УТВЕРЖДАЮ
Директор
МКК «Фонд поддержки
предпринимательства»
_____ П.В. Гришанов

Приказ № 16-ОД от «28» 08 2022 г.

ПОЛИТИКА
в отношении обработки персональных данных
Микрокредитной компании Фонд поддержки предпринимательства

Редакция № 1

Заречный, 2022

Оглавление

1. ОПРЕДЕЛЕНИЯ

Наименование термина	Определение термина
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
Безопасность информации	состояние защищенности информации, характеризуемое способностью технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами
Блокирование персональных данных	временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Вирус (компьютерный, программный)	исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению
Вредоносная программа	программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных
Доступ к информации	возможность получения информации и ее использования
Защищаемая информация	информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Информационная система персональных данных	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Источник угрозы безопасности информации	субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации
Накопитель информации	устройство, предназначенное для записи и (или) чтения информации на носитель информации. Накопитель информации конструктивно может содержать в себе неотчуждаемый носитель информации, либо может быть предназначен для использования сменных носителей информации. Накопители подразделяются на встроенные (в конструктиве системного блока) и внешние (подсоединяемые через порт). Встроенные накопители подразделяются на съемные и несъемные
Нарушитель безопасности персональных данных	физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке (в том числе техническими средствами) в информационных системах персональных данных
Несанкционированный доступ (несанкционированные действия)	доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств,

Наименование термина	Определение термина
	аналогичных им по своим функциональному предназначению и техническим характеристикам
Носитель информации	физический объект, предназначенный для хранения информации
Обезличивание персональных данных	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
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
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
Перехват (информации)	неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов
Персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Пользователь информационной системы персональных данных	лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования
Предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Система защиты персональных данных	комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в ИСПДн
Технические средства информационной системы персональных данных	средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации
Технический канал утечки информации	совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

Наименование термина	Определение термина
Трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
Угрозы безопасности персональных данных	совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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
Утечка (защищаемой) информации по техническим каналам	неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации
ИСПДн	информационная система персональных данных
НСД	несанкционированный доступ
ПДн	персональные данные
Политика	политика в отношении обработки персональных данных
СЗПДн	система защиты персональных данных
ТЗКИ	техническая защита конфиденциальной информации
ТС	техническое средство

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Настоящая Политика устанавливает порядок организации и проведения работ по защите информации в ИСПДн, создаваемых и эксплуатируемых в Компании.

2.2. Требования настоящей Политики распространяются на защиту информации с ограниченным доступом, отнесенной к информации, составляющей ПДн.

2.3. Политика является дополнением к действующим в РФ нормативным документам по вопросам обеспечения информационной безопасности ПДн, и не исключает обязательного выполнения их требований.

2.4. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн организации, а также нормативных и методических документов, обеспечивающих ее реализацию.

2.5. Политика определяет следующие основные вопросы защиты информации:

- цели сбора персональных данных;
- правовые основания обработки персональных данных;
- объем и категории обрабатываемых персональных данных, категории субъектов персональных данных;
- основные принципы и требования по защите информации, составляющей ПДн;
- порядок и условия обработки персональных данных;
- актуализацию, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным;
- порядок организации и проведения работ по защите информации, составляющей ПДн;
- порядок обеспечения защиты информации при эксплуатации ИСПДн;

– порядок организации делопроизводства, хранения и обращения накопителей и носителей информации.

3. ЦЕЛИ СБОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Сбор персональных данных осуществляется в целях:

– ведения хозяйственной деятельности согласно законодательству Российской Федерации;

– обеспечения соблюдения законодательных и иных нормативных правовых актов РФ и локальных нормативных актов Компании;

– исполнения обязанностей, возложенных законодательством РФ на Компанию, в том числе связанных с представлением ПДн в налоговые органы, Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования, Территориальный фонд обязательного медицинского страхования, а также в иные государственные органы;

– регулирования трудовых отношений с работниками, трудоустройства, контроля количества и качества выполняемой работы, обеспечения сохранности имущества;

– формирование кадрового резерва Компании;

– предоставления работникам Компании и членам их семей дополнительных гарантий и компенсаций, в том числе добровольного медицинского страхования, негосударственного пенсионного обеспечения и других видов социального обеспечения;

– подготовки, заключения, исполнения и прекращения договоров с контрагентами или субъектами ПДн (в том числе о предоставлении займа);

– исполнения актов государственных органов или должностных лиц;

– реализации прав и законных интересов в рамках ведения видов деятельности, определенных для Компании;

– в иных законных целях.

4. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Правовыми основаниями обработки ПДн являются:

– трудовые договоры или иные соглашения между Компанией и работником либо иным субъектом ПДн;

– договоры и иные документы, формируемые в рамках производственно-хозяйственной деятельности Компании, получения товарно-материальных ценностей и отгрузки продукции;

– законодательство Российской Федерации, в том числе Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», и др.;

– согласие субъекта ПДн на обработку ПДн.

5. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В Компании обрабатываются следующие категории персональных данных:

– персональные данные сотрудников в объеме менее 100000 субъектов персональных данных;

– персональные данные соискателей в объеме менее 100000 субъектов персональных данных;

– персональные данные посетителей в объеме менее 100000 субъектов персональных данных;

– персональные данные контрагентов в объеме менее 100000 субъектов персональных данных.

5.2. Персональные данные сотрудников Компании:
– фамилия, имя, отчество;
– год, месяц, дата и место рождения;
– паспортные данные (данные документа, удостоверяющего личность);
– семейное, социальное положение;
– идентификационный номер налогоплательщика (ИНН);
– страховое свидетельство;
– номер медицинского полиса;
– адрес проживания и регистрации;
– образование;
– квалификация, наличие специальных знаний, ученой степени, звания;
– профессия (специальность);
– сведения о трудовом и общем стаже;
– сведения о предыдущем месте работы;
– сведения о составе семьи;
– сведения о воинском учете;
– сведения о заработной плате;
– сведения о социальных льготах;
– сведения о награждениях, почетных званиях;
– занимаемая должность;
– имущественное положение;
– наличие судимостей;
– номер личного (домашнего, мобильного) телефона;
– электронная почта;
– содержание трудового договора;
– фотография (изображение гражданина);
– социальные льготы, социальный статус;
– график работы;
– сведения об особом характере труда;
– должностной разряд, класс, тарифная ставка;
– сведения о повышении квалификации, переподготовках, об аттестациях;
– сведения о приеме, переводах, увольнении;
– сведения о трудовой дисциплине;
– сведения об отпусках;
– сведений о страховом стаже и начисленных страховых взносах;
– сведения о должностном окладе, надбавках, доплатах;
– сведения о доходах;
– послужной список;
– информация о поощрениях;
– сведения, направляемые в органы статистики;
– сведения об инвалидности;
– сведения о результатах медицинского обследования на предмет годности к осуществлению трудовых обязанностей, обучению; сведения о заболеваниях, нетрудоспособности; информация об ограничениях и потребностях по здоровью;
– рекомендации, характеристики и иные сведения, необходимые для корректного документального оформления правоотношений с оператором.

5.3. Персональные данные соискателей:
- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- адрес места жительства;
- адрес регистрации;
- телефонный номер (домашний, рабочий, мобильный);
- информация об образовании (наименование образовательного учреждения, период обучения, специальность, квалификация по диплому);
- информация о трудовой деятельности до приема на работу;
- информация о трудовом стаже (место работы, должность, основные обязанности, количество подчиненных, период работы, причины увольнения);
- сведения о наличии личного автотранспорта.

5.4. Персональные данные посетителей:
- фамилия, имя, отчество;
- адрес регистрации;
- паспортные данные (серия, номер паспорта, кем и когда выдан).

5.5. Персональные данные контрагентов:
- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- паспортные данные (данные документа, удостоверяющего личность);
- семейное, социальное положение;
- идентификационный номер налогоплательщика (ИНН);
- основной государственный регистрационный номер (ОГРН);
- страховое свидетельство;
- адрес проживания и регистрации;
- образование;
- профессия (специальность);
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- сведения о заработной плате;
- сведения о социальных льготах;
- сведения о занимаемой должности;
- имущественное положение;
- наличие судимостей;
- номер личного (домашнего, мобильного) телефона;
- электронная почта;
- содержание трудового договора;
- фотография (изображение гражданина);
- сведения о доходах;
- рекомендации, характеристики и иные сведения, необходимые для корректного документального оформления правоотношений с оператором.

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка (сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) ПДн

субъектов ПДн в Компании осуществляется с использованием баз данных, находящихся на территории Российской Федерации в соответствующем законодательству Российской Федерации порядке.

6.2. Субъект ПДн обязан:

– передавать оператору достоверные, документированные ПДн, состав которых установлен законодательством РФ (в том числе Трудовым кодексом РФ, Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», и т.д.);

– в случае изменения сведений, содержащих ПДн (фамилия, имя, отчество, адрес, паспортные данные, сведения об образовании, семейном положении, состоянии здоровья (при выявлении противопоказаний для выполнения служебных обязанностей (работы, обучения), обусловленных служебным контрактом (трудовым договором), или иных, своевременно (как правило, в 3-дневный срок) сообщать о таких изменениях оператору ПДн.

