

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ
В МИКРОКРЕДИТНОЙ КОМПАНИИ ФОНД ПОДДЕРЖКИ РАЗВИТИЯ
АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА ГОРОДСКОГО ОКРУГА
«ГОРОД ЯКУТСК»

I. Общие положения

1.1. Положение об обработке и защите персональных данных сотрудников (далее - Положение) в Микрокредитной компании Фонд поддержки развития агропромышленного комплекса городского округа «город Якутск» (далее по тексту – Фонд) определяет политику, цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Фонде.

1.2. Настоящее Положение определяет действия Фонда как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.3. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Федеральными законами от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Обработка персональных данных в Фонде осуществляется с соблюдением принципов и условий, предусмотренных настоящим Положением и действующим законодательством Российской Федерации в области персональных данных.

1.5. Перечень должностей Фонда, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утверждается приказом Генерального директора Фонда.

II. Условия и порядок обработки персональных данных

2.1. Персональные данные кандидатов на работу, работников Фонда и физических лиц

обрабатываются в целях оказания услуг, выполнения функций, указанных в уставе Фонда, функций работодателя, обеспечения кадровой работы, в том числе в целях содействия трудовой деятельности, формирования кадрового резерва, обучения и должностного роста, учета результатов исполнения работниками Фонда должностных обязанностей, обеспечения личной безопасности работников Фонда и членов их семей, обеспечения работниками Фонда установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, сохранности имущества, а также в целях противодействия коррупции.

2.2. В целях, указанных в пункте 2.1 настоящего Положения, обрабатываются следующие категории персональных данных кандидатов на работу, работников Фонда и физических лиц:

2.2.1. Фамилия, имя, отчество (в том числе прежние фамилии, имена и (или) отчества в случае их изменения, причина изменения).

2.2.2. Пол.

2.2.3. Число, месяц, год рождения.

2.2.4. Место рождения, данные свидетельства о рождении.

2.2.5. Информация о гражданстве (в том числе предыдущие гражданства, иные гражданства).

2.2.6. Вид, серия, номер, документа, удостоверяющего личность на территории Российской Федерации, наименование органа, выдавшего документ, дата выдачи.

2.2.7. Адрес места жительства (адрес регистрации и фактического проживания, дата регистрации по месту жительства).

2.2.8. Номер контактного телефона или сведения о других способах связи.

2.2.9. Семейное положение, реквизиты свидетельств государственной регистрации актов гражданского состояния.

2.2.10. Состав семьи, данные свидетельств о рождении детей (при наличии).

2.2.11. Сведения о близких родственниках (в том числе бывших).

2.2.12. Реквизиты страхового свидетельства государственного пенсионного страхования.

2.2.13. Идентификационный номер налогоплательщика.

2.2.14. Реквизиты страхового медицинского полиса обязательного медицинского страхования.

2.2.15. Сведения о трудовой деятельности.

2.2.16. Сведения о трудовой деятельности, в том числе: дата, основания поступления на работу и назначения на должность, дата, основания назначения, перевода, перемещения на иную должность, наименование замещаемых должностей с указанием структурных подразделений, а также сведения о прежнем месте работы).

2.2.17. Отношение к воинской обязанности, сведения по воинскому учету.

2.2.18. Сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

2.2.19. Сведения об ученой степени, ученом звании.

2.2.20. Информация, содержащаяся в контракте (трудовом договоре), дополнительных соглашениях к контракту (трудовому договору).

2.2.21. Сведения, указанные в оригиналах и копиях приказов по личному составу.

2.2.22. Фотография.

2.2.23. Личная подпись.

2.2.24. Место работы, должность.

2.2.25. Сведения, содержащиеся в материалах по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям.

2.2.26. Сведения о заработной плате (номера расчетного счета и банковской карты, данные договоров, размер денежного содержания).

2.2.27. Сведения, содержащиеся в копиях решений судов.

2.2.28. Сведения, подаваемые в налоговую инспекцию, пенсионный фонд, фонд социального страхования и другие учреждения.

2.2.29. Сведения, содержащиеся в регистрах бухгалтерского учета и внутренней бухгалтерской отчетности.

2.2.30. Данные водительского удостоверения.

2.2.31. Иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.1 настоящего Положения.

2.3. Обработка персональных данных осуществляется с согласия граждан, данные которых обрабатываются, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.4. Обработка специальных категорий персональных данных не осуществляется.

2.5. Обработка персональных данных осуществляется при условии получения согласия граждан в следующих случаях:

2.5.1. При передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации.

2.5.2. При трансграничной передаче персональных данных.

2.5.3. При принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

2.6. В случаях, предусмотренных пунктом 2.5 настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.7. Обработка персональных данных кандидатов на работу, работников Фонда и физических лиц, включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, представление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем:

2.8.1. Получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы).

2.8.2. Копирования оригиналов документов.

2.8.3. Внесения сведений в учетные формы (на бумажных и электронных носителях).

2.8.4. Формирования персональных данных в ходе кадровой работы и работы с физическими лицами.

2.8.5. Внесения персональных данных в информационные системы Фонда.

2.9. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от кандидатов на работу, работников Фонда физическими лицами, иных законных источников.

2.10. В случае возникновения необходимости получения персональных данных кандидатов на работу, работников Фонда, физических лиц, у третьей стороны, следует известить об этом кандидата на работу, работника Фонда, физического лица, либо заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

2.11. Запрещается получать, обрабатывать и приобщать к личному делу персональные данные, не предусмотренные пунктом 2.2 настоящего Положения, и действующим законодательством, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.12. При сборе персональных данных работник, осуществляющий сбор (получение) персональных данных непосредственно от кандидатов на работу, работников Фонда, физических лиц, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа представить их персональные данные.

2.13. Передача (распространение, представление) и использование персональных данных кандидатов на работу, работников Фонда, физических лиц, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

III. Порядок обработки и защиты персональных данных субъектов персональных данных в информационных системах

3.1. Обработка персональных данных в Фонде осуществляется на законной и справедливой основе.

3.2. Классификация (определение уровня защищенности) информационных систем персональных данных Фонда, осуществляется в порядке, установленном законодательством Российской Федерации.

3.3. Работникам Фонда, имеющим право осуществлять обработку персональных данных в информационных системах Фонда, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе Фонда. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями работников.

Информация вносится в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

3.4. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Фондом, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

3.4.1. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3.4.2. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.

3.4.3. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации.

3.4.4. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

3.4.5. Учет машинных носителей персональных данных.

3.4.6. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

3.4.7. Восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

3.4.8. Установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Фонда, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

3.4.9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

3.5. Ответственными за выполнение требований по защите персональных данных при их обработке в информационных системах персональных данных являются лица, назначенные приказом Генерального директора Фонда, эксплуатирующих, а также использующих информационные системы, пользователи информационных систем, администратор безопасности.

Администратор безопасности принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

3.6. Обмен персональными данными при их обработке в информационных системах персональных данных Фонда осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения сертифицированных программных и технических средств.

3.7. Доступ работников, допущенных к обработке персональных данных,

предусматривает обязательное прохождение процедуры идентификации и аутентификации пользователя.

3.8. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Фонд уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

IV. Сроки обработки и хранения персональных данных

4.1. Сроки обработки и хранения персональных данных определяются в соответствии с законодательством Российской Федерации.

