнение требований нормативных документов и сохранности носителей ПД. Состав комиссии определяется в каждом случае видом и объемом проверочных мероприятий и утверждается директором Фонда.

3.2 Комиссия в своей деятельности руководствуется утвержденной инструкцией о проведении проверочных мероприятий.

4. Ролевые функции должностных лиц по защите персональных данных

4.1 Директор Фонда:

- утверждает планы мероприятий по обеспечению безопасности ПД
- утверждает состав ПДЭК и комиссий по проведению проверочных мероприятий;
- утверждает перечень ПД и носителей ПД;
- утверждает нормативные документы по обработке и защите ПД;
- выделяет ресурсы для создания и функционирования СЗПД.

4.2 Ответственный за организацию защиты персональных данных:

- координирует работу ПДЭК, отчитывается о результатах директору Фонда;
- организует работу по созданию и эффективному функционированию СЗПД;
- организует разработку организационно-распорядительных и нормативных документов по защите ПД;
- организует контроль состояния СЗПД, соблюдения служащими установленных норм и требований по защите информации;
- организует работу со сторонними организациями в части защиты ПД, в том числе с уполномоченными органами РФ по защите информации и организациями, оказывающими услуги по защите ПД;
- дает предложения по совершенствованию СЗПД.
- дает предложения в Перечень ПД;
- обеспечивает конфиденциальность ПД, обрабатываемых в рамках трудовых отношений, без использования средств автоматизации;

- участвует в работе комиссий в качестве председателя;

4.3 Ответственный за обеспечение безопасности персональных данных при их обработке с применением средств автоматизации (администратор безопасности):

- осуществляет установку, настройку и администрирование программных и программно-аппаратных средств защиты информации;
- контролирует состояние используемых средств защиты информации;
- реализует систему разграничения допуска и доступа в ИСПД при обработке ПД с использованием средств автоматизации;
- обеспечивает выполнение требований по обеспечению безопасности при организации технического обслуживания и отправке в ремонт средств вычислительной техники, на которых ведется обработка ПД;
- ведет учет, хранение, прием и выдачу персональных идентификаторов доступа пользователей в ИСПД;
- осуществляет резервное копирование, хранение и использования резервных и архивных копий баз данных, содержащих ПД и электронных носителей ПД.

4.4 Работники Фонда:

- выполняют требования по защите ПД, при их обработке в рамках исполнения своих должностных обязанностей, согласно нормативным документам Фонда и законодательства РФ.

5. Определение перечня персональных данных, подлежащих защите

5.1 Цели разработки перечня ПД:

- юридическое закрепление факта отнесения ПД к категории защищаемой информации;
- определение срока обработки конкретных ПД;
- определение состава сведений, составляющих ПД, для их последующей структуризации по носителям ПД и разработка матриц доступа служащих к данным носителям;
- выделение документов, содержащих ПД и их носителей в любой форме и организация защищенного документооборота.

5.2 Порядок разработки перечня ПД:

- Работники Фонда подают на рассмотрение ПДЭК предложения по ПД, обрабатываемым в подразделениях, по каждому из направлений деятельности;

- ПДЭК рассматриваем проект перечня ПД на предмет полноты представленных ПД, соответствия целям обработки и наличия избыточных сведений;
- Доработанный ПДЭК перечень ПД утверждается директором Фонда.

5.3 Перечень ПД должен содержать следующую информацию:

- цели обработки;
- категории субъектов ПД;
- правовые основания для обработки;
- сроки и правовые основания хранения (уничтожения) ПД.

5.4 Срок действия и порядок изменения перечня ПД.

5.4.1 Вносить изменения в перечень допускается только на основании мотивированного решения ПДЭК, зафиксированного в протоколе заседания ПДЭК, утвержденного директором.

5.4.2 Действующий перечень ПД регулярно (не реже 1 раза в год) пересматривается с целью исключения ПД, обработка которых прекращена, включения новых ПД, необходимых для осуществления основной деятельности Оператора и изменения целей, сроков обработки и категорий субъектов ПД, если это необходимо.