6.3. Доступ к ПДн субъектов ПДн разрешается только специально уполномоченным лицам, при этом указанные лица могут получать только те ПДн субъектов ПДн, которые необходимы для выполнения конкретных функций.

6.4. Руководитель Компании определяет перечень лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование ПДн субъектов ПДн и несущих ответственность за нарушение режима защиты этих ПДн в соответствии с законодательством Российской Федерации.

6.5. Все лица, в функциональные (должностные) обязанности которых входит получение, обработка и защита ПДн субъектов ПДн в ИСПДн оператора ПДн, при приёме на работу обязаны подписать обязательство о неразглашении ПДн.

6.6. Обработка ПДн допускается в следующих случаях:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

– обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (исполнение судебного акта);

– обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

– обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных

данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», при условии обязательного обезличивания персональных данных;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

6.7. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни - не осуществляется.

6.8. Обработка специальных категорий ПДн, касающихся состояния здоровья - не осуществляется.

6.9. Обработка персональных данных о судимости может осуществляться в случаях и в порядке, которые определяются в соответствии с федеральными законами.

6.10. Срок обработки ПД.

6.10.1. Персональные данные сотрудников Компании – в течение действия трудового договора и 75 лет после завершения действия трудового договора.

6.10.2 Персональные данные соискателей – 5 лет.

6.10.3. Персональные данные посетителей – постоянно.

6.10.4. Персональные данные контрагентов – постоянно.

6.10.5. Условием прекращения обработки персональных данных является достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

6.11. Компания (Оператор) вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обязанность по запросу оператора персональных данных в

течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии с настоящей статьей, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе требование об уведомлении оператора о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

6.12. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

7. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации оператором, а обработка должна быть прекращена, согласно статьей 20, 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7.2. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора).

Персональные данные подлежат уничтожению, если:

– иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

– оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или иными федеральными законами;

– иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.

7.3. Оператор обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу субъекту персональных данных.

8. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

8.1. Защита информации, составляющей ПДн должна осуществляться в соответствии со следующими основными принципами:

– законность — предполагает обеспечение защиты ПДн в соответствии с действующим в РФ законодательством и нормативными актами в области защиты ПДн. Пользователи и обслуживающий персонал ИСПДн должны быть осведомлены о правилах и порядке работы с защищаемой информацией и об ответственности за их нарушение;

– системность — предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн;

– комплексность — предполагает согласованное применение разнородных средств и систем при построении комплексной системы защиты информации, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях;

– непрерывность — предполагает функционирование СЗПДн в виде непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры, не допускающие переход ИСПДн в незащищенное состояние;

– своевременность — предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности;

– совершенствование — предполагает постоянное совершенствование мер и средств защиты информации на основе комплексного применения организационных и технических решений, квалификации персонала, анализа функционирования ИСПДн и ее системы защиты с учетом изменений условий функционирования ИСПДн, появления новых методов и средств перехвата информации, изменений требований нормативных документов по защите ПДн;

– персональная ответственность — предполагает возложение ответственности за обеспечение безопасности ПДн и ИСПДн на каждого исполнителя в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей исполнителей строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму;

– минимальная достаточность — предполагает предоставление исполнителям минимально необходимых прав доступа к ресурсам ИСПДн в соответствии с производственной необходимостью, на основе принципа «запрещено все, что не разрешено явным образом»;

– гибкость системы защиты — предполагает наличие возможности варьирования уровнем защищенности при изменении условий функционирования ИСПДн;

– обязательность контроля — предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации. Контроль за деятельностью каждого пользователя, каждого средства защиты и в отношении каждого объекта защиты должен осуществляться на основе применения средств контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

9. ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

9.1. Компания (Оператор) и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

9.2. Компания (Оператор) обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных указанным Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено другими федеральными законами.

9.3. Компания (Оператор) при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

9.4. Защита информации в ИСПДн является неотъемлемой составной частью управленческой и научной деятельности Компании и должна осуществляться во взаимосвязи с другими мерами по защите информации, составляющей ПДн.

9.5. Защита информации является составной частью работ по созданию и эксплуатации ИСПДн и должна осуществляться в установленном настоящей Политикой порядке и реализовываться в виде системы (подсистемы) защиты ПДн.

9.6. Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет НСД к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее санкционированной доступности и работоспособности ТС.

9.7. В ИСПДн должны использоваться сертифицированные по требованиям безопасности информации средства защиты информации и (или) технические и организационные решения, исключающие утечку информации по техническим каналам, за счет НСД, предупреждающие нарушение целостности информации и ее санкционированной доступности.

9.8. Защита информации должна быть дифференцированной в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую ПДн, утвержденной для ИСПДн модели угроз и установленного уровня защищенности ИСПДн.

