ЦЕНТР РАЗВИТИЯ КООПЕРАТИВОВ

МЕТОДИЧЕСКИЙ МАТЕРИАЛ «РАБОТА С ПЕРСОНАЛЬНЫМИ ДАННЫМИ ФИЗИЧЕСКИХ ЛИЦ»

Липецк – 2021 г.

Оглавление

I. Основные понятия, установленные в законодательстве о персональных данных:

персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу – субъекту персональных данных;

персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных в порядке, предусмотренном законом;

оператор персональных данных (Кооператив) – юридическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному, или неперсонифицированному поименно, кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных либо часть такого носителя;

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных (ИС ПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, в том числе программ для ЭВМ и программных комплексов для ЭВМ и компьютерного оборудования;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства, органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу либо на территорию, находящуюся под юрисдикцией государства, непризнанного Российской Федерацией, или органу власти, организации либо гражданину непризнанного государства;

субъект персональных данных – физическое лицо (человек), данные которого обрабатываются;

конфиденциальность персональных данных – обязательное для кооператива, его работников, членов и их представителей, получивших доступ к персональным данным, требование не раскрывать и не распространять 3-м лицам персональные данные без согласия субъекта персональных данных, если основание предоставления не предусмотрено законом.

II. Виды персональных данных: общие, специальные и биометрические.

Целью Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» является обеспечение 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.

 *Являются ли идентификаторы персональными данными?*

Такие идентификаторы, как **ИНН** (идентификационный номер налогоплательщика), **СНИЛС** (страховой номер индивидуального лицевого счета, идентифицирующий гражданина в системе пенсионного страхования), адрес электронной почты и тому подобные, **являются персональными данными**. Они присваиваются конкретному человеку и не могут быть отнесены к другому. Даже без дополнительной информации (такой, как имя человека, фото лица) идентификаторы являются персональными данными.

Комбинация: фамилия, имя и телефон – персональные данные.

Номер телефона без имени – не персональные данные, так как он относится не к пользователю, а к абонентскому устройству или линии связи.

Специальные персональные данные.

Это категория персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

Кооперативу могут быть предоставлены сведения об инвалидности, а также временной нетрудоспособности в связи с болезнью работника, члена, ассоциированного члена или заемщика, его беременности, рождении у него ребенка, уходе за ребенком до достижения им возраста *полутора лет / трех лет*, инвалидности его ребенка, его временной нетрудоспособности в связи с болезнью ребенка, его собственной смерти и смерти его ребенка или другого близкого родственника (на основании ч. 2 ст. 128 Трудового кодекса РФ).

Сведения о судимости являются специальными персональными данными (п. 3 ст. 10 152-ФЗ) и их обработка может осуществляться лицами, не являющимися государственными органами или муниципальными органами, только в тех случаях и в том порядке, которые определяются в соответствии с федеральными законами (в 190-ФЗ и 193-ФЗ установлены требования к членам правления и наблюдательного совета кооператива).

Биометрические персональные данные.

Сведения, которые характеризуют физиологические и биологические особенности человека (изображение лица (фотографический снимок), аудиозапись голоса, отпечатки пальцев), на основании которых можно установить его личность (биометрические персональные данные) и которые используются Кооперативом для установления личности субъекта персональных данных, могут обрабатываться только при наличии письменного согласия субъекта персональных данных, за исключением следующих случаев:

- в связи с реализацией международных договоров Российской Федерации о реадмиссии;

- в связи с осуществлением правосудия и исполнением судебных актов;

- в связи с проведением обязательной государственной дактилоскопической регистрации;

- в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

В личном деле работника или анкете физического лица, являющегося членом либо ассоциированным членом кооператива, как правило, содержится фотография его лица.

III. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным.

В случае неточности персональных данных или неправомерности их обработки Кооператив должен актуализировать информацию или прекратить обработку данных. Поэтому в Политике закреплено, что Кооператив обязан внести изменения, уничтожить или блокировать персональные данные, если субъект предоставит сведения о том, что данные устарели, недостоверны или получены незаконно.

В случае предоставления субъектом персональных данных фактов о неполных, устаревших, недостоверных или незаконно полученных персональных данных Кооператив обязан внести необходимые изменения, уничтожить или блокировать их, а также уведомить о своих действиях субъекта персональных данных.

В случае подтверждения факта неточности в персональных данных они подлежат актуализации Кооперативом, а при неправомерности их обработки такая обработка должна быть прекращена.

Условия, при которых данные подлежат уничтожению, Роскомнадзор рекомендует сформулировать так же, как это сделано в Законе № 152-ФЗ.

Когда цели обработки достигнуты или субъект ПДн отозвал свое согласие, персональные данные должны быть уничтожены, если:

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

- Кооператив не вправе осуществлять обработку без согласия субъекта ПДн на основаниях, предусмотренных Законом о ПДн или иными федеральными законами;

- иное не предусмотрено иным соглашением между Кооперативом и субъектом ПДн, например, соглашением о коммерческой тайне.

Кооператив обязуется сообщить о наличии у него персональных данных субъекту этих данных, а также предоставить такому субъекту возможность ознакомиться с его данными.

IV. Согласно каким нормативно-правовым актам составляются локальные правовые акты кооператива и каких ошибок следует избежать, чтобы не получить штраф от Роскомнадзора:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»:

Ошибка, обозначенная Роскомнадзором: не разработали и не опубликовали политику обработки персональных данных.

В соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) к обязанностям Кооператива персональных данных относится издание документа, определяющего политику Кооператива в отношении обработки персональных данных.

Что нужно сделать?

Издать Приказ об утверждении Политики кооператива в отношении обработки им персональных данных.
Роскомнадзор **рекомендует** указать ответственного за размещение этой Политики на сайте организации (при наличии сайта) и информационном стенде.

Ошибка, обозначенная Роскомнадзором: не назначили ответственного за обработку персональных данных.

Согласно ст. 22.1 Закона 152-ФЗ Кооператив, являющийся юридическим лицом, назначает лицо, ответственное за организацию обработки персональных данных (далее – ответственный сотрудник).

Что нужно сделать?

Назначить приказом одного сотрудника или члена кооператива, который будет отвечать за обработку персональных данных.
Ответственный должен подчиняться непосредственно руководителю организации. Ответственным может быть сам руководитель кооператива или внештатный сотрудник (аутсорсер), по внешнему совместительству или по договору оказания услуг, в том числе: индивидуальный предприниматель, глава крестьянского (фермерского) хозяйства или самозанятый гражданин (плательщик налога на профессиональный доход).

***Ответственный сотрудник или член кооператива* непосредственно *обязан*:**

- осуществлять внутренний контроль за соблюдением кооперативом, его работниками и членами законодательства о персональных данных, в том числе требований к защите персональных данных, полученных кооперативом (1);

- доводить до сведения работников и членов положения законодательства о персональных данных, локальных правовых актов по вопросам обработки персональных данных и требований к защите персональных данных (2).

Ошибка, обозначенная Роскомнадзором: работники не ознакомлены под подпись с законом о персональных данных.

Что нужно сделать?

- Вариант 1: оформить **Лист ознакомления работников с положениями законодательства о персональных данных и внутренними документами кооператива по вопросам обработки персональных данных** (п. 6 ч. 1 ст. 18.1 ФЗ от 27.07.2006 № 152-ФЗ).

- Вариант 2: вести **Журнал учета инструктажа** и утвердить приказом **Инструкцию по первичному инструктажу**. Журнал учета прохождения первичного инструктажа сотрудниками ведется Кооперативом в качестве меры, направленной на учет прохождения первичного инструктажа лицами, допущенными к обработке персональных данных на основании ***Приказа о допуске к обработке персональных данных***.

- Организовать прием и обработку обращений и запросов субъектов персональных данных, или их представителей, и осуществлять контроль за приемом и обработкой таких обращений и запросов (3).

- Издать **Приказ об утверждении Правил реагирования на запросы и обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва ранее предоставленного согласия и доступа субъекта персональных данных к его персональным данным**.

- Указать ответственного за размещение этой Политики на информационном стенде кооператива (рекомендуется).

В соответствии со ст. ст. 9 и 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обработка персональных данных осуществляется только с письменного согласия субъекта персональных данных и при наличии согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, которое оформляется отдельно от других согласий субъекта персональных данных на обработку его персональных данных.

Ошибка, обозначенная Роскомнадзором: используете неверный бланк согласия на обработку персональных данных.

Что нужно сделать?

- Утвердить приказом типовые формы согласия на обработку персональных данных. Согласие должно включать в себя все обязательные реквизиты, которые предусматривает закон (ч. 4 ст. 9 ФЗ от 27.07.2006 № 152-ФЗ). За некорректную форму согласия предусмотрено наложение административного штрафа на должностное лицо (председателя кооператива) – от двадцати тысяч до сорока тысяч рублей; на юридическое лицо (кооператив) – от тридцати тысяч до ста пятидесяти тысяч рублей (ч. 2 ст. 13.11 КоАП).

- Для выполнения требования ст. 7 Закона 152-ФЗ о сохранении конфиденциальности персональных данных – утвердить перечень лиц, имеющих доступ к персональным данным, обрабатываемым в организации, утвердить образец обязательства о неразглашении персональных данных и издать приказ об организации подписания с работниками, членами, ассоциированными членами и их представителями – сотрудниками, имеющими доступ к персональным данным, этих обязательств о неразглашении персональных данных.

Передача и распространение персональных данных: есть ли разница?

Распространение персональных данных – это действия, направленные на раскрытие персональных данных *неопределенному кругу лиц*. *Распространение* персональных данных является новой разновидностью передачи данных наряду с *предоставлением* и *доступом*, что следует из п. 3 ч. 1 ст. 3 и ч. 5 ст. 10.1 Закона №152-ФЗ.

Предоставление персональных данных – это действия, направленные на раскрытие персональных данных *определенному лицу* или *определенному кругу лиц*.

Доступ к персональным данным – это возможность ознакомления с персональными данными, включая визуальное ознакомление, прослушивание и (или) копирование персональных данных.

Статьей 10.1 Закона 152-ФЗ установлено понятие *персональных данных, разрешенных для распространения*. Чтобы разрешить распространять свои персональные данные, **субъект должен заполнить и подписать отдельное письменное согласие**.

Является заблуждением, что отдельное согласие нужно для распространения персональных данных только среди неограниченного круга лиц. Тогда как адресную передачу персональных данных третьему лицу можно оформлять в согласии на передачу в свободной форме.

1. Постановление Правительства РФ № 687 Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.

Согласно Постановлению № 687 обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, ***считается осуществленной без использования средств автоматизации (неавтоматизированной)***, если такие действия с персональными данными, как ***использование, уточнение, распространение, уничтожение*** персональных данных осуществляются при непосредственном участии человека.

Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в ИС ПДн, либо были извлечены из нее.

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

Ошибка, обозначенная Роскомнадзором: не утвердили перечень лиц, которые имеют доступ к персональным данным.

Что нужно сделать?

- **Утвердить** приказом перечень лиц, которым может понадобиться доступ к персональным данным в связи с их обязанностями. В приказе можно указать ФИО, должности конкретных сотрудников, структурное подразделение или перечень должностей и структурное подразделение, категорию: член кооператива, ассоциированный член кооператива, член правления или член наблюдательного совета кооператива.

- **Обеспечить** раздельное хранение персональных данных (материальных носителей данных), обработка которых осуществляется в различных целях.

- При хранении материальных носителей **соблюдать** условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним: перечень мер, необходимых для обеспечения таких условий, порядок их

принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются кооперативом.

 **Ошибка, обозначенная Роскомнадзором:** не утвердили перечень мест хранения персональных данных.

 ***Что нужно сделать?***

Издать приказ, которым утвердить перечень мест хранения материальных носителей персональных данных – журналов учета выданных займов, личных дел работников, председателя, заместителя председателя, членов правления, анкет членов, ассоциированных членов и т.д. (п. 13 Положения, утв. постановлением Правительства РФ от 15.09.2008 г. № 687). Во всех кабинетах, где ведется работа с персональными данными на бумаге, определите места хранения — например, сейфы, шкафы, тумбы, оснащенные замком.

Местом хранения может быть и само помещение, кабинет, архив организации.

При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим *одновременное копирование* персональных данных, подлежащих уничтожению и блокированию.

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

При этом сам процесс уничтожения должен проводиться специальной комиссией, созданной для таких случаев. После завершения уничтожения подписывается акт об уничтожении персональных данных, подписываемый членами комиссии и руководителем.

- Учитывая особенности носителей данных и то, что после уничтожения информации не должно быть возможности ее восстановить, – **рекомендуется *разделить*** процедуры уничтожения данных на бумажных носителях и уничтожения (стирания, форматировабния) съемных носителей персональных данных в электронно-цифровой форме и, соответственно, делать два различных акта об уничтожении.

- *Вести* ***Журнал учета съемных носителей, содержащих персональные данные,*** в качестве меры, направленной на обеспечение сохранности съемных носителей персональных данных.

- **Хранить** съемные носители с персональными данными (флэш-карты, внешние жесткие диски, мобильные устройства, планшеты и т.п.) в сейфах, шкафах, если персональные данные на самих носителях содержатся не в зашифрованном виде.

Журнал учета предназначен для учета каждого экземпляра съемных носителей.

2. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных установлены Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Для используемых в организации ИС ПДн установлена необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе (то есть для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников Кооператива или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Кооператива).

Для обеспечения 4-го уровня защищенности персональных данных – утвердить *Перечень лиц, доступ которых к персональным данным физических лиц, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых, договорных) обязанностей*.

Для обеспечения 3-го уровня защищенности персональных данных, помимо выполнения требований, предусмотренных для обеспечения 4-го уровня защищенности, – назначить должностное лицо (работника), ответственное за обеспечение безопасности персональных данных в информационной системе (системах), – издать ***Приказ о назначении ответственного за безопасность персональных данных в кооперативе.***

Издать ***Приказ об утверждении перечня ИС ПДн.*** В нем указывается назначение системы, составляющей основную цель обработки персональных данных. Например, автоматизация процессов кадрового учета. Также в документе указываются категории и объем персональных данных в соответствии с Постановлением Правительства РФ от 01.11.2012 №1119.