5.4.3 Предложения по изменению перечня ПД могут вносить работники Фонда и члены ПДЭК. В предложении в обязательном порядке указываются конкретные сведения, цели обработки, категории субъектов ПД, правовые основания для изменения Перечня. Предложения в письменном виде направляются председателю ПДЭК для рассмотрения на заседании ПДЭК и принятии решения.

6. Перечень общедоступных персональных данных

6.1 В целях осуществления уставной деятельности Фонда утверждается список общедоступных ПД, состоящий из сведений, входящих в открытые справочники Фонда, данные публикуемые на сайте и визитные карточки работников Фонда.

6.2 Общедоступные ПД не подлежат защите на законном основании.

6.3 Перечень общедоступных ПД утверждается Директором Фонда.

7. Структуризация перечня персональных данных на носители

7.1 Целью структуризации перечня ПД на носители является определение состава всех типов носителей, содержащих ПД, используемых Фондом.

7.2 Носители ПД подразделяются на материальные (бумажные документы, диски, flash-карты, CD/DVD) и электронные (файлы баз данных, жестких дисков персональных компьютеров, ноутбуков).

7.3 Этапы структуризации перечня ПД:

7.3.1 Первый — определение помещений, в которых обрабатываются ПД (защищаемые помещения).

7.3.2 Второй — определение реестра бумажных, электронных и отчуждаемых носителей для сведений ПД, утвержденных в перечне.

7.3.3 Третий — определение мест хранения носителей ПД относительно границ контролируемой зоны. Границы контролируемой зоны определяются ПДЭК и утверждаются директором Фонда.

7.4 Форма перечня носителей представлена в Приложении 1.

8. Разрешительная система допуска и доступа к персональным данным

8.1 Разрешительная (разграничительная) система представляет собой совокупность организационно-правовых норм и требований, устанавливаемых директором Фонда, с целью обеспечения правомерного ознакомления и использования работниками Фонда персональных данных, необходимых для исполнения своих должностных обязанностей.

8.2 Разрешительная система включает в себя две ограничительные процедуры: допуск работника к обработке ПД и непосредственный доступ к носителям ПД.

8.3 Допуск к защищаемой информации — процедура оформления права работника на обработку персональных данных определенного состава.

8.3.1 Разрешение на допуск дает Директор Фонда в форме отдельного распоряжения или утверждённого трудового договора с соответствующим пунктом. Наличие допуска предоставляет лицу формальное право на работу со строго определенным кругом носителей ПД, согласно его должностными обязанностями.

8.3.2 Оформлению допуска предшествует подписание служащим обязательства о неразглашении ПД. Процедура оформления допуска служащего к обработке ПД всегда носит добровольный характер.

8.3.3 Допуск может быть постоянным или временным на период выполнения служащим определенной работы.

8.4 Доступ к защищаемой информации — практическая реализация служащим, имеющим допуск, права на ознакомление и работу с носителями ПД. Доступ санкционируется Директором.

8.5 Право на доступ служащего Оператора к носителям ПД может быть предоставлено при соблюдении следующих условий:

- наличие распоряжения Директора Фонда о приеме на работу (переводе, назначении на должность);
- наличие подписанного сторонами трудового договора с пунктом (разделом) по защите ПД, или обязательства о неразглашении;
- соответствие должностных обязанностей служащего вверяемым ему носителям ПД;
- знание персоналом нормативных документов Фонда по обработке и защите ПД;
- наличие необходимых условий на рабочем месте для работы с ПД.

8.6 Разрешение на доступ к ПД всегда дается только в письменном виде:

- распоряжением;
- резолюцией на документе;
- списком-разрешением на оборотной стороне документа;
- на основании утвержденной матрицы доступа.

9. Уровень защищенности персональных данных

9.1 Оценка необходимого уровня защищенности ПД проводится в соответствии с Постановлением Правительства № 1119 и включает в себя определение следующих показателей:

- Тип ИСПД, в зависимости от обрабатываемых ПД;
- Категория и количество субъектов ПД;
- Актуальность угроз недекларированных возможностей (далее – НДВ) для ИСПД.