4.2. Сроки обработки и хранения персональных данных, представляемых субъектами персональных данных, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

4.3. Персональные данные граждан, обратившихся в Фонд лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в течение 5 (пяти) лет с момента прекращения трудовых отношений.

4.4. Персональные данные, представляемые субъектами на бумажном носителе хранятся на бумажных носителях в соответствующих структурных подразделениях, к полномочиям которых относится обработка персональных данных в соответствии с действующими нормативными актами.

4.5. Персональные данные при их обработке, осуществляющейся без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на разных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

4.6. Необходимо обеспечивать раздельное хранение персональных данных на разных материальных носителях, обработка которых осуществляется в различных целях, определенных настоящим Положением.

4.7. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляют руководители структурных подразделений.

4.8. Срок хранения персональных данных, внесенных в информационные системы персональных данных Фонда, должен соответствовать сроку хранения бумажных оригиналов.

V. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

5.1. Оценкой вреда, который может быть причинен субъектам персональных данных, в случае нарушения требований по обработке и обеспечению безопасности персональных данных является определение юридических или иным образом затрагивающих права и законные интересы последствий в отношении субъекта персональных данных, которые могут возникнуть в случае нарушения требований по обработке и обеспечению безопасности персональных данных.

5.2. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав субъектов персональных данных или иным образом затрагивающие их права, свободы и законные интересы.

5.3. В целях недопущения нарушения и обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также определения соотношения вреда, который может быть причинен субъектам персональных данных при обработке персональных данных должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы

ПЕРЕЧЕНЬ
ПДн сотрудников обрабатываемых в Фонде

1.1. Перечень (далее – «Перечень») ПДн сотрудников, подлежащих защите в Фонде, разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и внутренними документами Фонда.

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. В Фонде сведениями, составляющими персональные данные (далее – «ПДн») сотрудника, является любая информация, относящаяся к прямо или косвенно к сотруднику Фонда (субъекту ПДн) - физическому лицу, в том числе:

2.1.1. ПДн специальной (первой) категории.

2.1.1.1. Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья клиентов Фонда.

2.1.2. ПДн общей (третьей) категории, за исключением ПДн, относящихся к специальной категории и к обезличенным, общедоступным, биометрическим ПДн.

2.1.2.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.2.2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.1.2.3. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

2.1.2.4. Номера телефонов (мобильного, рабочего и домашнего).

2.1.2.5. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения).

2.1.2.6. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения).

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

2.1.2.8. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

2.1.2.9. Сведения о заработной плате.

2.1.2.10. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет).

2.1.2.11. Сведения о семейном положении (состояние в браке).

2.1.2.12. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

2.1.2.13. Сведения об идентификационном номере налогоплательщика.

2.1.2.14. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

2.1.3. Общедоступные ПДн (четвертой категории).

2.1.3.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.3.2. Номера телефонов (мобильного и домашнего).

2.1.3.3. Иные сведения, являющиеся общедоступными или сделанные таковыми с письменного согласия клиента.

**ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
КЛИЕНТОВ В МИКРОКРЕДИТНОЙ КОМПАНИИ ФОНД ПОДДЕРЖКИ
РАЗВИТИЯ АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА ГОРОДСКОГО
ОКРУГА «ГОРОД ЯКУТСК»**

1. Общие положения

Настоящее Положение об обработке и защите персональных данных клиентов (далее – Положение) устанавливает общую политику, порядок и условия проведения работ по обработке персональных данных (далее - ПДн) клиентов – индивидуальных предпринимателей, юридических лиц и их представителей (далее - клиенты) в Микрокредитной компании Фонд поддержки развития агропромышленного комплекса городского округа «город Якутск» (далее по тексту - Фонд) с использованием средств автоматизации и без использования таких средств.

Положение разработано с целью обеспечения защиты прав и свобод субъекта персональных данных (далее - субъект ПДн) при обработке его ПДн, а также с целью установления ответственности должностных лиц Фонда, имеющих доступ к ПДн его клиентов, за невыполнение требований и норм, регулирующих обработку ПДн.

Данное Положение разработано в соответствии с требованиями:

- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства Российской Федерации от 6 июля 2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
- Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации»;

Настоящее Положение вступает в силу с момента его утверждения директором Фонда и действует бессрочно до замены его новым Положением или до наступления иных случаев, предусмотренных законодательством.

Настоящее Положение является обязательным для исполнения всеми сотрудниками Фонда, имеющими доступ к ПДн клиентов – субъектов ПДн. Все сотрудники Фонда, связанные с обработкой ПДн и имеющих доступ к ПДн клиентов, должны быть ознакомлены с настоящим Положением под роспись.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам

проверок в рамках государственного контроля (надзора), а также в целях закрепления наработанной Фондом практики операций с ПДн.

Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм настоящего Положения возлагается на назначаемого приказом по Фонду сотрудника, ответственного за организацию обработки ПДн.

При появлении новых типов ПДн допускается разграничение доступа к ним на основании приказа директора Фонда.

Фонд учитывает требования настоящего Положения при разработке и утверждении любых внутренних документов Фонда, связанных с обработкой ПДн.

2. Основные понятия и определения

В Положении применяются термины и определения в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

«Положении об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации», утвержденном Постановлением Правительства РФ от 15 сентября 2008 года № 687, другими нормативно-правовыми актами, регулирующими защиту прав субъектов ПДн и обеспечение безопасности ПДн.

3. Состав ПДн

ПДн клиентов Фонда – это любая информация, относящаяся к прямо или косвенно определенному или определяемому клиенту Фонда (субъекту ПДн) - физическому лицу (индивидуальному предпринимателю). Перечень ПДн, обрабатываемых в Фонде (далее – Перечень ПДн), приведен в Приложении 1.

В ходе осуществления Фондом своих функций Перечень ПДн может быть изменен.

При получении ПДн, не указанных в Перечне ПДн, указанные данные подлежат немедленному уничтожению лицом, непреднамеренно получившим указанные данные.

4. Специальные категории ПДн

Запрещается обрабатывать ПДн о политических, религиозных и философских убеждениях, а также об интимной жизни клиента Фонда. Указанные специальные категории ПДн в деятельности Фонда не используются и не обрабатываются.

Фонд не вправе производить обработку данных о судимости клиента, за исключением в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Сведения о расовой и национальной принадлежности клиентов Фонда не обрабатываются. Фотографии, находящиеся в документах, удостоверяющего личность клиента Фонда, и иные аналогичные данные не относятся к сведениям о расовой и национальной принадлежности.

В случае если обработка специальных категорий ПДн клиента Фонда необходима по действующему законодательству или для осуществления деятельности Фонда, то такая обработка осуществляется с письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

5. Биометрические ПДн

Фонд не обрабатывает сведения, которые характеризуют физиологические особенности клиентов и на основе которых можно установить их личность. В соответствие с требованиями ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Данные изображения лица» система охранного видеонаблюдения, используемая в Фонде, не обрабатывает биометрические ПДн, на основании которых возможно идентифицировать личность клиента Фонда.

Сканирование фотографий в документах, идентифицирующих личность клиентов (например, в паспортах), в Фонде не осуществляется. Передаваемые в рамках договоров с определенными третьими копии паспортов клиентов не соответствуют требованиям,

предъявляемым к форматам записи изображения, установленными ГОСТ Р ИСО\ МЭК 19794-5-2006.