V. Уведомление в адрес Управления Роскомнадзора по Липецкой области

Уведомить ***Управление Роскомнадзора по Липецкой области*** (уполномоченный орган по защите прав субъектов персональных данных) о намерении осуществлять обработку персональных данных;

Осуществлять обработку без направления уведомления в адрес ***Управления Роскомнадзора по Липецкой области*** в отношении следующих категорий (видов) персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных; в Кооперативе персональные данные распространяются только при наличии письменного согласия субъекта персональных данных, указанного в пункте 4;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) разрешенных субъектом персональных данных для распространения при условии соблюдения оператором запретов и условий, предусмотренных статьей 10.1 настоящего Федерального закона; необходимо получать согласие на распространение персональных данных, образец согласия на обработку персональных данных, разрешенных субъектом персональных данных для их распространения, в приложении № 4 к Приложению 4 «Приказ об организации работы с персональными данными» настоящих методических материалов;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных; Кооператив может обрабатывать данные без использования средств автоматизации – вне программ (программных комплексов) для электронных вычислительных машин (ЭВМ);

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

VI. Пакет организационно-распорядительных документов по персональным данным.

- **Приказы об организации работ по защите персональных данных**:
  - об утверждении Политики Кооператива в отношении обработки и защиты персональных данных;
  - о назначении ответственного лица за организацию обработки персональных данных;
  - о назначении ответственного лица за безопасность персональных данных;
  - об утверждении перечня ИС ПДн;
  - об утверждении об организации работы с персональными данными (списки лиц, допущенных к работе с персональными данными, обрабатываемыми в информационной системе, для выполнения служебных обязанностей – в данном приказе);
  - об утверждении мест хранения материальных носителей персональных данных;
  - об уничтожении персональных данных;
- **Акты об уничтожении персональных данных**:
  - форма акта об уничтожении персональных данных на бумажных носителях;
  - форма акта об уничтожении съемных носителей персональных данных;
- **Журналы**:
  - регистрации входящих запросов и обращений субъектов персональных данных;
  - учета съемных носителей, содержащих персональные данные;
  - учета прохождения первичного инструктажа работниками;
  - инструкция по проведению первичного инструктажа.

VII. Образцы организационно-распорядительных документов* для работы с персональными данными

** В предлагаемых документах следует самостоятельно заполнить пустые графы (_____) или слова, выделенные курсивом (буквы под наклоном).*

Приложение 1. Приказ об утверждении политики Кооператива в отношении обработки и защиты персональных данных

_____
(наименование организации)

_____
(местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
об утверждении Политики Кооператива в отношении обработки и защиты персональных данных

_____ «___»_____20__ г.
(место издания)

С целью организации обработки персональных данных работников в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Политику Кооператива в отношении обработки и защиты персональных данных (прилагается).
2. Документ ввести в действие с «___»_____ 20__г.
3. Разместить документ на (сайте организации в сети интернет - при наличии) и на информационном стенде.
   Ответственный: _____
   (должность, Ф. И. О.)
4. Ознакомить работников с документом под подпись.
   Ответственный: _____
   (должность, Ф. И. О.)

5. Контроль за исполнением настоящего Приказа оставляю за собой.

_____
(должность, Ф. И. О.)

С Приказом ознакомлен:

_____
(должность, Ф. И. О.)

Приложение 2. Приказ о назначении ответственного за организацию обработки персональных данных

_____
(наименование организации)

_____
(местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
о назначении ответственного за организацию обработки персональных данных

_____ «___»_____20__ г.
(место издания)

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных:

_____
(должность, Ф. И. О.)

2. Обязать _____ (должность, Ф. И. О.):

осуществлять внутренний контроль за соблюдением _____ (сокращенное наименование организации) и его сотрудниками, членами, ассоциированными членами и их представителями законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводить до сведения сотрудников, членов, ассоциированных членов и их представителей _____ (сокращенное наименование организации) положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Внести в должностную инструкцию _____ (должность, Ф. И. О.) изменения в соответствии с п. 3 настоящего Приказа.
4. Заключить с _____ (должность, Ф. И. О.) дополнительное соглашение к Трудовому договору от «__»_____ 20__ г. N ____.
5. Контроль за исполнением настоящего Приказа оставляю за собой.

_____
(должность, Ф. И. О.)

С Приказом ознакомлен:

_____

(должность, Ф. И. О.)

Приложение 3. Приказ о назначении ответственного за безопасность персональных данных

_____
(наименование организации)

_____
(местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
о назначении ответственного за безопасность персональных данных при их обработке в информационных системах персональных данных

_____ «___»_____20__ г.
(место издания)

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию работ и обеспечение безопасности персональных данных _____
(должность, Ф. И. О.)
2. В срок до _____ назначенным лицам разработать и внедрить план мероприятий по обеспечению защиты персональных данных.
3. Внести в должностную инструкцию _____ (должность, Ф. И. О.) изменения в соответствии с положениями настоящего Приказа.
4. Заключить с _____ (должность, Ф. И. О.) дополнительное соглашение к Трудовому договору / Договору гражданско-правового характера от «__» _____ 202_ г. № ____, которое должно включать в себя положения о полной (индивидуальной) материальной ответственности.
5. Контроль за исполнением настоящего Приказа оставляю за собой.

_____
(должность, Ф. И. О.)

С Приказом ознакомлен:

_____

(должность, Ф. И. О.)

Приложение 4. Приказ об организации работы с персональными данными

_____
(наименование организации)

_____
(местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
об организации работы с персональными данными

_____ «___»_____20__ г.
(место издания)

В целях выполнения требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных"

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с момента подписания настоящего приказа:

   Правила реагирования на запросы / обращения субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к своим данным.

   Разместить указанный документ на информационном стенде. Ответственный: _____ (должность, Ф. И. О.).
2. Утвердить перечень лиц, имеющих доступ к персональным данным, обрабатываемым в организации (**приложение N 1** к настоящему приказу).
3. Определить объем их полномочий при работе с персональными данными. Ответственный: _____ (должность, Ф. И. О.).
4. Утвердить образец обязательства о неразглашении персональных (**приложение N 2** к настоящему приказу).
5. _____ (должность, Ф. И. О.) в течение ___ *рабочих дней* после издания настоящего приказа организовать подписание с работниками, членами, ассоциированными членами (их представителями – физическими лицами), имеющими доступ к персональным данным, обязательств о неразглашении персональных данных.
6. Утвердить:

   образец согласия члена кооператива на обработку персональных данных (**приложение N 3** к настоящему приказу);

образец согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (**приложение N 4** к настоящему приказу).

образец согласия на обработку и передачу персональных данных третьим лицам при заключении договора займа (**приложение N 5** к настоящему приказу).

образец согласия на обработку и передачу персональных данных третьим лицам при заключении договора поручительства (**приложение N 6** к настоящему приказу).

Разместить указанные документы на сайте организации в сети Интернет (при наличии) и на информационном стенде.

Ответственный: _____ (должность, Ф. И. О.).

7. Контроль за исполнением настоящего приказа оставляю за собой.

_____

(должность, Ф. И. О.)

С Приказом ознакомлен:

_____

(должность, Ф. И. О.)

Приложение N 1 к Приказу № __ от «___» _____ 20__ г.

Список лиц, допущенных к

_____ (должность, Ф. И. О.).

_____ (должность, Ф. И. О.).

_____ (должность, Ф. И. О.).

_____ (должность, Ф. И. О.).

Приложение N 2 к Приказу № __ от «___» _____ 20__ г.

Обязательство о неразглашении персональных данных

Я, _____ (Ф. И. О. полностью)

настоящим подтверждаю, что я понимаю, что я занимаюсь обработкой персональных данных физических лиц, а также что разглашение такого рода информации может нанести ущерб субъектам обрабатываемых мною персональных данных и _____ _____ (наименование кооператива).

В связи с этим принимаю на себя обязательство при работе с персональными данными соблюдать все установленные в (_____ наименование организации) (далее – организация) требования по защите персональных данных, в том числе:

1. Не разглашать сведения, составляющие персональные данные, которые мне будут переданы или станут известны во время исполнения мною трудовых обязанностей.

2. Не использовать сведения, составляющие персональные данные, в личных целях и в целях извлечения выгоды.

3. Не передавать третьим лицам и не раскрывать публично сведения, составляющие персональные данные, без письменного разрешения субъектов персональных данных.

4. Выполнять относящиеся ко мне требования Политики Кооператива в отношении обработки и защиты персональных данных и иных локальных нормативных актов и приказов по Кооперативу, касающихся вопросов обработки персональных данных.

5. В случае попытки посторонних лиц получить от меня сведения о персональных данных немедленно сообщить об этом руководству (председателю, правлению Кооператива).

6. В случае моего увольнения либо прекращения доступа к персональным данным в связи с переводом на другую должность или по иным причинам, все носители персональных данных, находившиеся в моем распоряжении, передать лицу, ответственному за организацию обработки персональных данных в организации, а с личных носителей, принадлежащих мне, стереть имеющиеся персональные данные.

7. Об утрате или недостаче носителей персональных данных и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможного разглашения персональных данных немедленно сообщать руководству кооператива.

Подписанием настоящего обязательства подтверждаю, что до моего сведения доведены положения действующего законодательства Российской Федерации, а также Политики Кооператива в отношении обработки и защиты персональных данных и иных локальных нормативных актов, касающихся вопросов обработки персональных данных.

Я предупрежден(а) о том, что в случае разглашения мною сведений, составляющих персональные данные, допущения при обработке персональных данных иных нарушений законодательства в области обработки персональных данных я несу дисциплинарную и индивидуальную материальную ответственность в порядке, установленном Трудовым кодексом Российской Федерации и Гражданским кодексом Российской Федерации, а также гражданско-правовую, административную и уголовную ответственность в порядке, установленном федеральными законами.

(подпись) (Ф. И. О. полностью)

«____» _____ 20__ г.

Приложение N 3 к Приказу № __ от «___»
_____ 20__ г.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____, паспорт серия _____ № _____ выдан «__» _____ г. _____,
(кем выдан)
зарегистрированный(ая) по адресу: _____ даю _____
(наименование Кооператива)
(ОГРН _____, ИНН _____), зарегистрированному по адресу: _____ _____, (далее – Кооператив) согласие на обработку своих персональных данных.

В лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных)

_____
(фамилия, имя, отчество полностью)
паспорт серия _____ № _____ выдан «__» _____ г. _____,
(кем выдан
проживающий по адресу: _____
действующий от имени субъекта персональных данных на основании _____
_____
(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

Цель обработки персональных данных:

- обеспечение соблюдения требований законодательства Российской Федерации;
- оформление и регулирование трудовых отношений;
- отражение информации в кадровых документах;
- начисление заработной платы;
- исчисление и уплата налоговых платежей и страховых взносов, предусмотренных законодательством Российской Федерации;
- предоставление законодательно установленной отчетности в отношении физических лиц в ИФНС и внебюджетные фонды;
- подача сведений в банк для оформления банковской карты и последующего перечисления на нее заработной платы;
- предоставление налоговых вычетов и льгот;
- охрана труда, обеспечение безопасных условий труда;
- исполнение обязательств, предусмотренных трудовым договором и договорами об обучении (профессиональной переподготовке, повышении квалификации, получении профессионального образования или дополнительного профессионального образования).

_____
указать иные цели (при наличии)
_____

Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- свидетельство о гражданстве (при необходимости);
- реквизиты документа, удостоверяющего личность;
- идентификационный номер налогоплательщика, дата постановки его на учет, реквизиты свидетельства постановки на учет в налоговом органе;
- номер свидетельства обязательного пенсионного страхования, дата регистрации в системе обязательного пенсионного страхования;
- номер полиса обязательного медицинского страхования;

- адрес фактического места проживания и регистрации по месту жительства и (или) по месту пребывания;
- почтовый и электронный адреса;
- номера телефонов;
- фотографии, фотографическое изображение лица;
- сведения об образовании, профессии, специальности и квалификации, реквизиты документов об образовании;
- сведения о семейном положении и составе семьи;
- сведения об имущественном положении, доходах, задолженности;
- сведения о занимаемых ранее должностях и стаже работы, воинской обязанности, воинском учете;
- сведения об адресе (месте нахождения) рабочего места или места осуществления трудовой функции;
-

_____
_____

(указать иные категории ПДн, в случае их обработки)

Наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Кооператива, если обработка будет поручена такому лицу_____

_____

(указать полное наименование юридического лица, фамилия, имя, отчество и адрес физического лица, осуществляющего обработку персональных данных по поручению Кооператива, которому будет поручена обработка)

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Кооперативом способов обработки персональных данных:
Обработка вышеуказанных персональных данных будет осуществляться путем смешанной (автоматизированной, не автоматизированной) обработки персональных данных следующими способами:
сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление, доступ, обезличивание, блокирование, удаление, уничтожение персональных данных (только те, которые применяются реально).

Обработка вышеуказанных персональных данных будет осуществляться путем _____
_____ обработки персональных данных.

(указать способ обработки (смешанной, автоматизированной, неавтоматизированной)

Даю согласие на передачу (предоставление) Кооперативом моих данных: _____
_____

(указать полное наименование и адрес юридического лица, на передачу которому дается согласие)

путем _____

(предоставления, допуска)

Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва

Настоящее согласие на обработку персональных данных действует с момента его предоставления Кооперативу на весь период исполнения обязательств, предусмотренных вышеуказанными договорами, и может быть отозвано мной в любое время путем подачи Кооперативу заявления в простой письменной форме, если иное не установлено законом.
Персональные данные субъекта подлежат хранению в течение сроков, установленных законодательством Российской Федерации. Персональные данные уничтожаются: по достижению целей обработки персональных данных; при ликвидации или реорганизации Кооператива; на основании письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных (Кооператив прекратит обработку таких персональных данных в течение *3 (трех) рабочих дней*, о

чем будет направлено письменное уведомление субъекту персональных данных в течение *10 (десяти) рабочих дней*.

Трансграничная передача персональных данных в процессе их обработки не осуществляется.

Место нахождения базы данных информации, содержащей персональные данные граждан РФ, находится на территории Российской Федерации.

При этом в полной мере обеспечивается безопасность персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

_____ /_____/ «__» _____ 20__ г.

Приложение N 4 к Приказу № __ от «___» _____ 20__ г.

Согласие на обработку персональных данных,
разрешенных субъектом персональных данных для распространения

Я,_____
_, паспорт серия _____ № _____ выдан «__» _____ г. _____,
зарегистрированный(ая) по адресу: _____
адрес электронной почты/телефон/почтовый адрес (*хотя бы одно из перечисленного*): _____
настоящим своей волей и в своем интересе даю свое согласие на обработку моих персональных данных и разрешаю их распространение.

Полное и сокращенное наименование Кооператива, осуществляющего обработку персональных данных:

_____
_____(далее – Кооператив),

ИНН _____, ОГРН _____,

Адрес Кооператива: _____.