На основании соотношения данных показателей определяется один из четырех уровней защищенности ПД в ИСПД.

9.1.1 ИСПД Фонда является информационной системой, **обрабатывающей иные категории ПД**, т.к. в ней не обрабатываются специальные, биометрические и общедоступные категории ПД.

9.1.2 ИСПД является информационной системой, **обрабатывающей ПД субъектов ПД, не являющихся сотрудниками Оператора, число которых менее 100 000.**

9.1.3 На основании экспертной оценки, вероятность реализации угрозы НДВ для системного ПО и прикладного ПО признана маловероятной согласно утвержденной Модели угроз безопасности ПД, таким образом, **для ИСПД актуальны угрозы 3-го типа.**

9.2 На основании полученных показателей и в соответствии с условием, указанным в части 2 п. 12 Постановления Правительства № 1119, в ИСПД следует обеспечить 4 уровень защищенности ПД.

9.3 Для обеспечения 4-го уровня защищенности ПД при их обработке в ИСПД необходимо выполнение следующих требований:

- Организация режима обеспечения безопасности помещений, в которых размещена ИСПД, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- Обеспечение сохранности носителей ПД;
- Определение перечня лиц, доступ которых к ПД, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.
- Другие требования в соответствии с приказом ФСТЭК № 21 от 18.02.13.

9.3.1 Данные требования по обеспечению 4-го уровня защищенности ПД, предъявляемые к ИСПД Фонда включены в Техническое задание «Информационная система персональных данных в защищенном исполнении».

10. Применяемые методы и способы защиты персональных данных

10.1 В соответствии с требованиями правовых и нормативных документов в Фонде создана СЗПД, состоящая из организационно-правовой, технической защиты, программно-аппаратной и криптографической подсистем.

10.2 Подсистема организационно-правовой защиты представляет собой комплекс распорядительных и нормативных документов, обеспечивающих:

- создание и организацию структуры управления СЗПД;
- организацию контрольно-пропускного;
- организация внутриобъектового режима;
- организацию разрешительной системы;
- защиту информации при работе с персоналом, партнерами;
- аналитические мероприятия по поддержанию СЗПД.

10.2.1 Структура управления СЗПД и функции должностных лиц описаны в разделе 4 настоящего положения.

10.2.2 Контрольно-пропускной режим предусматривает наличие системы контроля доступа при входной группе, оборудованной системой связи и осуществляющей функции препятствия допуску посторонних лиц. Имеется система видеоконтроля внутренних

проходных помещений Оператора и периметра здания. Отдельные помещения Оператора подключены к системе охранной сигнализации.

10.2.3 Внутриобъектовый режим предусматривает допуск служащих в помещения Оператора на основании правил внутреннего трудового распорядка, наличие помещений ограниченного доступа и допуск посетителей под контролем служащих Оператора на местах.

10.2.4 Разрешительная система описана в разделе 8 Положения.

10.2.5 Защита информации при работе с персоналом и третьими лицами включает в себя следующие мероприятия:

- повышенные требования к кандидатам на работу и служащим, участвующим в обработке ПД;
- проведение инструктажей, обучение персонала правилам обработки и защиты ПД;
- проведение плановых мероприятий по проверке исполнения служащими требований по защите ПД;
- в гражданско-правовые договоры с физическими и юридическими лицами включены дополнительные пункты соглашений, по вопросам обработки ПД, в том числе обязательства о неразглашении и обеспечении защиты ПД.

10.2.6 Аналитическая работа включает в себя:

- проведение предпроектных исследований;
- анализ изменений состава ПД и состава носителей ПД;
- анализ изменений компонентов ИСПД;
- анализ изменений состава допущенного персонала;
- анализ угроз безопасности ПД;
- анализ результатов проверочных мероприятий и др.

10.3 Подсистема технической защиты информации включает в себя физические барьеры и технические средства охраны.

10.3.1 Физические барьеры:

- запираемые шкафы и сейфы для хранения носителей ПД.