В случае если обработка биометрических ПДн клиента Фонда необходима по действующему законодательству или для осуществления деятельности Фонда, то такая обработка осуществляется с письменного согласия клиента, за исключением случаев, предусмотренных законодательством Российской Федерации в области ПДн.

6. Общедоступные ПДн

В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия клиента могут включаться его фамилия, имя, отчество, год и место рождения, адрес, включая адрес электронной почты, клиентский номер, IP-адрес, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн или находящиеся в Перечне ПДн.

Сведения о клиенте Фонда должны быть в любое время исключены из общедоступных источников ПДн по запросу клиента либо по решению суда или иных уполномоченных государственных органов.

В случае обработки общедоступных ПДн клиента обязанность доказывания того, что обрабатываемые ПДн являются общедоступными, возлагается на Фонд.

7. Цели и сроки обработки ПДн

Фонд обрабатывает ПДн с целью осуществления возложенных на Фонд законодательством Российской Федерации функций в соответствии с (в том числе, но не ограничиваясь), Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности, «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О несостоятельности (банкротстве) кредитных организаций», «О персональных данных», «О бухгалтерском учете», принятими в их исполнение нормативными актами Правительства России, а также в соответствии с нормативными актами Банка России и в иных целях в рамках действующего законодательства. Фонд собирает ПДн только в объеме, необходимом для достижения названных целей.

Допускаются иные цели обработки ПДн в случае, если указанные действия не противоречат действующему законодательству, деятельности Фонда и на проведение указанной обработки получено согласие клиента Фонда.

Хранение ПДн осуществляется в течение 5 (пяти) лет с момента исполнения обязательств по договору займа в полном объеме.

8. Обработка ПДн

Фонд осуществляет обработку ПДн в целях соблюдения законодательных и нормативных актов, минимизации финансовых рисков (включая сохранность активов и ресурсов Фонда), зависящих от ПДн клиента.

Обработку ПДн осуществляют сотрудники Фонда, уполномоченные на то должностными инструкциями, иными внутренними документами Фонда или организационно-распорядительными документами по Фонду.

Сотрудники Фонда имеют право получать только те ПДн, которые необходимы им для выполнения конкретных должностных обязанностей.

Сотрудники Фонда, осуществляющие обработку ПДн клиентов, должны быть проинформированы о факте такой обработки, об особенностях и правилах такой обработки, установленных нормативно-правовыми актами и внутренними документами Фонда.

В рамках информирования сотрудников Фонда о факте обработки ПДн, Фонд обязывает сотрудников Фонда самостоятельно изучать и соблюдать внутренние нормативные документы, регламентирующие как общий порядок работы с ПДн, так и специальные нормы, касающиеся совершения отдельных действий, связанных с обработкой ПДн клиентов Фонда.

9. Согласие на обработку ПДн

Обработка ПДн клиентов осуществляется с их согласия на обработку их ПДн, а также в иных случаях, предусмотренных статьей 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Согласие на обработку ПДн может быть дано клиентом или его законным представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя клиента полномочия данного представителя проверяются Фондом. Форма согласия может быть в письменной, конклюдентной или иной форме, предусмотренной действующим законодательством.

При недееспособности клиента письменное согласие на обработку его данных дает его законный представитель.

Фонд обязан иметь доказательство получения согласия клиента на обработку его ПДн (в том случае, если такое согласие является необходимым).

9.1. Письменная форма согласия

В случаях, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта персональных данных.

Согласие клиента на обработку его ПДн в Фонде должно включать в себя сведения и информацию, требующуюся для включения в согласие в соответствии с действующим законодательством и внутренними документами Фонда.

9.2. Конклюдентная форма согласия

В соответствии со статьей 158 Гражданского кодекса Российской Федерации конклюдентное или подразумеваемое согласие – это действия лица, выражющие его волю установить правоотношение (например, совершить сделку), но не в форме устного или письменного волеизъявления, а поведением, по которому можно сделать заключение о таком намерении.

Клиенты Фонда дают конклюдентное согласие на обработку их ПДн в случаях, описанных в Таблица 1.

Таблица 1. Случаи обработки ПДн на основании конклюдентного согласия

Вид обработки ПДн	Цель обработки	Обрабатываемые ПДн
Заполнение анкет, в т.ч. и на Web-сайте Фонда.	Изучение возможностей по получению и обслуживанию кредита.	п.2.1.3 Перечня ПДн
Регистрация на Web-сайте и мероприятиях, проводимых Фондом	Уведомление о мероприятиях, акциях, предоставляемых скидках	Фамилия, имя, отчество, контактная информация.
Участие в опросах, проводимых Фондом.	Проведение опросов и исследований в области финансовых услуг, проведения маркетинговых программ, статистических исследований.	п.2.1.3 Перечня ПДн.

9.3. Отзыв согласия

Клиент Фонда может в любой момент отозвать свое согласие на обработку ПДн при условии, что подобная процедура не нарушает требований законодательства РФ и допускается условиями договора, одной из сторон по которому является Фонд, а клиент является либо другой стороной по договору, либо выгодоприобретателем, либо поручителем, либо залогодателем.

В случае отзыва клиентом Фонда согласия на обработку ПДн Фонд вправе продолжить обработку ПДн без согласия клиента при наличии оснований, указанных в пунктах 2 - 11

части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9.4. Обработка ПДн без согласия

В соответствии с пунктами 2 - 11 части 1 статьи 6, а также пунктом 4 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» обработка ПДн может осуществляться без согласия. В Фонде к таким ситуациям относятся те, которые указаны в Таблице 2.

Таблица 2. Случаи обработки ПДн без согласия (по состоянию законодательства на дату утверждения Положения)

Вид обработки ПДн	Основание
Заключение договора с клиентом	Ст.6.1.5 ФЗ-152
Взаимодействие с Пенсионным фондом РФ	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с налоговыми органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с таможенными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Федеральной службой финансового мониторинга	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Банком России	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами предварительного следствия	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами внутренних дел	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с судебными органами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие со Счетной палатой Российской Федерации	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Федеральным органом исполнительной власти в области финансовых рынков	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с Фондом социального страхования Российской Федерации	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с органами принудительного исполнения судебных актов, актов других органов и должностных лиц	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с организациями, осуществляющими функции по обязательному страхованию вкладов	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с лицами, указанными клиентом Фонда в завещательном распоряжении	Ст.6.1.1 ФЗ-152, ст.26 ФЗ ФЗ- 395-1 и ст.1128 ГК РФ
Взаимодействие с нотариальными конторами	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Взаимодействие с иностранными консульскими учреждениями	Ст.6.1.1 ФЗ-152 и ст.26 ФЗ ФЗ- 395-1
Заполнение анкет и заявок на получение займов	Ст.6.1.5 ФЗ-152
Оформление договоров аренды, лизинга, доверительного управления, в которых клиент Фонда указан как	Ст.6.1.5 ФЗ-152

Идентификация клиентов в рамках законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма

Расчет платежными поручениями

Ст.6.1.1 ФЗ-152 и ФЗ-115

Ст.6.1.1 ФЗ-152 и ст.863 ГК РФ, а также Положения

10. Порядок обработки ПДн с использованием средств автоматизации

Обработка ПДн в Фонде может проводиться с использованием средств автоматизации (информационных систем) и без таковых. Конкретный способ обработки ПДн определяется на основании процедур использования данных, определенных внутренними документами Фонда.