Информационные ресурсы Кооператива, посредством которых будет осуществляться предоставление доступа неограниченному кругу лиц и иные действия: https://www._____/

Цель обработки персональных данных:

- обеспечение соблюдения требований законодательства Российской Федерации;
- оформление и регулирование трудовых отношений;
- отражение информации в кадровых документах;
- начисление заработной платы;
- исчисление и уплата налоговых платежей, предусмотренных законодательством Российской Федерации;
- представление законодательно установленной отчетности в отношении физических лиц в ИФНС и внебюджетные фонды;
- подача сведений в банк для оформления банковской карты и последующего перечисления на нее заработной платы;
- предоставление налоговых вычетов и льгот;
- обеспечение безопасных условий труда;
- исполнение обязательств, предусмотренных трудовым договором и договорами об обучении (профессиональной переподготовке, повышении квалификации, получении профессионального образования и дополнительного профессионального образования).

указать иные цели (при наличии)

_____

Категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных

1. Персональные данные, не относящиеся к специальным категориям:

Фамилия	*Да*
Имя	*Да*
Отчество (при наличии)	*Да*
Год рождения	*Да*
Месяц рождения	*Да*
Дата рождения	*Да*
Адрес места жительства	*Да*
Семейное положение, состав семьи	*Да*
Образование, квалификация	*Да*
Профессия	*Да*
Социальное положение	*Да*
Доходы	*Да*
Адрес места осуществления трудовой функции	*Да*
Должность, структурное подразделение	*Да*
2. Специальные категории персональных данных:	
Расовая принадлежность	*Нет*
Национальная принадлежность	*Нет*
Политические взгляды	*Нет*
Религиозные или философские убеждения	*Нет*
Состояние здоровья	*Нет*
Состояние интимной жизни	*Нет*
Сведения о судимости	*Да*
Сведения об административных правонарушениях, их отсутствии	*Да*
3. Биометрические персональные данные:	
Фотографическое изображение лица	*Да*
Аудиозапись голоса *Аудиовидеозапись человека*	*Да*

Категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов

Персональные данные		
Перечень	**Передача персональных данных Кооперативом неограниченному кругу лиц**	**Обработка персональных данных неограниченным кругом лиц**
Адрес места жительства	не запрещено	не запрещено
Семейное положение, состав семьи	-//-	-//-
Доходы	-//-	-//-
	-//-	-//-

Специальные категории персональных данных		
Перечень	**Передача персональных данных Кооперативом неограниченному кругу лиц**	**Обработка персональных данных неограниченным кругом лиц**
Сведения о судимости, включая ее отсутствие	не запрещено	не запрещено
Сведения об административных правонарушениях, их отсутствии	*-//-*	*-//-*
Биометрические персональные данные		
Перечень	**Передача персональных данных Кооперативом неограниченному кругу лиц**	**Обработка персональных данных неограниченным кругом лиц**
Фотографическое изображение лица	не запрещено	не запрещено
Аудиозапись голоса	*-//-*	*-//-*
Аудиовидеозапись человека	*-//-*	*-//-*

Условия, при которых полученные персональные данные могут передаваться Кооперативом, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных)

Условия передачи персональных данных Кооперативом по сети(-ям)	с использованием информационно-телекоммуникационных сетей (полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, с использованием информационно-телекоммуникационных сетей)

Отсутствуют условия и запреты для всех категорий и перечней данных	_____ *Подпись субъекта ПДн*

Срок действия согласия

Настоящее согласие на обработку персональных данных действует с момента его предоставления Кооперативу на период *исполнения обязательств, предусмотренных указанными выше договорами,* и может быть отозвано мной в любое время путем подачи Кооперативу заявления в простой письменной форме, если иное не установлено законом.

Трансграничная передача персональных данных в процессе их обработки не осуществляется.

Место нахождения базы данных информации, содержащей персональные данные граждан РФ, находится на территории Российской Федерации.

При этом в полной мере обеспечивается безопасность персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

_____ /____/ «__» _____ 202_ г.

Приложение N 5 к Приказу № __ от «___» _____ 20__ г.

(Согласие на обработку персональных данных и их передачу третьим лицам при заключении договора займа / членства / ассоциированного членства)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____, паспорт серия _____ № _____ выдан «__» _____ г. _____,
(кем выдан)
зарегистрированной(го) по адресу: _____ даю _____
(наименование Кооператива)
(ОГРН _____, ИНН _____), зарегистрированному по адресу: _____ _____, (далее – Кооператив) согласие на обработку своих персональных данных.

Цель обработки персональных данных:

исполнение обязательств, предусмотренных договорами о членстве (ассоциированном членстве) в Кооперативе и о предоставлении мне или мною (либо представителем юридического лица – члена или ассоциированного члена Кооператива) заемных денежных средств, а также обязательств, возникших из указанных договорных обязательств, их неисполнения или ненадлежащего исполнения.

Перечень персональных данных, на обработку которых дается согласие:

- *фамилия, имя и отчество (при наличии последнего);*
- *дата и место рождения;*
- *пол;*
- *гражданство;*
- *реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии);*
- *почтовый адрес места жительства (регистрации) или места пребывания;*
- *идентификационный номер налогоплательщика (при наличии);*
- *информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии);*
- *сведения о целях установления и предполагаемом характере деловых отношений с кооперативом, сведения о видах финансово-хозяйственной деятельности;*
- *сведения о статусе индивидуального предпринимателя;*
- *сведения о статусе плательщика налога на профессиональный доход (доход физических лиц от деятельности, при ведении которой они не имеют*

работодателя и не привлекают наемных работников по трудовым договорам, а также доход от использования имущества);

- *сведения о финансовом положении;*
- *сведения о семейном положении и составе семьи;*
- *сведения об имущественном положении как индивидуальном, так и совместном с супругом, доходах, задолженности, обязательствах (правах и обязанностях) имущественного характера;*
- *сведения о деловой репутации;*
- *сведения об источниках происхождения денежных средств и (или) иного имущества клиента;*
- *сведения о бенефициарном владельце;*
- *(в случае, если клиент имеет статус лица, указанного в п.п. 1 п. 1 ст. 7.3 Федерального закона № 115-ФЗ) должность клиента, наименование и адрес его работодателя;*
- *степень родства либо статус (супруг или супруга) клиента по отношению к лицу, указанному в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ;*
- *номера телефонов и факса (при наличии);*
- *адрес электронной почты;*
- *иная контактная информация (при наличии).*

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Кооперативом способов обработки персональных данных:

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной (автоматизированной и неавтоматизированной) обработки персональных данных следующими способами:

- сбор,
- запись,
- систематизация,
- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,
- передача (предоставление, доступ),
- обезличивание,
- блокирование,
- удаление,
- уничтожение –

персональных данных *(оставить только те, которые применяются реально)*

Обработка вышеуказанных персональных данных будет осуществляться путем _____ обработки персональных данных.

*(указать способ обработки: **смешанной, автоматизированной, неавтоматизированной**)*

Согласен на передачу (предоставление) Кооперативом моих данных:

указать полное наименование юридического лица; фамилия, имя, отчество и адрес физического лица; передачу которым предлагается Кооперативом	*дата*	*подпись*	Путем *(предоставления или доступа)*
1. Технические системы хранения, учета и анализа данных: «1С-Бухгалтерия» и т.п.			Доступа
2. Государственные органы: органы Федеральной налоговой службы, Центрального Банка РФ, Пенсионного фонда РФ, Фонда социального страхования, фондов обязательного медицинского страхования			Предоставления
3. Некоммерческая микрокредитная компания "Липецкий областной фонд поддержки малого и среднего предпринимательства"			Предоставления

Согласен на поручение Кооперативом обработки моих персональных данных:

указать полное наименование юридического лица, фамилия, имя, отчество и адрес физического лица, осуществляющего обработку персональных данных по поручению Кооператива, которому будет поручена обработка	*дата*	*подпись*
1.		
2.		

Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва.

Настоящее согласие на обработку персональных данных действует с момента его представления Кооперативу на период исполнения обязательств, предусмотренных вышеуказанными договорами, и может быть отозвано мной в любое время путем подачи Кооперативу заявления в простой письменной форме.

Персональные данные субъекта подлежат хранению в течение сроков, установленных законодательством Российской Федерации. Персональные данные уничтожаются: по достижению целей обработки персональных данных; при ликвидации или реорганизации Кооператива; на основании письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных (Кооператив прекратит обработку таких персональных данных в течение *3 (трех) рабочих дней*, о чем будет направлено письменное уведомление субъекту персональных данных в течение *10 (десяти) рабочих дней*.

Трансграничная передача персональных данных в процессе их обработки не осуществляется.

Место нахождения базы данных информации, содержащей персональные данные граждан РФ, находится на территории Российской Федерации.

При этом в полной мере обеспечивается безопасность персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

_____ /_____/

ФИО подпись

«__» _____ 202_ г.

Приложение N 6 к Приказу № __ от «___»
_____ 20__ г.

(Согласие на обработку персональных данных и их передачу третьим лицам при заключении договора поручительства)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____, паспорт серия _____ № _____ выдан «__» _____ г. _____,
(кем выдан)
зарегистрированный(ая) по адресу: _____

являясь поручителем по договору займа, заключенному (заключаемому) между _____
(*указывается ФИО или полное наименование заемщика-организации*)

и _____
(наименование займодавца)
(ОГРН _____, ИНН _____), зарегистрированному по адресу: _____ _____, (далее – Кооператив)

даю согласие на обработку своих персональных данных указанным выше Кооперативом.

Цель обработки персональных данных:

исполнение обязательств, предусмотренных договором поручительства.

Перечень персональных данных, на обработку которых дается согласие:

- *фамилия, имя и отчество (при наличии последнего);*
- *дата и место рождения;*
- *пол;*
- *гражданство;*
- *реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии);*
- *почтовый адрес места жительства (регистрации) или места пребывания;*
- *идентификационный номер налогоплательщика (при наличии);*
- *информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии);*
- *сведения о целях установления и предполагаемом характере деловых отношений с кооперативом, сведения о видах финансово-хозяйственной деятельности;*
- *сведения о статусе индивидуального предпринимателя;*
- *сведения о статусе плательщика налога на профессиональный доход (доход физических лиц от деятельности, при ведении которой они не имеют работодателя и не привлекают наемных работников по трудовым договорам, а также доход от использования имущества);*
- *сведения о финансовом положении;*
- *сведения о семейном положении и составе семьи;*

- *сведения об имущественном положении как индивидуальном, так и совместном с супругом, доходах, задолженности, обязательствах (правах и обязанностях) имущественного характера;*
- *сведения о деловой репутации;*
- *сведения об источниках происхождения денежных средств и (или) иного имущества клиента;*
- *сведения о бенефициарном владельце;*
- *(в случае, если клиент имеет статус лица, указанного в п.п. 1 п. 1 ст. 7.3 Федерального закона № 115-ФЗ) должность клиента, наименование и адрес его работодателя;*
- *степень родства либо статус (супруг или супруга) клиента по отношению к лицу, указанному в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ;*
- *номера телефонов и факса (при наличии);*
- *адрес электронной почты;*
- *иная контактная информация (при наличии).*

Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Кооперативом способов обработки персональных данных:

Обработка вышеуказанных персональных данных будет осуществляться путем смешанной (автоматизированной, не автоматизированной) обработки персональных данных следующими способами: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных *(только те, которые применяются реально)*.

Обработка вышеуказанных персональных данных будет осуществляться путем _____ обработки персональных данных.

(указать способ обработки (смешанной, автоматизированной, неавтоматизированной)

Согласен на передачу (предоставление) Кооперативом моих данных:

указать полное наименование юридического лица; фамилия, имя, отчество и адрес физического лица; передачу которым предлагается Кооперативом	*дата*	*подпись*	Путем *(предоставления или доступа)*
1. Технические системы хранения, учета и анализа данных: «1С-Бухгалтерия» и т.п.			Доступа
2. Государственные органы: органы Федеральной налоговой службы, Центрального Банка РФ			Предоставления
3. Некоммерческая микрокредитная компания "Липецкий областной фонд поддержки малого и среднего предпринимательства"			Предоставления

Согласен на поручение Кооперативом обработки моих персональных данных:

указать полное наименование юридического лица, фамилия, имя, отчество и адрес физического лица, осуществляющего обработку персональных данных по поручению Кооператива, которому будет поручена обработка	*дата*	*подпись*

1.		
2.		

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

Настоящее согласие на обработку персональных данных действует с момента его предоставления Кооперативу до завершения исполнения обязательств, предусмотренных вышеуказанным договором поручительства и может быть отозвано мной в любое время путем подачи Кооперативу заявления в простой письменной форме.
Персональные данные субъекта подлежат хранению в течение сроков, установленных законодательством Российской Федерации. Персональные данные уничтожаются: по достижению целей обработки персональных данных; при ликвидации или реорганизации Кооператива; на основании письменного обращения субъекта персональных данных с требованием о прекращении обработки его персональных данных (Кооператив прекратит обработку таких персональных данных в течение *3 (трех) рабочих дней*, о чем будет направлено письменное уведомление субъекту персональных данных в течение *10 (десяти) рабочих дней*.
Трансграничная передача персональных данных в процессе их обработки не осуществляется.
Место нахождения базы данных информации, содержащей персональные данные граждан РФ, находится на территории Российской Федерации.
При этом в полной мере обеспечивается безопасность персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ.

_____ /_____/ «__» _____ 20__ г.

Приложение 5. Приказ об утверждении перечня ИС ПДн

_____
(наименование организации)

_____
(адрес местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
об утверждении перечня информационных систем персональных данных

_____ «___»_____20__ г.
(место издания)

В целях выполнения требований Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить перечень информационных систем персональных данных (ИС ПДн) (**Приложение № 1**) _____ (наименование организации).
2. Вносить изменения в утверждаемые перечни дополнительным приказом на основании решения сотрудника, ответственного за безопасность персональных данных при их обработке в ИС ПДн.
3. Контроль за исполнением настоящего Приказа оставляю за собой.

_____
(должность, Ф. И. О.)

С Приказом ознакомлен:

_____
(должность, Ф. И. О.)

Приложение № 1 к Приказу № __ от «___» _____ 20__ г.