10.3.2 Технические средства охраны:

- Видеоконтроль, осуществляющийся с камер, установленных в коридорах и помещениях здания;
- Охранная сигнализация помещений;
- «Тревожная кнопка».

10.4 Подсистема программно-аппаратной защиты включает в себя использование штатных средств аутентификации операционной системы Windows Server 2008 R2

Standart код продукта 00477-OFM-8420095-82822 и антивирусной защиты Kaspersky Small Office Security.

10.4.1 В соответствии с приложением к Приказу ФСТЭК № 21 организационные и технические меры защиты информации, обеспечивают:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов к объектам;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

10.4.2 Защита от внедрения вредоносных программ обеспечивается лицензионными средством антивирусной защиты Антивирус Kaspersky Small Office Security.

10.5 Для передачи ПД третьим лицам на законном основании используются следующие криптографические средства:

- для организации межведомственного взаимодействия используется программа шифрования и работы с СКЗИ «Крипто Про».

10.6 Модернизация и изменение СЗПД может производиться в следующих случаях:

- изменение законодательства РФ в части защиты ПД;
- изменение нормативных документов уполномоченных органов (Роскомнадзор, ФСТЭК России, ФСБ России);
- изменение состава ПД и состава носителей ПД;
- изменение технических и программных компонентов ИСПД;
- изменение состава допущенного персонала;
- появления новых актуальных угроз безопасности ПД;
- по результатам проверочных мероприятий и аудита в случае выявления уязвимостей;
- в случае разглашения ПД.

11. Права и обязанности персонала по защите персональных данных

11.1 Работники Фонда обязаны:

- не разглашать сведения, содержащие ПД, ставшие ему известными в ходе выполнения своих должностных обязанностей;
- не передавать третьим лицам и не раскрывать публично сведения, содержащие ПД субъектов ПД, без их письменного согласия;
- выполнять требования распоряжений, положений, инструкций по защите ПД;
- об утрате или недостаче материальных носителей сведений, содержащих ПД субъектов ПД, и о других фактах, которые могут привести к разглашению ПД, а также о причинах и условиях возможной их утечки, немедленно сообщать Директору Фонда, либо ответственному за организацию обработки персональных данных;
- в случае отстранения от службы или перевода на другую должность, работник обязан передать все материальные носители ПД (рукописи, черновики, диски, дискеты, flash-карты и др.), которые находились в его распоряжении в связи с исполнением служебных обязанностей, ответственному за организацию обработки персональных данных.

11.2 Работник Фонда имеет право:

- обращаться для получения консультаций к администратору безопасности по вопросам работы и настройки АРМ;
- указывать на недостатки и вносить предложения по совершенствованию СЗПД;
- обжаловать решения, действия или бездействие ответственных лиц по защите ПД Директору Фонда.
- защищать свои права и законные интересы в судебном порядке.

12. Права и обязанности директора Фонда по защите персональных данных

12.1 Директор обязан:

- планировать и организовывать деятельность по обеспечению безопасности ПД;
- обеспечивать безопасность обработки ПД на всех стадиях их жизненного цикла в соответствии с настоящим Положением и другими нормативными документами;
- контролировать деятельность по обеспечению безопасности ПД;
- финансировать работы по обеспечению безопасности ПД в необходимом объеме.

12.2 Директор имеет право:

- привлекать нарушителей режима защиты ПД к ответственности на законном основании;

- поощрять служащих, добросовестно выполняющих требования по защите ПД и активно участвующих в совершенствовании методов и способов защиты.

- защищать свои права и законные интересы в судебном порядке.

13. Государственный контроль и надзор над исполнением требований закона

13.1 Уполномоченными органами, на которые возлагается обеспечение контроля и надзора исполнения требований закона, являются Федеральная служба по таможенному и экспортному контролю (ФСТЭК), Федеральная служба безопасности (ФСБ) и Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

13.1.1 ФСТЭК осуществляет контроль соответствия технической защиты информации установленным требованиям, включая защиту от утечки по физическим полям и защиту от НСД в ИСПД. ФСБ контролирует криптографическую защиту информации и использование специальных технических средств.