Обработка ПДн в ИСПДн с использованием средств автоматизации осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов ФСТЭК и ФСБ России по защите информации.

Список информационных систем, в которых обрабатываются ПДн, их классификация, требования по обеспечению безопасности обрабатываемых в них ПДн клиентов Фонда описаны в отдельных локальных документах Фонда.

Контроль за соответствием обработки ПДн заявленным целям возлагается на лицо, ответственное за обработку ПДн в Фонде, и на руководителей соответствующих подразделений.

10.1. Исключительно автоматизированная обработка ПДн

Исключительно автоматизированная обработка ПДн в Фонде не осуществляется. Во всех процессах обработки ПДн клиентов с использованием средств автоматизации принимают участие ответственные сотрудники Фонда.

10.2. Порядок обработки ПДн без использования средств автоматизации

Обработка ПДн без использования средств автоматизации (далее – неавтоматизированная обработка ПДн) осуществляется на бумажных носителях (журналах).

При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном 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;

при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в специально оборудованных шкафах и сейфах. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11. Получение/сбор ПДн

Источниками ПДн клиентов в Фонде являются:

Анкеты,

Договоры,

Официальный сайт,

Заявки/заявления,

Телефон,

Копии предоставляемых документов,

иные формы и источники в соответствии с действующим законодательством Российской Федерации.

Клиент обязан предоставлять Фонду достоверные сведения о себе и своевременно сообщать Фонду об изменении своих ПДн. Фонд имеет право проверять достоверность сведений, предоставленных субъектом, сверяя данные, предоставленные субъектом, с имеющимися у Фонда документами.

12. Получение ПДн не напрямую от клиента Фонда

Фонд получает ПДн клиента от него самого или от третьих лиц при условии наличия согласия на обработку и/или оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». В ряде случаев Фонд получает персональные данные от третьих лиц, получающих ПДн у субъектов, в том числе в качестве представителей Фонда на основании доверенности, а также имеющих договорные отношения с субъектом ПДн либо с Фондом. В качестве таких третьих лиц могут выступать страховые организации и другие лица. В данном случае, в соответствие с частью 4 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Фонд не обязан получать согласие субъекта ПДн на обработку его ПДн если ПДн получены не от субъекта ПДн и их обработка не поручена Фонду оператором, Фонд до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

цель обработки ПДн и ее правовое основание;

предполагаемые пользователи ПДн;

установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» права субъекта ПДн;

источник получения ПДн.

Фонд освобождается от обязанности предоставить субъекту ПДн указанные сведения в случаях, если:

ПДн получены Фондом на основании федерального закона или в связи с исполнением договора, стороны которого либо выгодоприобретателем или поручителем по которому является клиент Фонда.

ПДн сделаны общедоступными клиентом Фонда или получены из общедоступного источника.

Фонд осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы клиента Фонда.

Предоставление клиенту Фонда сведений, предусмотренных ч. 3 ст. 18 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», нарушает права и законные интересы третьих лиц.

13. Использование ПДн

Доступ к ПДн субъекта имеют сотрудники Фонда, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей. Перечень сотрудников, имеющих доступ к ПДн, утверждается приказом директора Фонда.

В случае если Фонду оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к ПДн клиентов Фонда, то соответствующие данные предоставляются Фондом

только после подписания с лицами, осуществляющими обработку ПДн по поручению Фонда, соответствующего соглашения, в котором должны быть определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

14. Использование ПДн с целью идентификации клиентов

В ходе выполнения функций, связанных с необходимостью идентификации состоящих на обслуживании клиентов, Фонд в соответствии с Федеральным законом №115-ФЗ от 07.08.2001 г. «О противодействии легализации (отмыванию) доходов, полученных преступным путем» обрабатывает персональные данные клиентов в соответствии с правилами внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансирования терроризма, утвержденного Генеральным директором Фонда.

15. Использование ПДн с целью выдачи займов

В ходе выполнения функций, связанных с проведением операций по выдаче займов, Фонд также обрабатывает ПДн клиента, указанные в Приложении 1 к настоящему Положению. Среди них в том числе:

- финансовое положение (доходы, долги, владение имуществом, денежные вклады, полученные гарантии и субсидии и др.);

В случае если указанные данные предоставлены на этапе рассмотрения заявки на предоставление займа, и договор займа не был заключен, то их обработка завершается, а данные уничтожаются по истечении 5 (пяти) лет от даты их предоставления. В случае же если договор займа был заключен, обработка ПДн завершается по истечении пяти лет с момента исполнения обязательств по договору займа в полном объеме.

Согласие на обработку указанных ПДн получается у потенциального заемщика до заключения договора займа и начала обработки таких данных.

16. Передача ПДн третьим лицам

Передача ПДн третьим лицам (включая надзорные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта ПДн.

В случае если обязанность либо возможность предоставления имеющихся в распоряжении Фонда ПДн иным лицам (включая органы государственной и муниципальной власти) установлена законодательством, Фонд обязан предоставить указанные данные в составе, виде и сроки, указанные в законодательных или нормативных актах.

Если обязанность предоставления ПДн фиксируется соответствующим запросом (ходатайством) уполномоченного лица, запрос подлежит обязательной проверке в целях контроля над обоснованностью предоставления запроса. При обоснованности подобного запроса, Фонд формирует ответ на запрос (при необходимости – организует деятельность иных подразделений по подготовке ответа). При необоснованности запроса, Фонд направляет отправителю запроса письменное уведомление об отказе в предоставлении ПДн.

Любые запросы на раскрытие ПДн от третьих лиц, не являющихся субъектами раскрываемых ПДн, подлежат обязательному рассмотрению на предмет обоснованности.

17. Передача ПДн третьим лицам без согласия

Фонд вправе осуществлять передачу ПДн в соответствующих целям запроса объемах без согласия субъекта ПДн следующим третьим лицам:

Пенсионный фонд РФ,
Налоговые органы,
Таможенные органы,
Федеральную службу финансового мониторинга,
Банк России,

Органы предварительного следствия (при наличии согласия руководителя следственного органа),

Органы внутренних дел,

Судебные органы,

Счетную палату Российской Федерации,

Федеральный орган исполнительной власти в области финансовых рынков,

Фонд социального страхования Российской Федерации,

Органы принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности,

Нотариальным конторам (по находящимся в их производстве наследственным делам),

а также другим третьим лицам в случаях, предусмотренных законодательными актами об их деятельности.

18. Трансграничная передача ПДн

Трансграничная передача ПДн осуществляется Фондом при осуществлении расчетной деятельности в порядке направления разъяснений в рамках исполнения требований национального законодательства о противодействии отмыванию доходов, полученных преступным путем и финансировании терроризма.

Трансграничная передача ПДн также может быть осуществлена в адрес организаций, зарегистрированных в иных странах, при условии, что законодательство указанных стран позволяет сделать вывод об адекватной защите ПДн. Оценку возможности подобной передачи осуществляет уполномоченный по обработке ПДн в Фонде в рамках действующего законодательства.

Иная трансграничная передача осуществляется исключительно с письменного согласия субъекта ПДн.

19. Передача ПДн в государственные органы

В соответствии с действующим законодательством Фонд вправе осуществлять передачу ПДн государственным органам, указанным в разделе «Передача ПДн третьим лицам без согласия», а также другим государственным органам и должностным лицам в случаях, предусмотренных законодательными актами об их деятельности.