ПЕРЕЧЕНЬ
информационных систем персональных данных

№ п/п	Наименование программных комплексов, входящих в состав ИС ПДн	Тип ИС ПДн по категории ПДн	Тип ИС ПДн по категории субъектов (сотрудники, субъекты, не являющиеся сотрудниками)	Количество субъектов ПДн
1	Информационная система персональных данных «Ведение бухгалтерского и кадрового учета»			
	Программа «1С: Предприятие» (Программа «1С: Управление МФО и КПК Проф»)	ИС ПДН, обрабатывающая иные категории ПДн (не специальные, не биометрические, не общедоступные)	Сотрудники, члены, ассоциированные члены и их представители	Менее чем 100 000
2	Информационная система персональных данных «Ведение учета членов и ассоциированных членов кооператива»			
	Программа «1С: Учет в МФО» (Программа «1С: Управление МФО и КПК Проф»)	ИС ПДН, обрабатывающая иные категории ПДн (не специальные, не биометрические, не общедоступные)	Субъекты, не являющиеся сотрудниками; члены, ассоциированные члены и их представители	Менее чем 100 000

	Пакет офисных приложений	ИС ПДН, обрабатывающая иные категории ПДн (не специальные, не биометрические, не общедоступные)	Субъекты, не являющиеся сотрудниками; члены, ассоциированные члены и их представители	Менее чем 100 000

Приложение 6. Приказ об утверждении мест хранения материальных носителей персональных данных

_____
(наименование организации)

_____
(адрес местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
об утверждении мест хранения материальных носителей персональных данных

_____ «___»_____20__ г.
(место издания)

В целях обеспечения режима конфиденциальности при работе с материальными носителями персональных данных в _____ (наименование организации) и в соответствии с требованиями положения об особенностях обработки персональных данных субъектов, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства РФ от 15 сентября 2008 года N 687

ПРИКАЗЫВАЮ:

1. Обеспечить раздельное хранение материальных носителей персональных данных ответственными лицами в соответствии с **приложением** к настоящему приказу.
2. Утвердить места хранения материальных носителей персональных данных в соответствии с приложением к настоящему приказу.
3. Хранить материальные носители персональных данных только в утвержденных местах.
4. Назначить ответственными лицами за обеспечение сохранности материальных носителей персональных данных в соответствии с приложением к настоящему приказу.
5. Довести до лиц, ответственных за обеспечение сохранности материальных носителей персональных данных, Постановление Правительства Российской Федерации № 687 от 15 сентября 2008 г. "Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" под роспись.

5. Контроль за исполнением настоящего Приказа оставляю за собой.

_____

(должность, Ф. И. О.)

С Приказом ознакомлены:

_____

(должность, Ф. И. О.)

_____

(должность, Ф. И. О.)

_____

(должность, Ф. И. О.)

Приложение N 1 к Приказу № __ от «___» _____ 20__ г.

№ п\п	Категория персональных данных	Место хранения	Ответственное лицо (должность, фамилия и инициалы)
1	Бумажные носители персональных данных (трудовая книжка; журналы учета трудовых книжек; личные дела; журнал учета командировок; материалы по учету рабочего времени; личная карточка Т-2; журналы сверки по военнообязанным; приказы по личному составу)	специально отведенный железный сейф (шкаф) в кабинете	_____ (должность, Ф. И. О.)
2	Бумажные носители персональных данных – досье членов и ассоциированных членов кооператива	специально отведенный железный сейф (металлические шкафы) в кабинете	_____ (должность, Ф. И. О.)
3	Электронные носители персональных данных для обработки данных в ИС ПДН	жесткие диски персональных компьютеров	_____ (должность, Ф. И. О.)
4	Съемные носители информации	специально отведенный железный сейф (шкаф) в кабинете	_____ (должность, Ф. И. О.)

Приложение 7. Приказ об уничтожении персональных данных

_____
(наименование организации)

_____
(адрес местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
об уничтожении персональных данных

_____ «___»_____20__ г.
(место издания)

Во исполнение требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и в связи с поступлением заявления о персональных данных, которые не являются необходимыми для заявленных целей обработки,

ПРИКАЗЫВАЮ:

1. На основании заявления _____ (Ф.И.О.) ____ (регистрационный номер) _____ от «____» _____ 20__ г.) удалить из информационных систем персональные данные, которые не соответствуют целям обработки. Уничтожить печатные документы с аналогичными данными, если они не подлежат обязательному хранению.
2. Оформить акт уничтожения и представить его на утверждение руководителю организации. Срок: *семь рабочих дней*.
3. Письменно уведомить субъект персональных данных о факте уничтожения.
   Ответственный: _____
   (должность, Ф. И. О.)
4. Контроль за исполнением настоящего Приказа оставляю за собой.

_____
(должность, Ф. И. О.)

С Приказом ознакомлены:

_____
(должность, Ф. И. О.)

Приложение 8. Форма акта об уничтожении персональных данных на бумажных носителях

УТВЕРЖДАЮ
_____
(наименование должности руководителя)
_____
(наименование организации)
_____
(Ф.И.О.)
«__»_____ 20__ г.

АКТ N __
об уничтожении (о прекращении обработки)
персональных данных

_____ «___»_____20__ г.
(место издания)

Комиссия в составе председателя - _____ (должность, Ф.И.О.), членов комиссии - _____ (должность, Ф.И.О.), _____ (должность, Ф.И.О.), созданная на основании приказа от «__» _____ 20__ N __, руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", составила акт о том, что произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся в _____ (наименование организации), в следующем объеме:

N п/п	Содержание персональных данных	Тип носителя	Объем	Причина уничтожения
1		Бумажный		Истечение срока хранения / достижение цели обработки
2		Бумажный		

Перечисленные носители персональных данных уничтожены путем (сжигания полностью / иным способом).

Председатель комиссии: _____ Ф.И.О

Члены комиссии: _____ Ф.И.О

_____ Ф.И.О

Приложение 9. Форма акта об уничтожении съемных носителей персональных данных

УТВЕРЖДАЮ

_____
(наименование должности руководителя)

_____
(наименование организации)

_____
(Ф.И.О.)
«__»_____ 20__ г.

АКТ N __
уничтожения съемных носителей персональных данных

_____ «___»_____20__ г.
(место издания)

Комиссия в составе председателя - _____ (должность, Ф.И.О.), членов комиссии - _____ (должность, Ф.И.О.), _____ (должность, Ф.И.О.), созданная на основании приказа от «__» _____ 20__ N __, руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", составила акт уничтожения съемных носителей персональных данных в _____ (наименование организации) в следующем объеме:

N п/п	Вид, наименование съемного носителя персональных данных	Емкость, иные характеристики	Регистрационный (учетный, серийный) номер	Маркировка носителей информации, неотторгаемая цифровая метка	Дата уничтожения	Способ уничтожения съемного носителя	Персональные данные на уничтожаемом носителе
1	2	3	4	5	6	7	8
1							
2							
3							
4							

Съемные носители персональных данных, указанные выше, полностью уничтожены.

_____ Ф.И.О

Председатель комиссии:

Члены комиссии: _____ Ф.И.О

_____ Ф.И.О

Приложение 10. Типовая форма журнала учета
съемных носителей конфиденциальной информации (персональных данных)

УТВЕРЖДАЮ

_____
(наименование должности руководителя)

_____
(наименование организации)

_____
(Ф.И.О.)
«__»_____ 202_ г.

ЖУРНАЛ
учета съемных носителей конфиденциальной информации (персональных данных)

Начат _____
Окончен _____

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра /количество экземпляров	Место установки (использования)/ дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя ПДн	Сведения об уничтожении машинных носителей ПДн, стирании информации на них (подпись, дата)
1									
2									
3									
…									

Приложение 11. Типовая форма журнала учета прохождения первичного инструктажа лицами, допущенными к работе с персональными данными

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

Журнал учета

прохождения первичного инструктажа лицами, допущенными к работе с персональными данными

Начат _____

Окончен _____

№ п/п	ФИО лица	Дата прохождения инструктажа	Подпись лица	ФИО проводившего инструктаж	Подпись проводившего инструктаж

Приложение 12. Инструкция по проведению первичного инструктажа

УТВЕРЖДАЮ
_____
(наименование должности руководителя)
_____
(наименование организации)
_____
(Ф.И.О.)
«__»_____ 202_ г.

ИНСТРУКЦИЯ
по проведению первичного инструктажа лиц, допущенных к работе с информационными системами персональных данных _____
(наименование организации).

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных _____ (наименование организации) (далее – ИС ПДн).

2. При поступлении на работу сотрудника, в том числе после выхода из отпуска по уходу за ребенком до достижения им возраста *3-х лет*, или при вступлении в кооператив члена либо ассоциированного члена, которому для исполнения обязанностей и (или) реализации прав необходим доступ к ИС ПДн (далее – новый сотрудник), лицо, ответственное в кооперативе за организацию обработки персональных данных:

а) в соответствии с п. 6 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными правовыми актами организации в отношении обработки и защиты персональных данных, перечисленными в Приложении № 1 к данной Инструкции;

б) знакомит нового сотрудника с мерами ответственности, предусмотренными за неисполнение требований по обеспечению безопасности персональных данных в ИС ПДн, которая установлена действующим законодательством Российской Федерации, правилами внутреннего трудового распорядка, трудовым договором, соглашением о полной (индивидуальной) материальной ответственности работника и другими соглашениями;

в) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа нового сотрудника.

3. Новый сотрудник может приступить к исполнению своих непосредственных обязанностей, связанных с обработкой персональных данных физических лиц, только после успешного прохождения первичного инструктажа.

Приложение N 1 к Инструкции по проведению первичного инструктажа лиц, допущенных к работе с информационными системами персональных данных

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, локальных правовых актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа.

Законодательные акты Российской Федерации о персональных данных:

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
2) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные, в том числе без использования средств автоматизации).

Локальные правовые акты _____ _____ (наименование организации):

1) Политика в отношении обработки персональных данных.
2) Инструкция администратору ИС ПДн
3) Инструкция пользователю ИС ПДн
4) Инструкция по учёту носителей персональных данных
5) Инструкция по резервному копированию и восстановлению персональных данных
6) Инструкция о порядке допуска лиц к информационным ресурсам ИС ПДн
7) Инструкция по использованию ресурсов сети Интернет
8) Инструкция по организации антивирусной защиты в ИС ПДн
9) Инструкция по организации парольной защиты

(примерный перечень)

Приложение 13. Политика в отношении обработки и защиты персональных данных физических лиц

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ФИЗИЧЕСКИХ ЛИЦ

Сельскохозяйственного потребительского кредитного кооператива «_____»

1. Общие положения

1.1. Настоящая Политика в отношении обработки и защиты персональных данных физических лиц (далее – Политика) определяет политику в отношении обработки персональных данных Сельскохозяйственного кредитного потребительского кооператива «_____» (далее – «Кооператив» или «Кооператив»).

1.2. Настоящая Политика разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» (далее - Закон о персональных данных).

1.3. Настоящая Политика определяет общий порядок, принципы и условия обработки персональных данных Кооперативом и обеспечивает защиту прав субъектов персональных данных при обработке их персональных данных.

1.4. Действие настоящей Политики распространяется на все операции, совершаемые Кооперативом с персональными данными с использованием средств автоматизации или без их использования.

1.5. Основные понятия, используемые в Политике:

- ***персональные данные*** - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
- ***персональные данные, разрешенные субъектом персональных данных для распространения*** - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Законом о персональных данных;
- ***Оператор персональных данных (Кооператив)*** – юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В настоящей Политике под «Кооперативом» понимается Кооператив;
- ***обработка персональных данных*** - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;
- ***автоматизированная обработка персональных данных*** - обработка персональных данных с помощью средств вычислительной техники;
- ***распространение персональных данных*** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- ***предоставление персональных данных*** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- ***блокирование персональных данных*** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- ***уничтожение персональных данных*** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- ***обезличивание персональных данных*** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- ***информационная система персональных данных*** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- ***трансграничная передача персональных данных*** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- ***субъект персональных данных*** - физическое лицо, данные которого обрабатываются;
- ***конфиденциальность персональных данных*** - обязательное для Кооператива и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным за ном.

2. Основные права и обязанности Кооператива персональных данных

2.1. Кооператив обязан:

2.1.1. предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных;

2.1.2. разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом;

2.1.3. при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных Законом о персональных данных;

2.1.4. принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами;

2.1.5. опубликовать, разместить в сети интернет или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных;

2.1.6. принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

2.1.7. рассматривать обращения субъекта персональных данных (его законного представителя) по вопросам обработки персональных данных и давать мотивированные ответы;

2.1.8. предоставлять субъекту персональных данных (его законному представителю) возможность безвозмездного доступа к его персональным данным;

2.1.9. обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения;

2.1.10. в срок не позднее *трех рабочих дней* с момента получения соответствующего согласия субъекта персональных данных опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

2.2. Кооператив вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Кооператива, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных.

3. Основные права субъекта персональных данных

3.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

3.2. Если субъект персональных данных считает, что Кооператив осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Кооператива в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

3.3. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3.4. Субъект персональных данных вправе:

3.4.1. требовать от Кооператива уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

3.4.2. отозвать согласие на обработку персональных данных;

3.4.3. определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения;

3.4.4. в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, установить запреты на передачу (кроме предоставления доступа) этих персональных данных Кооперативом неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц;

3.4.5. обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Закона о персональных данных или обратиться с таким требованием в суд.

4. Цели сбора персональных данных

4.1. Кооператив обрабатывает персональные данные в целях:

- осуществления деятельности, предусмотренной уставом Кооператива и Федеральным законом от 09.12.1995 № 193-ФЗ «О сельскохозяйственной кооперации»;
- заключения, исполнения, изменения и прекращения гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством Российской Федерации и уставом Кооператива;
- оформления трудовых отношений, организации кадрового делопроизводства в Кооперативе, обеспечение соблюдения трудового и пенсионного законодательства Российской Федерации, законодательства об обязательном медицинском страховании и социальном страховании;
- исполнение требований налогового законодательства Российской Федерации в связи с исчислением и уплатой налога на доходы физических лиц;
- выполнения требований действующего законодательства.

4.2. Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.3. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

4.7. В Кооперативе не собираются и не обрабатываются специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

5. Правовые основания обработки персональных данных

5.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Кооператив осуществляет обработку персональных данных, включая договоры, соглашения и иные сделки с субъектами персональных данных.