13.1.2 Роскомнадзор осуществляет защиту прав субъектов ПД.

13.2 Проверка Фонда уполномоченными органами может быть проведена по следующим основаниям:

- плановая проверка (контроль соответствия защиты ПД требованиям нормативных документов).

- внеплановая проверка (обращения юридических и физических лиц с жалобами на нарушение закона и прав субъектов, факты разглашения и утечки ПД).

13.3 Роскомнадзор имеет право:

- запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;

- осуществлять проверку сведений, содержащихся в уведомлении об обработке ПД, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

- требовать от директора Фонда уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПД;

- принимать в установленном законодательством РФ порядке меры по приостановлению или прекращению обработки ПД, осуществляемой с нарушением требований Закона;

- обращаться в суд с исковыми заявлениями в защиту прав субъектов ПД, в том числе в защиту прав неопределенного круга лиц, и представлять интересы субъектов ПД в суде;

- направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПД;

- привлекать к административной ответственности лиц, виновных в нарушении Закона.

13.4 Роскомнадзор обязан:

- организовать в соответствии с требованиями Закона защиту прав субъектов ПД;

- рассматривать жалобы и обращения граждан или юридических лиц по вопросам, связанным с обработкой ПД, а также принимать в пределах своих полномочий решения по результатам рассмотрения указанных жалоб и обращений;

- вести реестр операторов;

- осуществлять меры, направленные на совершенствование защиты прав субъектов ПД;

- принимать в установленном законодательством РФ порядке по представлению уполномоченных федеральных органов исполнительной власти меры по приостановлению или прекращению обработки ПД;

- информировать государственные органы, а также субъектов ПД по их обращениям или запросам о положении дел в области защиты прав субъектов ПД.

14. Внутренний контроль и надзор над исполнением требований закона

14.1 Директором Фонда установлена трехступенчатая система контроля выполнения требований по обработке и защите ПД: текущий, периодический и внеплановый контроль.

14.2 Текущий контроль:

- самоконтроль работниками Фонда правил обработки и защиты ПД в ходе исполнения своих должностных обязанностей;

- ежедневное наблюдение, за выполнением работниками Фонда требований по обработке и защите ПД в процессе работы, осуществляемое начальниками структурных подразделений.

14.3 Периодический контроль выполнения требований по обработке и защите ПД осуществляется ПДЭК на основании годовых планов проведения проверочных

мероприятий, утверждаемых директором Фонда.

14.4 Внеплановый контроль - проводится в случаях обнаружения факта разглашения ПД, обнаружения факта утери (утраты) носителя ПД и нарушения процессов обработки ПД.

14.5 Контроль выполнения требований по обработке ПД осуществляется в соответствии с инструкцией о проведении проверочных мероприятий.

14.6 Если по результатам проверки выявляются грубые нарушения требований по защите информации или выявляется факт нанесения ущерба субъекту ПД или Оператора, организуется служебное расследование.

15. Ответственность за неисполнение требований закона

15.1 Лица, виновные в нарушении требований Закона, несут предусмотренную законодательством Российской Федерации ответственность.

15.2 Моральный вред, причиненный субъекту ПД вследствие нарушения его прав, нарушения правил обработки ПД, установленных Законом, а также требований к защите ПД, установленных в соответствии с Законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПД убытков.

Приложение 1

Форма перечня носителей персональных данных

ПЕРЕЧЕНЬ

носителей персональных данных

№ п/п	Документ	Должность (ФИО) / Тип и размещение носителей		
		Электронный носитель*	Бумажный носитель	Отчуждаемый носитель
1.	Личная карточка	АРМ – 2	Начальник отдела; сейф	-
2.	Книга учета трудовых книжек и вкладышей в них	-	Начальник отдела; запираемый шкаф	-
3.	Копия документа об образовании	-	Начальник отдела; запираемый шкаф	-
4.	…	…	…	…

* Маркировка носителей в соответствии с утвержденными схемами размещения носителей относительно границ контролируемой зоны.