20. Уточнение ПДн

Уточнение ПДн Клиента производится путем обновления или изменения данных в информационной системе и на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн клиента.

Уточнение ПДн производится в рамках действующей в Фонде системы документооборота с соблюдением принципов, изложенных в настоящем Положении.

21. Хранение ПДн

Хранение ПДн клиентов должно осуществляться в форме, позволяющей определить клиента, не дольше, чем этого требуют цели и сроки обработки ПДн, указанные в разделе «Цели и сроки обработки персональных данных» данного Положения. Обрабатываемые ПДн подлежат уничтожению и обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Хранение ПДн клиентов, цели обработки которых различны, должно осуществляться раздельно в рамках информационной системы или, при условии хранения на материальных носителях, в рамках структуры дел Фонда.

Сотрудник Фонда, имеющий доступ к ПДн клиентов в связи с исполнением трудовых обязанностей:

Обеспечивает хранение информации, содержащей ПДн клиента, исключающее доступ к ним третьих лиц.

В отсутствие сотрудника на его рабочем месте не должно находиться документов, содержащих ПДн клиентов.

При уходе в отпуск, служебную командировку и иных случаях длительного отсутствия сотрудника на своем рабочем месте (более трех дней), он обязан передать документы и иные носители, содержащие ПДн клиентов.

При увольнении сотрудника, имеющего доступ к ПДн клиентов, документы и иные носители, содержащие ПДн клиентов, передаются другому сотруднику, имеющему доступ к ПДн клиентов по указанию Генерального директора Фонда и с уведомлением лица, ответственного за обработку ПДн в Фонда.

22. Архивирование ПДн

ПДн, неиспользуемые в операционной деятельности Фонда и цель обработки которых не достигнута, могут быть переведены на архивное хранение с соблюдением всех необходимых требований, предусмотренных Федеральным законом от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативными актами в сфере организации хранения, комплектования, учета и использования архивных документов независимо от их форм собственности, либо хранится в помещениях Фонда в специализированных шкафах с описью вложения.

Архивирование ПДн производится в рамках действующих в Фонде систем документооборота и работы с архивными документами с соблюдением принципов, изложенных в настоящем Положении. Обязательным условием архивирования ПДн является обеспечение их конфиденциальности и безопасности.

Фонд обязан обеспечить в архивных ПДн на бумажных носителях ограничение доступа к указанным данным только тех сотрудников, деятельность которых непосредственно связана с обработкой хранимого типа архивных ПДн. Доступ к архивным ПДн, хранение которых осуществляется на электронных носителях, должен быть ограничен исходя из требований информационной безопасности, указанных в данном Положении и отдельных локальных нормативных актах Фонда.

23. Обезличивание ПДн

С целью уменьшения объема ПДн, подлежащих защите в соответствие с требованиями 152-ФЗ, подзаконных актов и методических указаний, а также в целях снижения нагрузки и обременений на Фонд, приводящих к дополнительным затратам без повышения уровня защищенности ПДн и прав клиентов Фонда, может быть произведено обезличивание ПДн клиентов Фонда. Также обезличивание производится в целях предоставления статистической отчетности, агрегированной информации о деятельности Фонда, а также в иных целях, предусмотренных действующим законодательством, например, по достижении целей их обработки или в случае утраты необходимости в достижении этих целей в соответствии со статьей 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Обезличенные ПДн должны представлять собой информацию на бумажном или магнитном носителе, принадлежность которой к конкретному физическому лицу невозможно определить без использования дополнительной информации в силу произведенных при обработке ПДн действий. Применяемые в Фонде механизмы обезличивания приведены в Таблица 4.

Таблица 4. Механизмы обезличивания ПДн

Алгоритм обезличивания	Описание	Примечание
Абстрагирование ПДн	Сделать ПДн менее точными путем группирования общих или непрерывных характеристик, т.е. не позволяющими отличить с помощью данного атрибута одного субъекта ПДн от других	Например, вместо указания конкретного возраста использовать кодификаторы (18-25 лет – 2, 26-33 года – 3 и т.д.).

Скрытие ПДн	Удалить всю или часть записи ПДн, не требуемые для деятельности организации	Применяется в том случае, если Фонд уже хранит неиспользуемые ПДн.
Внесение шума в ПДн		Добавить небольшое количество посторонней информации в ПДн
Замена ПДн		Переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи
Замена данных средним значением		Заменить выбранные данные средним значением для группы ПДн
Разделение ПДн на части	Использование таблиц перекрестных ссылок	Например, вместо одной таблицы использовать две – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн.
Использование специальных алгоритмов	Маскирование ПДн или подмена определенных символов другими	Отдельные корпоративные СУБД могут быть оснащены специальными функциями маскирования (data masking pack).
Использование алгоритмов криптографического преобразования	Хэширование или шифрование	Использование средств криптографической защиты регулируется отдельным законодательством.

24. Права и обязанности клиента Фонда

В целях обеспечения защиты ПДн клиенты Фонда вправе:

получать полную информацию о своих ПДн и способе обработки этих данных (в том числе автоматизированной);

осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом «О персональных данных». Физический доступ клиентов Фонда на территорию Фонда осуществляется в соответствии с внутренними документами Фонда;

требовать внесения необходимых изменений, уничтожения или блокирования соответствующих ПДн, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц Фонда.

Субъект ПДн вправе обратиться в Фонд с составленным с соблюдением требования законодательства запросом об обработке ПДн Фондом. Запрос должен быть зарегистрирован и обработан. В данном запросе может быть уточнена следующая информация:

- 1) подтверждение факта обработки ПДн Фондом;
- 2) правовые основания и цели обработки ПДн;
- 3) цели и применяемые Фондом способы обработки ПДн;
- 4) наименование и место нахождения Фонда, сведения о лицах (за исключением работников Фонда), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Фондом или на основании федерального закона;

- 5) обрабатываемые ПДн, относящиеся к соответствующему Клиенту, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;
- 7) порядок осуществления клиентом прав, предусмотренных федеральным законом;
- 8) информация об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Фонда, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные федеральным законодательством.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе если обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

Сведения, указанные выше, предоставляются клиенту или его представителю оператором при обращении либо при получении запроса клиента или его уполномоченного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность клиента или его уполномоченного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие клиента в отношениях с Фондом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Фондом, подпись клиента или его уполномоченного представителя.

В случае, если сведения, указанные выше, а также обрабатываемые ПДн были предоставлены для ознакомления клиенту по его запросу, клиент вправе обратиться повторно к Фонду или направить ему повторный запрос в целях получения сведений, указанных выше, и ознакомления с такими ПДн не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является клиент.

Клиент вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных выше, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в предыдущем абзаце, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

25. Права и обязанности Фонда в отношении обработки ПДн

Доступ работников Фонда к ПДн субъектов ПДн, обрабатываемым в Фонде, документально определен соответствующим приказом Генерального директора Фонда.

В Фонде документально определен перечень лиц, осуществляющих обработку ПДн. Лица, осуществляющие такую обработку, проинформированы о факте обработки ими ПДн, об особенностях и правилах осуществления такой обработки, а также об ответственности за нарушение действующего законодательства в области ПДн. Лица, осуществляющие обработку ПДн, ознакомлены под роспись с настоящим положением и подписали обязательство о соблюдении конфиденциальности ПДн и соблюдении правил обработки ПДн.