5.2. Обработка персональных данных осуществляется Кооперативом в связи с выполнением законодательно возложенных на него функций на основании:

- Конституции Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Трудового кодекса Российской Федерации;
- Налогового кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 09.12.1995 № 193-ФЗ «О сельскохозяйственной кооперации»;
- Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – Федеральный закон № 115-ФЗ);
- Федерального закона от 21.12.2013 № 353-ФЗ «О потребительском кредите (займе)»;
- Постановления Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Положения Банка России от 12.12.2014 № 444-П «Положение об идентификации некредитными финансовыми организациями клиентов, представителей клиента, выгодоприобретателей, бенефициарных владельцев в целях противодействия

легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

- Указания Банка России от 10.12.2015 N 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных»;
- иных федеральных законов, нормативных правовых актов и нормативных актов Банка России, регулирующих обработку персональных данных с участием некредитных финансовых организаций;
- устава Кооператива;
- договоров, заключаемых между Кооперативом и субъектами персональных данных;
- согласий субъектов персональных данных на обработку персональных данных (работников, заемщиков, поручителей и иных контрагентов по трудовым и гражданско-правовым договорам) и отзывов таких согласий;
- согласий на обработку персональных данных, разрешенных субъектом персональных данных для распространения, и отзывов таких согласий;
- заявлений об уточнении, изменении персональных данных физического лица.

6. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

6.1. Категории субъектов персональных данных, чьи данные обрабатываются:

6.1.1. Сотрудники Кооператива (Кооператива), бывшие сотрудники, кандидаты на трудоустройство, а также члены семьи сотрудников и кандидатов на трудоустройство.

6.1.2. Клиенты – физические лица, являющиеся или являвшиеся членами (ассоциированными членами) Кооператива.

6.1.3. Представитель клиента – физическое лицо, уполномоченное действовать от имени и в интересах клиента и (или) связанных с ним лиц во взаимоотношениях с Кооперативом.

6.1.4. Выгодоприобретатель клиента – физическое лицо, к выгоде которого клиент участвует в финансовой взаимопомощи, в том числе на основании агентского договора, договоров поручения, комиссии и доверительного управления.

6.1.5. Бенефициарный владелец клиента – физическое лицо, которое владеет клиентом – юридическим лицом либо прямо или косвенно контролирует действия клиента, в том числе имеет возможность определять решения, принимаемые клиентом.

6.1.6. Поручитель – физическое лицо, обязавшееся перед Кооперативом исполнить обязательство по предоставленному займу в случае неисполнения обязательства Клиентом.

6.1.7. Иные физические лица, персональные данные которых могут обрабатываться Кооперативом в связи с осуществлением им своей уставной деятельности, контрагенты и сотрудники (работники, руководители, представители по доверенности или в силу иной сделки) контрагентов, уполномоченные подписывать

документы и исполнять обязательства по договору (соглашению, сделке) с данным контрагентом.

6.2. В отношении категории, указанной в пункте 6.1.1 (за исключением членов семьи сотрудников), обрабатываются такие персональные данные, как:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- адреса места жительства и постоянной и (или) временной регистрации;
- контактный телефон;
- гражданство;
- образование, квалификация;
- профессия, должность;
- стаж работы;
- семейное положение, наличие детей;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- данные страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- табельный номер;
- сведения о доходах, налоговых вычетах и льготах, суммах налога на доходы и страховых взносов в государственные внебюджетные фонды;
- сведения о воинском учете;
- сведения о судимостях и административных правонарушениях, имеющих значение в связи с трудовой функцией;
- сведения о повышении квалификации, о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о социальных гарантиях;
- сведения о наличии инвалидности, беременности и иных состояний здоровья, влияющих на выполнение трудовой функции;
- адрес места осуществления трудовой функции;
- сведения по результатам специальной оценки условий труда на рабочем месте;
- сведения о занимаемой должности, структурном подразделении, ранее занимаемых должностях.

6.3. Персональные данные родственников сотрудников обрабатываются в объеме, переданном сотрудником и необходимом для предоставления гарантий и компенсаций сотруднику, предусмотренных трудовым, налоговым законодательством и законодательством о социальном обеспечении:

- фамилия, имя, отчество;
- дата и место рождения;
- серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

- серия и номер свидетельства о рождении (смерти) ребенка, сведения о выдаче указанного документа и выдавшем его органе;
- серия и номер свидетельства о заключении (расторжении) брака, сведения о выдаче указанного документа и выдавшем его органе.

6.4. В отношении клиентов обрабатываются (п. п. 1 и 1.1 ч. 1 ст. 7 Федерального закона № 115-ФЗ, Приложение 1 к Положению Банка России № 444-П):

- *фамилия, имя и отчество (при наличии последнего);*
- *дата и место рождения;*
- *пол;*
- *гражданство;*
- *реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии);*
- *почтовый адрес места жительства (постоянной и временной регистрации) или места пребывания;*
- *идентификационный номер налогоплательщика (при наличии);*
- *информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии);*
- *сведения о целях установления и предполагаемом характере деловых отношений с Кооперативом, сведения о видах финансово-хозяйственной деятельности;*
- *сведения о статусе индивидуального предпринимателя;*
- *сведения о статусе плательщика налога на профессиональный доход (доход физических лиц от деятельности, при ведении которой они не имеют работодателя и не привлекают наемных работников по трудовым договорам, а также доход от использования имущества);*
- *сведения о финансовом положении;*
- *сведения о семейном положении и составе семьи;*
- *сведения об имущественном положении как индивидуальном, так и совместном с супругом, доходах, задолженности, обязательствах (правах и обязанностях) имущественного характера;*
- *сведения о деловой репутации;*
- *сведения об источниках происхождения денежных средств и (или) иного имущества клиента;*
- *сведения о бенефициарном владельце;*
- *(в случае, если клиент имеет статус лица, указанного в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ) должность клиента, наименование и адрес его работодателя;*
- *степень родства либо статус (супруг или супруга) клиента по отношению к лицу, указанному в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ;*
- *номера телефонов и факса (при наличии);*
- *адрес электронной почты;*

- *иная контактная информация (при наличии).*

6.5. В отношении категории, указанной в пункте 6.1.2 (за исключением ассоциированных членов сельскохозяйственных кредитных кооперативов), обрабатываются (ч. 17 ст. 40.1 Федерального закона от 08.12.1995 г. N 193-ФЗ «О сельскохозяйственной кооперации»):

- сведения о наличии или отсутствии неснятой, или непогашенной судимости за преступления в сфере экономики или преступления против государственной власти.

6.6. В отношении категории, указанной в пункте 6.1.2 (за исключением ассоциированных членов сельскохозяйственных кредитных кооперативов), в связи с рассмотрением вопроса о предоставлении ипотечного займа или изменении условий договора ипотечного займа обрабатываются (ст. 6.1, ч. 2 и 8 ст. 6.1-1 Федерального закона от 21.12.2013 N 353-ФЗ «О потребительском кредите (займе)»):

- свидетельство о рождении и (или) свидетельство об усыновлении (удочерении) и (или) акт органа опеки и попечительства о назначении опекуна или попечителя;
- справка о полученных физическим лицом доходах и удержанных суммах налога;
- выписка из Единого государственного реестра недвижимости о правах отдельного лица на имевшиеся (имеющиеся) у него объекты недвижимости;
- выписка из регистра получателей государственных услуг в сфере занятости населения – физических лиц о регистрации гражданина в качестве безработного;
- справка, подтверждающая факт установления/снятия инвалидности;
- листок временной нетрудоспособности / медицинская справка из учреждения здравоохранения.

6.7. Персональные данные родственников клиентов обрабатываются в объеме, переданном клиентом в связи с рассмотрением вопроса о предоставлении ипотечного займа (за исключением ассоциированных членов сельскохозяйственных кредитных кооперативов) и исполнением требований п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ:

- фамилия, имя, отчество;
- дата и место рождения;
- адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);
- серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- серия и номер свидетельства о заключении/расторжении брака, сведения о выдаче указанного документа и выдавшем его органе;
- справка о полученных физическим лицом доходах и удержанных суммах налога, суммах страховых взносов в государственные внебюджетные фонды.

6.8. В отношении категорий, указанных в пунктах 6.1.3 - 6.1.5, обрабатываются:

- фамилия, имя и отчество (при наличии последнего);
- дата и место рождения;
- гражданство;

- реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии);
- адрес места жительства (постоянной или временной регистрации) или места пребывания;
- идентификационный номер налогоплательщика (при наличии);
- информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии);
- сведения, подтверждающие наличие у лица полномочий представителя клиента;
- номера телефонов и факсов (при наличии), адреса электронной почты;
- иная контактная информация (при наличии).

6.9. В отношении категорий, указанных в подпункте 6.1.6, обрабатываются:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес фактического места жительства);
- серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- сведения о финансовом положении, доходах и их источниках;
- номера телефонов и факсов (при наличии);
- иная контактная информация (при наличии).

7. Порядок и условия обработки персональных данных

7.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

7.2. Кооператив не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных положениями статьи 6 Закона о персональных данных.

7.3. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

7.4. Письменное согласие субъекта персональных данных должно включать:

1) фамилию, имя, отчество;
2) адрес субъекта персональных данных;
3) номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
4) наименование и адрес Кооператива;
5) цель обработки персональных данных;

6) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Кооперативом способов обработки персональных данных;
8) срок, в течение которого действует согласие, или событие, которым обусловлено ;
9) способ его отзыва;
10) подпись субъекта персональных данных;
11) средства связи с субъектом персональных данных: телефонный номер, адрес электронной почты, адрес фактического места жительства.

7.5. Кооператив вправе обрабатывать персональные данные субъекта, разрешенных субъектом персональных данных для распространения, только с его письменного согласия, которое оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Кооператив обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

7.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, должно содержать следующую информацию:

1) фамилия, имя, отчество (при наличии) субъекта персональных данных;
2) контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);
3) сведения о Кооперативе – наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер;
4) сведения об информационных ресурсах Кооператива (адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;
5) цель (цели) обработки персональных данных;
6) категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

- персональные данные (фамилия, имя и отчество (при наличии последнего); дата и место рождения; пол; гражданство; реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии); почтовый адрес места жительства (постоянной и временной регистрации) или места пребывания; идентификационный номер налогоплательщика (при наличии);

информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии); сведения о целях установления и предполагаемом характере деловых отношений с Кооперативом, сведения о видах финансово-хозяйственной деятельности; сведения о статусе индивидуального предпринимателя; сведения о статусе плательщика налога на профессиональный доход (доход физических лиц от деятельности, при ведении которой они не имеют работодателя и не привлекают наемных работников по трудовым договорам, а также доход от использования имущества); сведения о финансовом положении; сведения о семейном положении и составе семьи; сведения об имущественном положении как индивидуальном, так и совместном с супругом, доходах, задолженности, обязательствах (правах и обязанностях) имущественного характера; сведения о деловой репутации; сведения об источниках происхождения денежных средств и (или) иного имущества клиента; сведения о бенефициарном владельце; в случае, если клиент имеет статус лица, указанного в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ, – должность клиента, наименование и адрес его работодателя; степень родства либо статус (супруг или супруга) клиента по отношению к лицу, указанному в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ; номера телефонов и факса (при наличии); адрес электронной почты; иная контактная информация при ее наличии);

- специальные категории персональных данных (состояние здоровья, сведения об инвалидности, судимости, совершении административных правонарушений);
- биометрические персональные данные (фотографическое изображение лица, аудиозапись голоса, аудиовидеозапись человека);

7) категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта персональных данных);
8) условия, при которых полученные персональные данные могут передаваться Кооперативом, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);
9) срок действия согласия или обстоятельство, с которым связано прекращение действия согласия.

7.7. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются Кооперативом без права распространения.

7.8. В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных или если в предоставленном согласии не указаны категории и перечень персональных данных, такие персональные данные обрабатываются Кооперативом без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

Кооператив в срок не позднее *трех рабочих дней* с момента получения соответствующего согласия субъекта персональных данных опубликовывает информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения.

7.9. Передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных.

Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению.

7.10. Обработка персональных данных осуществляется Кооперативом следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

7.11. Кооператив организует обработку персональных данных в следующем порядке:

1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;
2) принимает настоящую Политику, локальные акты по вопросам обработки персональных данных;
3) применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных;
4) осуществляет внутренний контроль соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, другим локальным актам Кооператива;
5) проводит ознакомление сотрудников Кооператива, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, настоящей Политики, локальными

актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

7.12. Кооператив при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

- определяет угрозы безопасности персональных данных при их обработке;
- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Кооператива;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- организует работу с информационными системами, в которых обрабатываются персональные данные;
- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;
- организует обучение работников Кооператива, осуществляющих обработку персональных данных.

7.13. При обработке персональных данных Кооператив выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.14. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только сотрудниками Кооператива, осуществляющими данную работу в соответствии с трудовыми обязанностями или договорными обязательствами гражданско-правового характера.

7.15. Кооператив получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Кооперативом, а также в случаях, установленных федеральным законом.

7.16. Кооператив осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

7.17. Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

7.17.1. Персональные данные субъекта, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.

7.17.2. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

7.18. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода сотрудника из рабочего помещения.

7.19. При увольнении сотрудника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются сотрудником своему непосредственному руководителю.

7.20. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд, Фонд социального страхования и другие уполномоченные органы исполнительной власти, государственные внебюджетные фонды и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

8. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

8.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, которые должны быть предоставлены субъекту персональных данных Кооперативом в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

8.2. Сведения предоставляются субъекту персональных данных или его представителю Кооперативом при личном обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Кооперативом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Кооперативом, подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.3. Если в запросе субъекта персональных данных не отражены все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Кооператив вправе отказать в доступе к персональным данным, которые обрабатываются согласно п. 6.4 настоящей Политики, поскольку обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

8.4. В случае если субъекту персональных данных информация, касающаяся обработки его персональных данных, а также обрабатываемые персональные данные были предоставлены для ознакомления согласно п. 8.1 настоящей Политики, субъект персональных данных вправе обратиться повторно к Кооперативу или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее, чем через *30 дней* после первоначального обращения или направления первоначального запроса.

8.5. Субъект персональных данных вправе обратиться повторно к Кооперативу или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 8.4 настоящей Политики, в случае, если обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

8.6. Кооператив вправе отказать субъекту персональных данных в выполнении повторного запроса. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Кооперативе.

8.7. В срок, не превышающий *семи рабочих дней* со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Кооператив обязан внести в них необходимые изменения.

8.8. В срок, не превышающий *семи рабочих дней* со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Кооператив обязан уничтожить такие персональные данные.

8.9. Кооператив обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

8.10. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа

по защите прав субъектов персональных данных Кооператив обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки.

8.11. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Кооператив обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

8.12. В случае подтверждения факта неточности персональных данных Кооператив на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные в течение *семи рабочих дней* со дня представления таких сведений и снять блокирование персональных данных.