9.10. Все используемые в ИСПДн средства защиты информации должны быть проверены на соответствие ограничениям и условиям эксплуатации, изложенным в сертификате соответствия, эксплуатационной документации или формуляре (для технических и программных средств защиты информации соответственно).

9.11. Обработка информации, составляющей ПДн в ИСПДн осуществляется на основании письменного разрешения (приказа) руководителя Компании.

9.12. Ответственность за обеспечение выполнения установленных требований по защите информации возлагается на руководителя Компании, в котором создается (совершенствуется) и эксплуатируется ИСПДн.

9.13. Все ИСПДн должны пройти оценку эффективности принимаемых мер по обеспечению безопасности ПДн до начала обработки информации, составляющей ПДн.

10. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

10.1. Организация работ по защите информации возлагается на руководителя Компании, осуществляющего разработку (модернизацию) и (или) эксплуатацию ИСПДн.

10.2. Организация и проведение работ по защите информации, составляющей ПДн на различных стадиях разработки, внедрения и эксплуатации ИСПДн определяется действующими в РФ нормативными документами и настоящим документом.

10.3. Проведение работ по защите информации, составляющей ПДн, осуществляется силами Компании, в которой создается (совершенствуется) ИСПДн. В случае невозможности или нецелесообразности выполнения работ по защите информации силами Компании к этим работам должна привлекаться специализированная организация, имеющая соответствующие лицензии на право выполнения работ и оказания услуг по технической защите конфиденциальной информации.

10.4. Стадии создания системы защиты информации:

– предпроектная стадия — включает предпроектное обследование создаваемой ИСПДн, разработку аналитического обоснования необходимости создания системы защиты информации и технического задания на ее создание;

– стадия проектирования (разработки проектов) и реализации ИСПДн — включает разработку СЗПДн в составе ИСПДн;

– стадия ввода в действие системы СЗПДн — включает опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку эффективности принимаемых мер по обеспечению безопасности ПДн.

11. ПОРЯДОК ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ИСПДН

11.1. Эксплуатация ИСПДн должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией ИСПДн.

11.2. Ответственность за обеспечение защиты информации в процессе эксплуатации ИСПДн возлагается на руководителя Компании.

11.3. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИСПДн возлагается на непосредственных исполнителей ИСПДн (пользователей, администраторов, обслуживающий персонал).

11.4. За нарушение установленных требований по защите информации руководитель Компании и (или) непосредственный исполнитель привлекаются к ответственности в соответствии с действующим в РФ законодательством.

12. ПОРЯДОК ОРГАНИЗАЦИИ ДЕЛОПРОИЗВОДСТВА, ХРАНЕНИЯ И ОБРАЩЕНИЯ НАКОПИТЕЛЕЙ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

12.1. Все накопители и носители информации, содержащие ПДн на бумажной, магнитной, магнито-оптической и иной основе, используемые в технологическом процессе обработки информации в ИСПДн, подлежат учету, хранению и обращению в соответствии с требованиями конфиденциального делопроизводства.

12.2. Организация и ведение учета накопителей и носителей ПДн, организация их хранения, обращения и уничтожения осуществляются ответственными делопроизводителями конфиденциального делопроизводства.

12.3. ПДн, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

12.4. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

12.5. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

12.6. Обработка ПДн без использования средств автоматизации должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

12.7. Должно обеспечиваться раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

12.8. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ. Контроль состояния и эффективности защиты ИСПДн.

12.9. В ИСПДн должен осуществляться контроль и (или) аудит соответствия обработки ПДн действующим в РФ законодательству и требованиям к защите ПДн, а также настоящей Политике и локальным актам Компании.

12.10. Контроль заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер и оценке эффективности принятых мер по обеспечению ПДн.

12.11. Контроль подразделяется на оперативный и плановый (периодический).

12.12. В процессе эксплуатации ИСПДн в целях защиты информации от НСД осуществляются оперативный контроль и периодический контроль за выполнением исполнителями требований действующих нормативных документов по вопросам обеспечения безопасности и защиты ПДн.

12.13. С целью своевременного выявления и предотвращения утечки информации, исключения или существенного затруднения НСД и предотвращения специальных воздействий (программно-технических и др.), вызывающих нарушение целостности информации или работоспособность технических средств, в ИСПДн Компании проводится плановый периодический (не реже одного раза в год) контроль состояния защиты информации.

12.14. При проведении плановых проверок осуществляется контроль ведения учетной документации, защищенности ИСПДн от утечки ПДн по техническим каналам, выборочный контроль содержимого накопителей и носителей информации, и т.п.

12.15. Результаты контроля оформляются актами, заключениями и записями в эксплуатационной документации.