Фонд не вправе заставлять клиентов к предоставлению ПДн, однако вправе требовать этого, если подобные обязательства прямо вытекают из договорных отношений с клиентами или требований нормативных и законодательных актов.

Фонд обязан обеспечивать субъекту ПДн возможность ознакомления в доступной форме с документами и материалами, непосредственно к нему относящимися (если подобный запрет прямо не установлен действующим законодательством) при получении запроса, соответствующего требованиям статьи 14 Федерального закона от 27 июля 2006

года № 152-ФЗ «О персональных данных» и раздела «Права и обязанности клиентов Фонда» данного Положения.

Если сбор ПДн осуществляется во исполнение требований федерального закона, сотрудники Фонда, осуществляющие сбор ПДн обязаны разъяснить субъекту ПДн юридические последствия отказа предоставить ПДн.

Фонд обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 30 (тридцати) календарных дней с даты получения такого запроса.

26. Уведомление уполномоченного органа по защите прав субъектов ПДн

В случаях, установленных статьей 22 Федерального закона «О персональных данных», Фонд вправе направить уведомление в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор).

27. Обеспечение безопасности ПДн

Фонд при обработке ПДн клиентов принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

Обеспечение безопасности ПДн в Фонде достигается, в частности:

1) определением угроз безопасности ПДн при их обработке в информационных системах ПДн;

2) применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности ПДн;

3) применением прошедших в установленном порядке процедуры оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн;

5) учетом машинных носителей ПДн;

6) обнаружением фактов несанкционированного доступа к ПДн и принятием мер;

7) восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к ПДн, обрабатываемым в информационной системе ПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в информационной системе ПДн;

9) контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности информационных систем ПДн.

Фонд не должен обеспечивать безопасность и конфиденциальность ПДн клиентов в следующих случаях:

ПДн обезличены;

ПДн являются общедоступными или включены в источники общедоступных данных.

28. Ответственность за нарушение требований настоящего Положения

Сотрудники Фонда, обрабатывающие ПДн Клиентов, и лица, которым Фонд поручает обработку ПДн клиентов, несут гражданскую, уголовную, административную и иную предусмотренную законодательством Российской Федерации ответственность за нарушение режима защиты, обработки и порядка использования этих ПДн.

За неисполнение или ненадлежащее исполнение уполномоченными сотрудниками Фонда по его вине возложенных на него обязанностей по соблюдению установленного порядка работы с ПДн Фонд вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

Административная ответственность также предусмотрена в случаях неправомерного отказа уполномоченными лицами Фонда в предоставлении собранных в установленном

порядке документов, в случаях несвоевременного предоставления таких документов, либо в случаях предоставления неполной или заведомо ложной информации.

Сотрудники Фонда, получающие доступ к обрабатываемым ПДн, несут персональную ответственность за конфиденциальность полученной информации.

ПЕРЕЧЕНЬ ПДн клиентов обрабатываемых в Фонде

1.1. Перечень (далее – Перечень) ПДн клиентов, подлежащих защите в Фонде, разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и внутренними документами Фонда.

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. В Фонде сведениями, составляющими персональные данные (далее – ПДн) клиента, является любая информация, относящаяся к прямо или косвенно определенному или определяемому клиенту Фонда (субъекту ПДн) - физическому лицу, в том числе:

2.1.1. ПДн специальной (первой) категории.

2.1.1.1. Сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья клиентов Фонда.

2.1.2. ПДн общей (третьей) категории, за исключением ПДн, относящихся к специальной категории и к обезличенным, общедоступным, биометрическим ПДн.

2.1.2.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.2.2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.1.2.3. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

2.1.2.4. Номера телефонов (мобильного, рабочего и домашнего), в случае их регистрации на клиента Фонда или по адресу его места жительства (по паспорту).

2.1.2.5. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения).

2.1.2.6. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения).

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

2.1.2.8. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

2.1.2.9. Содержание и реквизиты гражданско-правового договора с клиентом Фонда, в котором он является стороной по договору, выгодоприобретателем, поручителем или залогодателем.

2.1.2.10. Сведения о заработной плате.

2.1.2.11. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет).

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

2.1.2.13. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);
- недвижимое имущество (полные адреса размещения объектов недвижимости и его реквизиты);
- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкарточек);
- кредиты (займы), банковские счета (в том числе спецкарточка), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкарточек, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости).

2.1.2.14. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

2.1.2.15. Сведения об идентификационном номере налогоплательщика.

2.1.2.16. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

2.1.3. Общедоступные ПДн (четвертой категории).

2.1.3.1 Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.1.3.2. Номера телефонов (мобильного и домашнего), в случае их регистрации на клиента Фонда или по адресу его места жительства (по паспорту).

2.1.3.3. иные сведения, являющиеся общедоступными или сделанные таковыми с письменного согласия клиента.

2.1.3.3. Государственная регистрация в качестве юридического лица или ИП.

2.1.3.4. Вид деятельности.

2.1.3.5. Получение информации с управления (государственного органа) по вопросам миграции (для иностранных граждан и лиц без гражданства).

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ
ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
В МИКРОКРЕДИТНОЙ КОМПАНИИ ФОНД ПОДДЕРЖКИ РАЗВИТИЯ
АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА ГОРОДСКОГО ОКРУГА
«ГОРОД ЯКУТСК»

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система (AC) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор AC - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Администратор безопасности AC - лицо, ответственное за защиту АС от несанкционированного доступа к информации.

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

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

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов.

Контролируемая зона (КЗ) - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия) (НСД) - 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, аналогичных им по своим техническим характеристикам и функциональному предназначению.

Объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, вероисповедание, национальность, другая информация.

Побочные электромагнитные излучения и наводки (ПЭМИН) - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Средства вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Система защиты информации - совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Технические средства информационной системы персональных данных (ТСИСПДн) - 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, приложения и т. п.), средства защиты информации.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о порядке организации и проведения работ по обеспечению безопасности конфиденциальной информации (далее - КИ) при их

обработке в учреждении (далее - Положение) относится к основополагающим документам, определяющим политику и общие принципы организации работ по информационной безопасности КИ в Микрокредитной компании Фонд поддержки развития агропромышленного комплекса городского округа «город Якутск» (далее по тексту – Фонд). Положение разработано в соответствии с Федеральным законом от 08.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», руководящим документом (РД) «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» — Гостехкомиссия России, 1992 год, РД Специальные требования и рекомендации по технической защите конфиденциальной информации (СТРК) — Гостехкомиссия России, 2002 год, РД «Защита от несанкционированного доступа к информации» Термины и определения — Гостехкомиссия России, 1992.

1.2. Организация и проведение работ по обеспечению безопасности информации, содержащей КИ, на объектах информатизации Фонда проводится на основании законодательных и нормативных актов Российской Федерации в области защиты информации и настоящего Положения.

1.3. Требования настоящего Положения являются обязательными для исполнения в Фонде.

1.4. Положение определяет порядок организации и проведения работ по защите информации, содержащей КИ, на объектах информатизации Фонда как в период их создания, так и в процессе повседневной эксплуатации.

1.5. Принимаемые меры по защите информации на объектах информатизации Фонда должны обеспечивать выполнение действующих требований и норм по защите информации.