8.13. В случае выявления неправомерной обработки персональных данных, осуществляемой Кооперативом, Кооператив в срок, не превышающий *трех рабочих дней* с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае если обеспечить правомерность обработки персональных данных невозможно, Кооператив в срок, не превышающий *10 рабочих дней* с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение.

Об устранении допущенных нарушений или об уничтожении персональных данных Кооператив обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

8.14. В случае достижения цели обработки персональных данных Кооператив обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий *тридцати дней* с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Кооперативом и субъектом персональных данных либо если Кооператив не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

8.15. В случае отсутствия возможности уничтожения персональных данных в течение указанных сроков Кооператив осуществляет блокирование таких персональных данных

и обеспечивает уничтожение персональных данных в срок не более чем *шесть месяцев*, если иной срок не установлен федеральными законами.

8.15.1. Уничтожение персональных данных осуществляется комиссией либо иным должностным лицом, созданной (уполномоченным) на основании приказа Кооператива.

8.15.2. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

8.15.3. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

8.15.4. Факт уничтожения персональных данных оформляется актом о прекращении обработки персональных данных. Типовая форма акта утверждаются Кооперативом.

8.16. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Кооператив обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий *30 дней* с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Кооперативом и субъектом персональных данных либо если Кооператив не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

8.17. В случае предъявления субъектом персональных данных требования прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, вследствие несоблюдения положений Закона о персональных данных или обращения с таким требованием в суд, Кооператив обязан прекратить передачу (распространение, предоставление, доступ) персональных данных в течение *трех рабочих дней* с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение *трех рабочих дней* с момента вступления решения суда в законную силу.

9. Защита персональных данных

9.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

9.2. В соответствии с требованиями нормативных документов Кооперативом создана система защиты персональных данных, состоящая из подсистем правовой, организационной и технической защиты.

9.3. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование системы защиты персональных данных.

9.4. Подсистема организационной защиты включает в себя организацию структуры управления системы защиты персональных данных, разрешительной системы, защиты информации при работе с сотрудниками, клиентами и иными лицами.

9.5. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

9.6. Основными мерами защиты персональных данных, используемыми Кооперативом, являются:

9.6.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите персональных данных.

9.6.2. Определение актуальных угроз безопасности персональных данных при их обработке в информационной системе и разработка мер и мероприятий по защите персональных данных.

9.6.3. Разработка политики в отношении обработки персональных данных.

9.6.4. Установление правил доступа к персональным данным, обрабатываемым в информационной системе, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе.

9.6.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их должностными обязанностями.

9.6.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

9.6.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

9.6.8. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ.

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

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

9.6.11. Обучение работников Кооператива, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам,

определяющим политику Кооператива в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

9.6.12. Осуществление внутреннего контроля, учета и аудита.

9.7. Требования к системе защиты персональных данных:

9.7.1. Система защиты персональных данных должна соответствовать требованиям Постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9.7.2. Система защиты персональных данных должна обеспечивать:

- своевременное обнаружение и предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

9.7.3. Средства защиты информации, применяемые в информационных системах, должны в установленном порядке проходить процедуру оценки соответствия.

9.8. Методы и способы защиты информации в информационных системах персональных данных.

9.8.1. Методы и способы защиты информации в информационных системах персональных данных Кооператива должны соответствовать требованиям:

- приказа ФСТЭК 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»;
- приказа ФСБ от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (в случае определения Кооперативом необходимости использования средств криптографической защиты информации для обеспечения безопасности персональных данных).

9.8.2. Основными методами и способами защиты информации в информационных системах персональных данных являются методы и способы защиты информации от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование,

копирование, распространение персональных данных, а также иных несанкционированных действий.

9.8.3. Выбор и реализация методов и способов защиты информации в информационно-телекоммуникационной сети осуществляется в соответствии с рекомендациями регуляторов в области защиты информации – ФСТЭК России и ФСБ России, с учетом определяемых Кооперативом угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы.

9.8.4. Выбранные и реализованные методы и способы защиты информации должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке.

10. Заключительные положения

10.1. Положение утверждается и вводится в действие приказом председателя (руководителя) Кооператива. Установленные положением режим и требования обязательны для соблюдения всеми работниками, членами и ассоциированными членами Кооператива.

10.2. Положение изменяется и дополняется в связи с изменениями и дополнениями в законодательство и нормативные акты Банка России о защите персональных данных, касающимися установленного в Кооперативе режима обработки персональных данных.

10.3. Изменения и дополнения в Положение утверждаются и вводятся в действие приказом председателя Кооператива

10.4. К действующей редакции Положения и к обновляемым впоследствии редакциям обеспечен неограниченный доступом для всех заинтересованных лиц.

10.5. Действующая редакция Положения хранится в месте нахождения Кооператива и размещается на его официальном сайте в информационно-телекоммуникационной сети «Интернет», при отсутствии последнего – на сайте саморегулируемой организации сельскохозяйственных кредитных потребительских кооперативов или кредитных потребительских кооперативов, членом которой является Кооператив.

10.6. Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации, правилами внутреннего трудового распорядка и трудовыми договорами, дополнительными соглашениями к ним (соглашениями об индивидуальной материальной ответственности), заключенными с работниками.

Приложение 14. Отзыв согласия на обработку персональных данных, ранее разрешенных для распространения

_____

_____

(***наименование и адрес СКПК, получившего согласие субъекта персональных данных на распространение персональных данных***)

От _____

(*Ф. И. О.; почтовый адрес; номер телефона; адрес электронной почты субъекта персональных данных*)

Отзыв согласия на обработку персональных данных, ранее разрешенных для распространения

Настоящим, в соответствии с требованиями статьи 10.1 Федерального закона "О персональных данных" от 27.07.2006 г. № 152-ФЗ, отзываю свое согласие на обработку персональных данных, ранее разрешенных для распространения моим согласием на обработку персональных данных от __.__.202_ г. (***дата*)**.

Прошу прекратить обработку следующих персональных данных:

- _____.

(перечень персональных данных, обработка которых должна быть прекращена)

в срок, не превышающий *трех рабочих дней* с даты поступления настоящего отзыва.

_____ _____

(Число, месяц, год) *(**подпись)*** *(**Ф. И. О.**)*

Приложение 15. Приказ об утверждении технической документации (инструкций, классификаций и положения о проверках)

_____
(наименование организации)

_____
(адрес местонахождения организации)
ИНН _____, ОГРН _____

Приказ № __
Об утверждении технической документации
для применения в работе с персональными данными физических лиц

_____ «___»_____20__ г.
(место издания)

Во исполнение требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и подзаконных нормативных правовых актов

ПРИКАЗЫВАЮ:

1. Утвердить следующие технические документы, применяемые в работе с персональными данными физических лиц:

- Акт определения уровня защищенности персональных данных контрагентов кооператива и представителей контрагентов (**приложение 1** к настоящему приказу);

- Акт определения уровня защищенности персональных данных сотрудников кооператива (**приложение 2** к настоящему приказу);

- Инструкция администратора информационной безопасности информационных систем (**приложение 3** к настоящему приказу);

- Инструкция по организации парольной защиты в ИС ПДн (**приложение 4** к настоящему приказу);

- Инструкция по антивирусной защите в информационных системах (**приложение 5** к настоящему приказу);

- Инструкция по резервному копированию в информационных системах (**приложение 6** к настоящему приказу);

- Инструкция по использованию, хранению, учету и ликвидации машинных носителей информации в информационных системах (**приложение 7** к настоящему приказу);

- Инструкция пользователя информационных систем (**приложение 8** к настоящему приказу);

- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (**приложение 9** к настоящему приказу);

- Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах (**приложение 10** к настоящему приказу);

- Частная модель угроз безопасности персональных данных при их обработке в ИС ПДн (**приложение 11** к настоящему приказу).

2. Использовать в работе, связанной с обращением с персональными данными физических лиц, документы, указанные в пункте 1 настоящего приказа.

3. При наличии необходимости, вносить изменения и дополнения в данные документы. О необходимых изменениях и дополнениях сообщать мне.

3. Контроль за исполнением настоящего приказа оставляю за собой.

_____
(должность, Ф. И. О.)

С Приказом ознакомлены:

_____
(должность, Ф. И. О.)

_____
(должность, Ф. И. О.)

_____
(должность, Ф. И. О.)

Приложение № 1. Акт определения уровня защищенности персональных данных контрагентов кооператива и представителей контрагентов

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

АКТ

определения уровня защищенности персональных данных в «*Наименование ИС ПДн, например, 1С-Бухгалтерия*»

1. На основании Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», комиссия в составе:

Председатель комиссии: *должность* *ФИО*

Члены комиссии: *должность* *ФИО*

должность *ФИО*

должность *ФИО*

рассмотрела исходные данные об информационной системе, необходимые для определения уровня защищенности персональных данных в «*Наименование ИС ПДн*», расположенной по адресу: *адрес*.

2. В ходе обследования комиссия установила:

2.1 «*Наименование ИС ПДн*» является информационной системой, обрабатывающей иные категории персональных данных;

2.2 «*Наименование ИС ПДн*» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками Кооператива;

2.3 Объем обрабатываемых персональных данных в «*Наименование ИС ПДн*» составляет менее 100 000 субъектов персональных данных.

2.4 Для «*Наименование ИС ПДн*» актуальны угрозы 3-го типа, т.е. не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Заключение комиссии:

В соответствии с п. 11 Постановления Правительства РФ от 01.11.2012 № 1119 «Об учреждении требований к защите персональных данных при их обработке в информационных системах персональных данных» признать необходимым обеспечение 4-го уровня защищенности персональных данных при их обработке в «*Наименование ИС ПДн*».

Председатель
комиссии:

Члены комиссии:

«__» _____ 20__ г.

Приложение № 2. Акт определения уровня защищенности персональных данных сотрудников кооператива

УТВЕРЖДАЮ

_____
(наименование должности руководителя)

_____
(наименование организации)

_____
(Ф.И.О.)
«__»_____ 20__ г.

АКТ
определения уровня защищенности персональных данных в «*Наименование ИС ПДн*»

1. На основании Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», комиссия в составе:

Председатель комиссии: *должность* *ФИО*
Члены комиссии: *должность* *ФИО*
должность *ФИО*
должность *ФИО*

рассмотрела исходные данные об информационной системе, необходимые для определения уровня защищенности персональных данных в «*Наименование ИС ПДн*», расположенной по адресу: *адрес*.

2. В ходе обследования комиссия установила:

a. «*Наименование ИС ПДн*» является информационной системой, обрабатывающей иные категории персональных данных.

b. «*Наименование ИС ПДн*» является информационной системой, обрабатывающей персональные данные субъектов персональных данных, являющихся сотрудниками Кооператива.

c. Объем обрабатываемых персональных данных в «*Наименование ИС ПДн*» составляет менее 100 000 субъектов персональных данных.

d. Для «*Наименование ИС ПДн*» актуальны угрозы 3-го типа, т.е. не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Заключение комиссии:

В соответствии с п. 11 Постановления Правительства РФ от 01.11.2012 г. № 1119 «Об учреждении требований к защите персональных данных при их обработке в информационных системах персональных данных» признать необходимым обеспечение 4-го уровня защищенности персональных данных при их обработке в «*Наименование ИС ПДн*».

Председатель
комиссии:

Члены комиссии:

«__» _____ 20__ г.

Приложение № 3. Инструкция администратора информационной безопасности информационных систем

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

ИНСТРУКЦИЯ АДМИНИСТРАТОРА

информационной безопасности информационных систем *Полное наименование организации*

1. Общие положения

1.1. Инструкция Администратора информационной безопасности информационных систем *Полное наименование организации* (далее – ИС Кооператива) (далее – Инструкция) определяет функции, права и обязанности Администратора информационной безопасности (далее – Администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении (применении) документов об обработке персональных данных в ИС Кооператива.

1.2. Обязанности Администратора ИБ исполняет сотрудник Кооператива, назначенный ответственным за безопасность персональных данных при их обработке в ИС ПДн приказом руководителя Кооператива и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС Кооператива.

1.3. Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.

2. Должностные обязанности

2.1. Администратор ИБ обязан:

2.1.1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей ИС Кооператива.

2.1.2. Осуществлять оперативный контроль за работой пользователей ИС Кооператива, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на

возникающие нештатные ситуации.

2.1.3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС Кооператива СЗИ.

2.1.4. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.

2.1.5. Не реже *одного раза в месяц* проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил.

2.1.7. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже, чем *один раз в неделю*.

2.1.8. Управлять средствами антивирусной защиты в соответствии с «Инструкцией по антивирусной защите в информационных системах *Полное наименование организации*».

2.1.9. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

2.1.10. Проводить не реже *одного раза в 6 месяцев* контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в соответствии с «Инструкцией по организации парольной защиты *Полное наименование организации*».

2.1.11. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС Кооператива.

2.1.12. По каждому экземпляру документа осуществлять учет в соответствующем журнале:

- СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);
- эксплуатационной и технической документации к СЗИ.

2.1.13. Осуществлять хранение:

- носителей дистрибутивов СЗИ;
- лицензий и сертификатов на СЗИ.

2.1.14. Не реже *одного раза в месяц* осуществлять проверки состояния защищенности информационных ресурсов от сбоев в системе электропитания.

2.1.15. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС Кооператива по

вопросам работы с СЗИ.

2.1.16. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС Кооператива, связанные с работой СЗИ.

2.1.17. Составлять инструкции по работе с СЗИ.

2.1.18. Докладывать руководителю Кооператива об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

2.1.19. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать руководителю Кооператива о случаях возникновения внештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС Кооператива.

3. Права

3.1. Администратор ИБ имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС Кооператива.

3.1.2. Непосредственно обращаться к пользователям автоматизированного рабочего места с требованием прекращения работы в ИС Кооператива при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. В пределах своей компетенции сообщать руководителю Кооператива обо всех недостатках в работе ИС Кооператива и их системы защиты.

3.1.4. Требовать от руководителя Кооператива обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

3.1.6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей, в т.ч. вести мониторинг действий пользователей ИС Кооператива.

3.1.7. Вносить свои предложения по совершенствованию мер защиты информации в ИС Кооператива.

4. Ответственность

4.1. Администратор ИБ ИС Кооператива несет ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей

деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Лист ознакомления
с Инструкцией администратора информационной безопасности информационных систем *Полное наименование организации*

№ п/п	**ФИО**	**Должность**	**Дата ознакомления**	**Подпись**
1.				
2.				
3.				

Приложение № 4. Инструкция по организации парольной защиты в ИС ПДн

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

ИНСТРУКЦИЯ
по организации парольной защиты в ИС ПДн *(Полное наименование организации)*

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в *Полное наименование организации* (далее по тексту – Кооператив), а также контроль над действиями пользователя при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на сотрудника, назначенного ответственным за безопасность персональных данных при их обработке в ИС ПДн (далее – Ответственный сотрудник).
2. Личный пароль должен выбираться и генерироваться пользователем ИС самостоятельно с учетом следующих требований:
   - длина пароля должна быть не менее шести символов;
   - в числе символов пароля ***обязательно должны присутствовать*** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
   - символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
   - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (например: ЭВМ, USER, СКПК и т.п.);
   - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
   - личный пароль пользователь не имеет права сообщать никому.

Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование пароля, не соответствующего данным требованиям, а также за разглашение парольной информации.

3. При возникновении нештатных ситуаций, форс-мажорных обстоятельств и технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передать Ответственному сотруднику. Опечатанные конверты с паролями исполнителей должны храниться в сейфах Правления (а если Правление не формировалось – Председателя) Кооператива.
4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже *одного раза в 6 месяцев*.
5. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри Кооператива и т.п.) должна производиться Ответственным сотрудником немедленно после окончания последнего сеанса работы данного пользователя с системой.
6. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Кооператива и другие обстоятельства) Ответственного сотрудника.
7. В случае компрометации личного пароля пользователя ИС, должны быть немедленно предприняты меры в соответствии с п. 5 или п. 6 настоящей Инструкции – в зависимости от полномочий владельца скомпрометированного пароля.
8. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в сейфе Председателя Кооператива.
9. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Ответственного сотрудника.

Лист ознакомления
с инструкцией по парольной защите

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
4.				
5.				
6.				

Приложение № 5. Инструкция по антивирусной защите в информационных системах

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

ИНСТРУКЦИЯ

по антивирусной защите в информационных системах *Полное наименование организации*

1. Общие положения

1.1. Настоящая Инструкция предназначена для всех сотрудников *Полное наименование организации* (далее – Кооператив), имеющих доступ к информационным системам (ИС) Кооператива.

1.2. Инструкция устанавливает требования и ответственность при организации защиты информации от воздействия вредоносных компьютерных программ (вирусов).

1.3. Инструкция регулирует вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС Кооператива.

2. Обеспечение антивирусной защиты

2.1. Порядок организации антивирусной защиты.

2.1.1. Для организации антивирусной защиты ИС допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства общего применения.

2.1.2. Антивирусное средство защиты должно быть установлено на все средства вычислительной техники (СВТ) при наличии технической возможности.

2.1.3. Права по управлению (администрированию) средствами антивирусной защиты предоставлены только сотруднику, назначенному ответственным за безопасность персональных данных при их обработке в ИС ПДн (далее – Ответственный сотрудник).

2.1.4. В Кооперативе обеспечивается централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной

защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (автоматизированных рабочих местах).

2.1.5. В Кооперативе обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

2.2. Порядок проведения антивирусного контроля.

2.2.1. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется Ответственным сотрудником на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка администратором информационной безопасности.

2.2.2. При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.

2.2.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИС Кооператива обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и Ответственного сотрудника, владельца зараженных файлов, а также контрагентов Кооператива, контрольно-ревизионные органы и организации, использовавшие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на съемном носителе информации Ответственному сотруднику для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку (при наличии).

2.3. Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.1. Ответственный сотрудник обеспечивает получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

2.3.2. Контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивается путем автоматического получения или предварительно скачиваемых обновлений из официальных источников, например, с сервера обновлений производителя антивирусного средства.

3. Ответственность при организации антивирусной защиты

3.1. Ответственность за организацию антивирусной защиты ИС Кооператива в

соответствии с требованиями настоящей Инструкции возлагается на Ответственного сотрудника.

Лист ознакомления
с инструкцией по антивирусной защите в информационных системах *Полное наименование организации*

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				

Приложение № 6. Инструкция по резервному копированию в информационных системах

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

ИНСТРУКЦИЯ

по резервному копированию в информационных системах *Полное наименование организации*

1. Общие положения

1.1. Целью настоящей Инструкции по резервному копированию в информационных системах (далее - ИС) *Полное наименование организации* (далее – Кооператива) (далее – Инструкция) является превентивная защита элементов ИС Кооператива от потери защищаемых информационных ресурсов.

1.2. Настоящая Инструкция регламентирует порядок использования систем резервного копирования, архивирования и восстановления информации.

1.3. Защита резервируемой информации в ИС Кооператива обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации в Кооперативе.

1.4. В ИС Кооператива обеспечивается регистрация событий, связанных с резервным копированием информации на резервные машинные носители информации и восстановлением информации с резервных машинных носителей информации.

1.5. Сотрудник Кооператива, назначенный ответственным за безопасность персональных данных при их обработке в ИС ПДн (далее – Ответственный сотрудник) осуществляет не реже *одного раза в три месяца* проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

1.6. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже *раза в неделю*;
- для технологической информации – не реже *раза в месяц*;

- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС ПДн – не реже *раза в месяц*, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

2. Методы резервного копирования

2.1. При применении метода инкрементного копирования (Incremental Back-Up – метод сохранения информации, при котором архивируются только измененные с момента последнего бэк-апа данные) производится резервное копирование файлов, изменившихся со времени последнего выполнения операции резервного копирования.

2.2. При применении метода полного резервного копирования (Full Back-Up) производится полное резервное копирование информационного ресурса.

3. Порядок хранения носителей резервных копий

3.1. Носители, на которые произведено резервное копирование, должны быть идентифицированы – пронумерованы номером носителя и датой проведения резервного копирования.

3.2. Хранение (размещение) резервных копий информации должно осуществляться на отдельных, размещенных вне информационной системы, средствах хранения резервных копий и в помещениях, которые исключают воздействие внешних факторов на хранимую информацию.

3.3. Носители должны храниться не менее *одного года* для возможности восстановления данных.

4. Порядок восстановления информации

4.1. Восстановление информации из резервных копий производится Ответственным сотрудником.

4.2. Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС Кооператива и доступности информации:

- для обрабатываемых персональных данных – не более *6 часов*;
- для технологической информации – не более *24 часов*;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС Кооператива – не более *24 часов*.

Лист ознакомления

с Инструкцией по резервному копированию в информационных системах *Полное наименование организации*

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
7.				
8.				
9.				

Приложение № 7. Инструкция по использованию, хранению, учету и ликвидации машинных носителей информации в информационных системах

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

ИНСТРУКЦИЯ

по использованию, хранению, учету и ликвидации машинных носителей информации в информационных системах *Полное наименование организации*

1. Общие положения

1.1. Настоящие правила регулируют вопросы защиты машинных носителей информации в информационных системах *Полное наименование организации* (далее – ИС Кооператива) от несанкционированного доступа к ним, уничтожения, а также неразрешенного раскрытия, модификации, удаления информации на них.

1.2. В качестве машинных носителей информации в настоящей инструкции рассматриваются:

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках);
- съемные машинные носители информации (CD-диски, DVD-диски, дискеты, флэш-накопители информации);
- портативные вычислительные устройства, имеющие встроенные носители информации.

1.3. Под использованием машинных носителей информации в ИС Кооператива понимается их подключение к инфраструктуре ИС Кооператива с целью обработки, приема/передачи информации между информационной системой и носителями информации.

2. Использование машинных носителей информации

2.1. В ИС Кооператива допускается использование только учтенных машинных носителей информации, которые являются собственностью Кооператива и подвергаются регулярной ревизии и контролю.

2.2. Машинные носители информации предоставляются сотрудникам Кооператива по инициативе сотрудника, ответственного за безопасность персональных данных при их обработке в ИС ПДн (далее – Ответственный сотрудник), в следующих случаях:

- необходимости выполнения вновь принятым сотрудником своих должностных обязанностей (трудовой функции) или вновь избранным (назначенным) председателем, заместителем председателя, членами правления и членами наблюдательного совета кооператива своих полномочий;
- возникновения у сотрудника (члена, ассоциированного члена или его представителя) Кооператива производственной необходимости.

2.3. При использовании сотрудниками машинных носителей информации необходимо:

2.3.1. Использовать машинные носители информации исключительно для выполнения своих обязанностей, реализации прав и полномочий.

2.3.2. Ставить в известность Ответственного сотрудника о любых фактах нарушения требований настоящих правил.

2.3.3. Бережно относиться к машинным носителям информации.

2.3.4. Обеспечивать физическую безопасность машинных носителей информации.

2.3.5. Извещать Ответственного сотрудника о фактах утраты (кражи) машинных носителей информации.

2.3.6. Перед началом работы с машинными носителями информации пользователь обязан проверять их на наличие вредоносных программ (вирусов) с помощью штатных антивирусных программ.

2.3.7. В случае обнаружения вирусов, пользователь обязан действовать в соответствии с «Инструкцией по антивирусной защите».

2.4. При использовании машинных носителей информации запрещено:

2.4.1. Использовать машинные носители информации в личных целях.

2.4.2. Передавать носители информации другим лицам (за исключением администратора информационной безопасности).

2.4.3. Оставлять машинные носители информации без присмотра или передавать на хранение другим лицам;

2.4.4. Выносить машинные носители информации из служебных помещений для работы с ними на дому и т.д.

2.5. Ответственность за подключение машинных носителей информации, не учтенных соответствующим образом, не прошедших проверку, несет пользователь, подключивший данное устройство.

3. Хранение и учет машинных носителей информации

3.1. Все находящиеся на хранении и в обращении машинные носители информации в Кооператива подлежат обязательному учёту. На каждый машинный носитель должна наноситься маркировка, позволяющая его идентифицировать.

3.2. Регистрацию машинных носителей информации осуществляет Ответственный за защиту информации в Журнале регистрации, учета и выдачи машинных носителей информации (далее – Журнал регистрации) путем занесения регистрационного или иного номера с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

3.3. Учет выдачи машинных носителей информации ведётся Ответственным сотрудником в Журнале регистрации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество лица, получившего средство, его роспись.

3.4. Сотрудники Кооператива получают учтенный машинный носитель от Ответственного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале регистрации. По окончании работ пользователь сдает машинный носитель для хранения Ответственному сотруднику, о чем делается соответствующая запись в журнале регистрации.

3.5. При поступлении нового машинного носителя информации, который будет использоваться в ИС Кооператива, Ответственный сотрудник регистрирует его в Журнале регистрации. Перед использованием новый машинный носитель информации в обязательном порядке должен пройти антивирусную проверку (при наличии технической возможности).

3.6. При передаче средств вычислительной техники (далее – СВТ) ИС Кооператива сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители (накопители на жестких дисках) изымаются из состава СВТ.

3.7. В случае возврата машинного носителя информации в Журнале регистрации Ответственным сотрудником проставляется отметка о возврате с указанием

даты, времени возврата, личных подписей передающей и принимающей стороны.

3.8. В случае увольнения или выхода члена (ассоциированного члена) из Кооператива, предоставленные машинные носители информации изымаются.

3.9. Хранить машинные носители информации нужно вдали от источников электромагнитного излучения и тепла.

4. Ликвидация машинных носителей информации и уничтожение (стирание) информации на машинных носителях

4.1. В случае утраты или уничтожения машинных носителей информации немедленно ставится в известность Ответственный сотрудник.

4.2. На утраченные носители составляется акт, соответствующие отметки вносятся в Журнал регистрации.

4.3. Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, должны быть уничтожены без возможности восстановления с составлением Акта уничтожения машинных носителей информации и последующей регистрацией в Журнале регистрации. Уничтожение машинных носителей осуществляется комиссией.

4.4. В Кооперативе обеспечивается уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации:

4.4.1. Уничтожение (стирание) информации на машинных носителях исключает возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

4.4.2. В ИС Кооператива используются следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации: полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

4.5. Ответственный сотрудник обеспечивает регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей

информации путем составления соответствующих актов и занесения в Журнал регистрации.

5. Ответственность

5.1. Ответственность за выполнение правил эксплуатации машинных носителей информации при выполнении непосредственных работ со средствами несут пользователи ИС Кооператива.

5.2. Контроль выполнения установленных правил эксплуатации, а также регистрацию и учёт машинных носителей информации осуществляет Ответственный сотрудник.

Лист ознакомления
с Правилами обращения с машинными носителями информации в информационных системах *Полное наименование организации*

№ п/п	Дата ознакомления	ФИО сотрудников	Подпись сотрудников
1.			
2.			
3.			
4.			

Приложение № 8. Инструкция пользователя информационных систем

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

ИНСТРУКЦИЯ

пользователя информационных систем *Полное наименование организации*

1 Общие положения

1.1 Инструкция пользователя информационных систем (далее – Инструкция) *Полное наименование организации* (далее – Кооператив) определяет функциональные обязанности, права и ответственность пользователей ИС Кооператива, в которых обрабатывается информация согласно утвержденному Перечню информационных систем и информации, обрабатываемой в Кооперативе.

1.2 Настоящая Инструкция подготовлена в соответствии с требованиями нормативно-методических документов по защите информации ограниченного доступа, в том числе персональных данных, не содержащей сведений, составляющих государственную тайну (далее – Информация), обрабатываемой с использованием средств автоматизации.

1.3 В настоящей Инструкции используются следующие понятия и определения:

1.3.1 Автоматизированное рабочее место (АРМ) – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

1.3.2 Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность персональных данных. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь ими): несанкционированное сообщение пароля другому лицу; утеря бумажного или машинного носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном или ином носителе информации, доступ к которому не контролируется.

1.3.3 Конфиденциальность информации – обязательное для соблюдения лицом,

получившим доступ к информации, требование не допускать ее распространение без наличия иного законного основания.

1.3.4 Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц.

1.3.5 Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.

1.3.6 Ответственный сотрудник – сотрудник или член Кооператива, в том числе член правления Кооператива, председатель или заместитель председателя Кооператива, который назначен ответственным за безопасность персональных данных при их обработке в ИС ПДн.

1.3.7 Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в информационных системах.

1.3.8 Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

1.3.9 ПДн – персональные данные.

1.3.10 Утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем.

1.3.11 Электронная вычислительная машина (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав информационной системы. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.

2 Обязанности пользователя

2.1 Пользователь ИС Кооператива обязан:

2.1.1 Знать и выполнять требования:

- настоящей инструкции;
- внутренних распорядительных документов по режиму обработки ПДн, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн;
- нормативных правовых актов действующего законодательства в области защиты ПДн.