1.6. Разработка мер и обеспечение защиты информации на объектах информатизации осуществляется ответственным за защиту информации работником в Фонде .

Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии ФСТЭК России и ФСБ России на право проведения соответствующих работ.

Согласование планируемых мер, контроль выполнения работ на местах, соответствия принятых мер и проводимых мероприятий по защите информации действующим требованиям и нормам производит ответственный за защиту информации работник.

1.7. Объекты информатизации организации должны соответствовать требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

1.8. Защита информации организуется в соответствии с действующими нормативными документами ФСТЭК России.

1.9. Ответственность за общее состояние и организацию работ по созданию и эксплуатации объектов информатизации возлагается на работника, ответственного за защиту информации.

1.10. Контроль выполнения требований настоящего Положения возлагается на генерального директора Фонда.

1.11. Финансирование мероприятий по защите информации предусматривается сметами организации на планируемый год. При этом:

- расходы по защите информации при эксплуатации существующих помещений, технических систем и средств включаются в стоимость их содержания;
- затраты, связанные с защитой информации в создаваемых информационно-вычислительных и других технических системах, предусматриваются в стоимости создания и развития этих систем;
- расходы по защите информации при ремонте и реконструкции помещений предусматриваются в стоимости этих работ.

2 ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ОРГАНИЗАЦИИ

2.1. В организации должен выполняться комплекс организационно-технических мероприятий по защите информации, циркулирующей в помещениях, технических системах и средствах передачи, хранения и обработки информации.

2.2. Накопление, обработка, хранение и передача защищаемой информации в организации происходит на объектах информатизации, которые представляют собой совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения, помещений, в которых они установлены, или помещений, предназначенных для ведения конфиденциальных переговоров.

К объектам информатизации в организации относятся защищаемые помещения и объекты вычислительной техники.

2.3. Целями защиты информации на объектах информатизации организации являются:

- предотвращение утечки информации по техническим каналам;
- предотвращение уничтожения, искажения, копирования, блокирования информации в системах информатизации за счет НСД к ней;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах ее обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

2.4. К основным задачам защиты информации на объектах информатизации организации относятся задачи по предотвращению:

- несанкционированного доведения защищаемой информации до лиц, не имеющих права доступа к этой информации;
- получения защищаемой информации заинтересованным лицом с нарушением установленных прав или правил доступа к защищаемой информации;
- получения защищаемой информации разведкой с помощью технических средств;
- воздействия на защищаемую информацию с нарушением установленных прав или правил на изменение информации, приводящего к ее искажению,

- уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
- воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств АС, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

2.5. Защита информации на объектах информатизации Фонда достигается выполнением комплекса организационных мероприятий с применением сертифицированных средств защиты информации от утечки или воздействия на нее по техническим каналам путем НСД к ней, по предупреждению преднамеренных программно-технических воздействий, предпринятых с целью нарушения целостности (модификации, уничтожения) информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

3. ПОРЯДОК ОПРЕДЕЛЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

3.1. К защищаемой информации организации относится:

- информация, содержащая коммерческую тайну, служебную информацию, ПДн;
- общедоступная информация, уничтожение, изменение, блокирование которой может нанести ущерб Фонду.

3.2. По результатам анализа информации, обрабатываемой в Фонде, составляются:

- «Список работников, допущенных к обработке АС»;

3.3. Защищаемая информация организации может быть представлена:

- на бумажных носителях в виде отдельных документов или дел с документами;
- на машинных носителях в виде файлов, массивов, баз данных, библиотек и пр.;
- в виде речевой информации, при проведении совещаний, переговоров и пр.

3.4. С целью определения технических средств и систем, с помощью которых обрабатывается информация, содержащая КИ, а также помещений, где проводятся обсуждения с использованием такой информации, ответственным работником Фонда составляются и утверждаются перечни технических средств АС и защищаемых помещений.

4. ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНИЗАЦИИ

4.1. Технический канал утечки информации (ТКУИ) представляет собой совокупность следующих факторов:

- источника информативного сигнала;
- физической среды его распространения;
- приемника, способного зарегистрировать данный сигнал.

4.2. При ведении переговоров и использовании технических средств для обработки и передачи информации на объектах информатизации организации возможна реализация следующих ТКУИ:

- акустического излучения информативного речевого сигнала;
- электрических сигналов, возникающих при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям, выходящим за пределы КЗ;
- НСД к обрабатываемой в АС информации и несанкционированные действия с ней;
- воздействия на технические или программные средства АС в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств;
- ПЭМИН информативных сигналов от технических средств АС и линий передачи информации;
- наводок информативного сигнала, обрабатываемого техническими средствами АС, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучений, модулированных информативным сигналом, возникающим при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучений или электрических сигналов от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации («закладочные устройства»), модулированных информативным сигналом;
- радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- просмотра информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- прослушивания телефонных и радиопереговоров;
- хищения технических средств с хранящейся в них информацией или носителей информации.

4.3. Перехват информации, циркулирующей на объекте информатизации, или воздействие на нее с использованием технических средств могут вестись:

- из-за границы КЗ из близлежащих строений и транспортных средств;
- из смежных помещений, принадлежащих другим организациям и расположенным в том же здании, что и объект информатизации;
- при посещении организаций посторонними лицами;
- за счет НСД к информации, циркулирующей в АС, как с помощью технических средств автоматизированной системы, так и через сети.

4.4. В качестве аппаратуры перехвата или воздействия на информацию и технические средства объекта информатизации могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта либо подключаемые к каналам связи или техническим средствам обработки

информации, а также электронные устройства съема информации - «закладочные устройства», размещаемые внутри или вне защищаемого помещения.

4.5. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах контролируемой зоны, вследствие:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемого помещения и его инженерно-технических систем;
- некомпетентных или ошибочных действий пользователей;
- непреднамеренного просмотра информации с экранов мониторов и пр.

5. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНИЗАЦИИ

5.1. Защита информации, циркулирующей на объекте информатизации, должна быть комплексной и дифференцированной. С этой целью для каждого объекта информатизации создается система защиты информации.

5.2. Комплексная защита информации на объектах информатизации проводится по следующим основным направлениям работы:

- охрана помещений объекта;
- определение перечня информации, подлежащей защите;
- составление организационно-распорядительной, эксплуатационной и иной документации по защите информации;
- защита речевой информации при осуществлении конфиденциальных переговоров (при необходимости);
- защита информации, содержащей КИ, при обработке, передаче с использованием технических средств, а также на бумажных или иных носителях;
- защита информации при взаимодействии абонентов с информационными сетями связи общего пользования.

5.3. Перечень необходимых мер защиты информации определяется с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрываемости.

Основное внимание должно быть уделено защите информации, содержащей КИ, в отношении которой угрозы реальны и сравнительно просто реализуемы без применения сложных технических средств перехвата информации. К информации такого рода относится:

- речевая информация, циркулирующая в защищаемом помещении;
- информация, обрабатываемая СВТ;
- информация, выводимая на экраны мониторов;
- документированная информация, содержащая КИ;
- информация, передаваемая по каналам связи, выходящим за пределы КЗ.

5.4. Создание системы защиты информации объекта информатизации осуществляется при необходимости по следующим стадиям:

- предпроектная стадия, включающая в себя предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания системы защиты конфиденциальной информации (далее СЗКИ) и технического задания на ее создание;
- стадия проектирования (разработки проектов) и реализации АС, включающая в себя разработку СЗКИ в составе объекта информатизации;
- стадия ввода в действие СЗКИ, включающая в себя опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации (далее СрЗИ), а также оценку соответствия АС требованиям безопасности информации (аттестация).

5.4.1. Предпроектная стадия обследования объекта информатизации включает в себя:

- установление необходимости обработки КИ в АС;
- определение КИ, подлежащих защите от НСД;
- определение условий расположения технических средств АС относительно границ КЗ;
- определение конфигурации и топологии АС в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- определение технических средств и систем, предполагаемых к использованию в разрабатываемой АС, условий их расположения, общесистемных и прикладных программных средств, имеющихся и предлагаемых к разработке;
- определение режимов обработки КИ в АС в целом и в отдельных ее компонентах;
- определение класса защищенности АС;
- уточнение степени участия должностных лиц в обработке КИ, характер их взаимодействия между собой;
- определение (уточнение) угроз безопасности КИ применительно к конкретным условиям функционирования АС.

5.4.2. По результатам предпроектного обследования на основе документов ФСТЭК России, с учетом установленного класса защищенности АС делаются конкретные требования по обеспечению безопасности КИ, включаемые в техническое (частное техническое) задание на разработку СЗКИ.

5.4.3. Предпроектное обследование может быть поручено специализированной организации, имеющей соответствующую лицензию. Порядок ознакомления (при необходимости) специалистов подрядной организации с защищаемыми сведениями определяется организацией.

5.4.4. Аналитическое обоснование необходимости создания СЗКИ должно содержать:

- информационную характеристику и организационную структуру объекта информатизации;

- характеристику комплекса технических средств АС, программного обеспечения, режимов работы, технологического процесса обработки информации;
- возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
- перечень предлагаемых к использованию сертифицированных СрЗИ;
- обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
- оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗКИ;
- ориентировочные сроки разработки и внедрения СЗКИ;
- перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем организации, проводившей предпроектное обследование, согласовывается с ответственным лицом и утверждается руководителем организации.

5.4.5. Техническое (частное техническое) задание на разработку СЗКИ должно содержать:

- обоснование разработки СЗКИ;
- исходные данные создаваемой (модернизируемой) АС в техническом, программном, информационном и организационном аспектах;
- класс защищенности АС;
- ссылку на нормативные документы, с учетом которых будет разрабатываться СЗКИ и приниматься в эксплуатацию АС;
- конкретизацию мероприятий и требований к СЗКИ;
- перечень предполагаемых к использованию сертифицированных СрЗИ;
- обоснование проведения разработок собственных СрЗИ при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных СрЗИ;
- состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗКИ.

5.4.6. В целях дифференциированного подхода к обеспечению безопасности КИ в зависимости от объема обрабатываемых КИ и угроз безопасности важным интересам организации, общества и государства АС подразделяются на классы защищенности.

Класс АС устанавливается в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» — Гостехкомиссия России, 1992, и оформляется актом. Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение хотя бы одного из критериев, на основании которых он был установлен.

5.4.7. На стадии проектирования и создания АС (СЗКИ) проводятся следующие мероприятия:

- разработка задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) АС в соответствии с требованиями технического (частного технического) задания на разработку СЗКИ;
- выполнение работ в соответствии с проектной документацией;
- обоснование и закупка совокупности используемых в АС серийно выпускаемых технических средств обработки, передачи и хранения информации;
- разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;
- обоснование и закупка совокупности используемых в АС сертифицированных технических, программных и программно-технических СрЗИ и их установка;
- проведение сертификации по требованиям безопасности информации технических, программных и программно-технических СрЗИ, в случае когда на рынке отсутствуют требуемые сертифицированные СрЗИ;
- разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на АС информации;
- определение подразделений и назначение лиц, ответственных за эксплуатацию СрЗИ, с их обучением по направлению обеспечения безопасности ПДн;
- разработка эксплуатационной документации на АС и СрЗИ, а также организационно-распорядительной документации по защите информации (распоряжений, инструкций и других документов);
- выполнение других мероприятий, характерных для конкретных АС и направлений обеспечения безопасности КИ.

5.4.8. На стадии ввода в действие АС (СЗКИ) осуществляются:

- выполнение генерации пакета прикладных программ в комплексе с программными СрЗИ;
- опытная эксплуатация СрЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе АС;
- приемо-сдаточные испытания СрЗИ по результатам опытной эксплуатации;
- организация охраны и физической защиты помещений АС, исключающих несанкционированный доступ к техническим средствам АС, их хищение и нарушение работоспособности, хищение носителей информации;
- оценка соответствия АС требованиям безопасности КИ.

6. ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ ЗА ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ

6.1. Генеральный директор Фонда несет ответственность за общую организацию работ по защите информации на объектах информатизации.

6.2. Администратор безопасности ИСПДн Фонда несет ответственность за:

- руководство и координацию работ по защите информации на объектах информатизации;

- организацию выполнения требований по защите информации на объекте информатизации;
- обоснованность необходимости создания СЗКИ объекта информатизации;
- разработку организационно-распорядительных документов по защите информации на объектах информатизации;
- организацию разработки технического задания на создание СЗКИ, подготовку проектов договоров со сторонними организациями на выполнение работ по защите информации на объектах информатизации;
- организацию контроля состояния СЗКИ объекта информатизации, соблюдения работниками установленных норм и требований по защите информации;
- организацию контроля охраны помещений объекта;
- совершенствование СЗКИ.
- сопровождение СЗИ от несанкционированного доступа;
- непосредственное управление режимами работы и административную поддержку функционирования применяемых специальных программных и программно- аппаратных СЗИ от несанкционированного доступа;
- настройку и сопровождение в процессе эксплуатации подсистемы управления доступом;
- проверку состояния используемых СЗИ от несанкционированного доступа, правильности их настройки;
- выполнение требований по обеспечению безопасности при организации технического обслуживания и отправке в ремонт СВТ;
- учет, хранение, прием и выдачу персональных идентификаторов и журналов ответственным исполнителям;
- контроль учета, создания, хранения и использования резервных и архивных копий массивов данных.
- организация выбора типа и версии серверных и клиентских операционных систем, установку, настройку, сопровождение операционных систем серверов;
- организация обновления справочного и антивирусного программного обеспечения;
- организация настройки аппаратной и программной составляющей серверного, коммутационного, телекоммуникационного оборудования, средств аппаратной безопасности сегментов, сетевого периферийного оборудования;
- организация регистрации пользователей и предоставление им прав доступа к сетевым информационным ресурсам, регистрацию компьютеров в сети;
- организация обеспечения работоспособности структурированной кабельной сети;
- организация архивирования, резервного копирования информации;
- контроль физической сохранности средств и оборудования сети.

6.3. Работники Фонда, эксплуатирующие объект информатизации, несут ответственность за:

- выполнение требований по защите информации на объекте информатизации;
- ведение необходимой документации объекта информатизации;
- правильность определения пользователям необходимости и прав доступа к защищаемым информационным ресурсам.

- 6.4. Пользователи АС объекта информатизации несут ответственность за:
- соблюдение мер по защите информации и правил эксплуатации СВТ;
 - обеспечение сохранности СВТ, машинных носителей информации и целостность установленного программного обеспечения;
 - соблюдение установленных требований по обращению с машинными носителями информации.