2.1.2 Знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах в соответствии с инструкциями, требованиями, регламентирующими функционирование установленных средств защиты.

2.1.3 Хранить в тайне свой пароль доступа в ИС Кооператива, а также информацию о системе защиты, установленной в ИС Кооператива.

2.1.4 Немедленно ставить в известность Ответственного сотрудника:

- в случае утери носителя с ПДн и (или) при подозрении компрометации личных ключей и паролей;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС Кооператива.

2.1.5 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в ИС Кооператива программно-аппаратных средств защиты информации ставить в известность Ответственного сотрудника.

2.2 В случае увольнения Пользователь обязан вернуть все документы и материалы, относящиеся к ИС. В том числе: отчеты, инструкции, служебную переписку, списки сотрудников, перечни членов и ассоциированных членов, заемщиков и займодавцев Кооператива, должников, имеющих задолженность перед Кооперативом, и кредиторов Кооператива, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к ИС Кооператива, полученные в течение срока работы.

2.3 Вынос технических средств ИС Кооператива, на которых проводилась обработка ПДн, за пределы контролируемой зоны с целью их ремонта, замены и т. п. без согласования с Ответственным сотрудником запрещен.

2.4 АРМ, используемые для работы с Информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра монитора (экрана), в том числе через окна или двери в помещение.

2.5 Пользователю категорически запрещается:

- передавать кому бы то ни было, устно или письменно, Информацию, а также личные ключи и атрибуты доступа к ресурсам ИС Кооператива, открыто осуществлять ввод персонального пароля в присутствии других лиц, с ведением видеозаписи, фотосъемки и т.п.;
- выполнять работы с документами, содержащими ПДн, на дому, выносить их

из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного сотрудника;

- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие ПДн;
- использовать компоненты программного и аппаратного обеспечения ИС Кооператива в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства, в том числе отключать (блокировать) СЗИ;
- осуществлять обработку ПДн в присутствии посторонних, не допущенных к данной информации лиц;
- подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;
- записывать и хранить ПДн на неучтенных носителях информации;
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (например, временную блокировку экрана);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Ответственного сотрудника.
- обсуждать с посторонними лицами процедуры доступа к ИС Кооператива и обрабатываемые ПДн.

2.6 Без согласования с Ответственным сотрудником Пользователю запрещается:

- производить установку программных средств;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение;
- изменять установленный алгоритм функционирования аттестованной ИС Кооператива;
- запускать на рабочем месте файлы, не связанные с исполнением Пользователем служебных обязанностей;
- открывать общий доступ к папкам на своей рабочей станции (компьютере);
- привлекать посторонних лиц для производства ремонта или настройки АРМ ИС Кооператива.

3 Права пользователя

3.1 Пользователь имеет право:

3.1.1 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.2 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

4 Ответственность пользователя

4.1 Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации (ПДн).

4.2 Пользователь несет ответственность за нарушения, происходящие при работе в аттестованной ИС Кооператива, которые вызваны его неправомерными действиями, бездействием или неправильным использованием предоставленных прав, предусмотренных настоящей инструкцией.

4.3 Пользователь отвечает за правильность включения и выключения АРМ ИС Кооператива и всех действий при работе с ним.

4.4 За разглашение конфиденциальной информации (персональных данных и сведений, составляющих коммерческую тайну, в том числе тайну членов или ассоциированных членов Кооператива, либо иную охраняемую законом тайну), а также за нарушение порядка работы с документами или машинными носителями информации, сотрудники могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности, а члены и ассоциированные члены могут быть исключены из Кооператива.

Лист ознакомления

с Инструкцией пользователя информационных систем *Полное наименование организации*

№ п/п	Ф.И.О.	Должность, статус (член, ассоциированный член или его представитель)	Дата ознакомления	Подпись

№ п/п	Ф.И.О.	Должность, статус (член, ассоциированный член или его представитель)	Дата ознакомления	Подпись

Приложение № 9. Правила осуществления внутреннего контроля соответствия обработки

персональных данных требованиям к защите персональных данных

УТВЕРЖДАЮ

_____

(наименование должности руководителя)

_____

(наименование организации)

_____

(Ф.И.О.)

«__»_____ 20__ г.

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
в *Полное наименование организации*

1. Общие положения

1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в *Полное наименование организации* (далее – Кооператив) определяют план и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

2. План проведения внутренних проверок

2.1. План проведения внутренних проверок (далее – План) приведен в Приложении № 1 к настоящим Правилам.

2.2. План содержит перечень внутренних проверок и определяет для каждой из них:

- название проверки;
- периодичность проведения проверки;
- ответственного исполнителя.

2.3. Внутренние проверки проводятся в структурных подразделениях Кооператива, обрабатывающих персональные данные.

2.4. Общий срок проведения проверки не должен превышать *30 рабочих дней*.

2.5. Информация о проведенной проверке, дата ее начала и окончания, а также ее результаты, фиксируется в «Журнале учета мероприятий по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» (**приложение N 2**).

3. Порядок проведения внутренних проверок

3.1. Порядок проведения контроля выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, и соблюдения прав субъектов персональных данных.

В ходе проведения проверки необходимо:

- Провести проверку соблюдения условия по обработке персональных данных, совместимых с целями сбора персональных данных;
- Провести проверку наличия согласий в письменной форме субъектов персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ;
- Провести проверку соблюдения требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных;
- Провести проверку наличия запросов или обращений субъектов персональных данных по предоставлению информации, касающейся обработки их персональных данных, уточнению, блокированию или уничтожению персональных данных;
- Провести проверку выполнения Кооперативом в сроки, установленные законодательством РФ, обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных;
- Провести проверку выполнения Кооперативом в сроки, установленные законодательством РФ, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- Провести проверку ведения Журнала учета обращений и запросов субъектов персональных данных по вопросам обработки персональных данных.

3.2. Порядок проведения контроля выполнения требований, утвержденных Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных,

осуществляемой без использования средств автоматизации»

В ходе проведения проверки необходимо:

- Провести проверку исполнения обязанностей по соблюдению условий хранения материальных носителей персональных данных, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- Провести проверку соблюдения мер по обеспечению раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, провести проверку соблюдения мер по обеспечению раздельной обработки персональных данных (при осуществлении таких действий как использование, распространение, уничтожение, блокирование).

3.3. Порядок проведения контроля выполнения требований, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

В ходе проведения проверки необходимо:

- провести анализ реализации организационных и технических мер по обеспечению безопасности персональных данных при их обработке в «*ИС ПДн Кооператива*», утвержденных 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», путем проверки выполнения лицами, ответственными за обеспечения безопасности персональных данных в «*ИС ПДн Кооператива*», Правил осуществления внутреннего контроля (мониторинга) за обеспечением уровня защищенности персональных данных.

3.4. Порядок проведения проверки наличия и актуальности внутренней нормативной документации по обработке персональных данных

В ходе проведения проверки необходимо:

- Проверить наличие в Кооперативе и соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы порядка обработки персональных данных;
- Проверить наличие доказательств ознакомления сотрудников, членов и ассоциированных членов Кооператива, а также их представителей с внутренними нормативными документами (распоряжениями, правилами и

т.п.), регулирующими вопросы порядка обработки персональных данных в Кооперативе;

- Принять решение о необходимости актуализации внутренней нормативной базы.

Приложение N 1
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в *Полное наименование организации*

План проведения внутренних проверок

Проверка	**Периодичность**	**Методика (программа) проверки**	**Ответственный исполнитель**
Контроль выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, и соблюдения прав субъектов персональных данных	*1 раз в полгода*	Пункт 3.1 настоящих Правил	Ответственный за безопасность персональных данных при их обработке в ИС ПДн
Контроль выполнения требований, утвержденных Постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»	*1 раз в полгода*	Пункт 3.2 настоящих Правил	Ответственный за безопасность персональных данных при их обработке в ИС ПДн
Контроль выполнения требований, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	*1 раз в полгода*	Пункт 3.3 настоящих Правил	Ответственный за безопасность персональных данных при их обработке в ИС ПДн
Проверка наличия и	*1 раз в год*, а	Пункт 3.4	Ответственный

актуальности внутренней нормативной документации по обработке персональных данных	также перед проверками регуляторов	настоящих Правил	за безопасность персональных данных при их обработке в ИС ПДн

Приложение N 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в *Полное наименование организации*

ЖУРНАЛ
учета мероприятий по осуществлению внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных
(форма)

№ п/п	Мероприятие	Дата	Фамилия И.О. исполнителя	Результат	Подпись исполнителя

Приложение № 10. Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах

УТВЕРЖДАЮ

Председатель СКПК
«_____»

_____ (_____)

« ____ » _____ 20__ г.

ПОЛОЖЕНИЕ
о разграничении прав доступа к обрабатываемым персональным данным в информационных системах СКПК «_____»

1. Общие положения

В данном документе представлен список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а также их уровень прав доступа к обрабатываемым персональным данным.

Разграничение прав осуществляется на основании Отчета по результатам проведения внутренней проверки, а также исходя из характера и режима обработки персональных данных в ИС ПДн.

Список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а также их уровень прав доступа для каждой ИС ПДн представлен в Приложениях №1, 2.

Приложение N 1 к Положению о разграничении прав доступа к обрабатываемым персональным данным

ИС ПДн работников СКПК «_____»

Перечень групп, участвующих в обработке персональных данных в ИС ПДн:

Группа	Роль	Разрешенные действия
Бухгалтерия	Привилегированный пользователь	Конфигурирование, обработка, внесение дополнений (чтение, запись, модификация, удаление)
Правление, Председатель, Заместитель Председателя, Бухгалтерия, Наблюдательный совет	Пользователь	Обработка, внесение дополнений (чтение, запись, модификация)
Общий отдел, внешний пользователь (аутсорсер)	Администратор	Конфигурирование средств защиты и обработки информации, сетевых устройств и сервисов

Перечень лиц, получивших доступ к персональным данным:

№	Должность	ФИО сотрудника, члена, ассоциированного члена, их представителя	Группа	Роль
1	Главный бухгалтер		Бухгалтерия	привилегированный пользователь
2	Бухгалтер		Бухгалтерия	привилегированный пользователь
3	Бухгалтер-кассир		Бухгалтерия	пользователь
4	Председатель кооператива		Дирекция	пользователь
5	Исполнительный директор		Дирекция	пользователь

6	Программист 1С-бухгалтерии		Общий отдел	администратор
7	Программист		Общий отдел	администратор

Приложение N 2 к Положению о разграничении прав доступа к обрабатываемым персональным данным

ИС ПДн контрагентов СКПК «_____»

Перечень групп, участвующих в обработке персональных данных в ИС ПДн:

Группа	Роль	Разрешенные действия
Правление, Наблюдательный совет, председатель, заместитель председателя, главный бухгалтер	Привилегированный пользователь	Конфигурирование, обработка, внесение дополнений (чтение, запись, модификация, удаление)
Бухгалтерия, юридический отдел	Пользователь	Обработка, внесение дополнений (чтение, запись, модификация)
Общий отдел	Администратор	Конфигурирование средств защиты и обработки информации, сетевых устройств и сервисов

Перечень лиц, получивших доступ к персональным данным

№	Должность	ФИО сотрудника, члена, ассоциированного члена, их представителя	Группа	Роль
1	Председатель кооператива, заместитель председателя		Правление	пользователь

2	Исполнительный директор		Правление	пользователь
3	Главный бухгалтер		Бухгалтерия	привилегированный пользователь
4	Бухгалтер		Бухгалтерия	пользователь
5	Кассир		Бухгалтерия	пользователь
6	Экономист		Бухгалтерия	пользователь
7	Старший специалист по займам		Подразделение по выдаче и привлечению займов	привилегированный пользователь
8	Специалист по займам		Подразделение по выдаче и привлечению займов	привилегированный пользователь
9	Специалист по займам		Подразделение по выдаче и привлечению займов	привилегированный пользователь
10	Специалист по займам		Подразделение по выдаче и привлечению займов	привилегированный пользователь
11	Юрисконсульт		Юридический отдел	пользователь
12	Программист 1С- бухгалтерии		Бухгалтерия	администратор

Приложение № 11. Частная модель угроз безопасности персональных данных при их обработке в ИС ПДн

УТВЕРЖДАЮ

Председатель
СКПК «_____»

(_____)

« ___ » _____ 20__ г.

Частная модель угроз безопасности персональных данных при их обработке в ИС ПДн в СКПК «_____»

с./г. _____

20__ год

Содержание частной модели угроз:

Перечень сокращений

АРМ – автоматизированное рабочее место;
БД - база данных
ИБ - информационная безопасность
ИНН - идентификационный номер налогоплательщика
ИС ПДн – информационная система персональных данных;
НДВ – не декларированные возможности;
НСД – несанкционированный доступ;
ОС – операционная система;
ПДн – персональные данные;
ПО – программное обеспечение;
ППО - прикладное программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки;
СВТ – средства вычислительной техники
СУБД - система управления базами данных
УБПДн – угрозы безопасности персональным данным.
ФСТЭК - Федеральная служба по техническому и экспортному контролю

Термины и определения

В настоящем документе используются следующие **термины** и их определения (значения):

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами не-санкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – 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 так средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

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

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

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение

(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – 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.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный программу с целью осуществить утечку, изменить, блокировать, уничтожать информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

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

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к

персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

1. Общие положения

Настоящий документ разработан в соответствии с требованием п. 7 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Определение нарушителей и угроз безопасности персональных данных при их обработке и последующее формирование на их основе модели угроз и нарушителей является одним из необходимых мероприятий по обеспечению безопасности ПДн в информационных системах.

Выявление и учет угроз безопасности ПДн в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в информационных системах ПДн.

Настоящая Модель угроз и нарушителей учитывает требования следующих законодательных актов и нормативно-методических документов:

- Федеральный закон №152-ФЗ от 27 июля 2006 года «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК Российской Федерации № 21 от 18.02.2013 «Состав и содержание технических и организационных мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Выписка ФСТЭК Российской Федерации 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена зам. директора ФСТЭК России 14.02.2008;
- Приказ ФСБ Российской Федерации от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005);
- Указание ЦБ от 10 декабря 2015 г. N 3889-У «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

2. Основные виды угроз безопасности ПДн В ИС ПДн

2.1. Типы угроз безопасности ПДн.

Угрозы безопасности ПДн классифицируются по типу используемой уязвимости ИС ПДн. Выделяются следующие типы угроз:

- угрозы, связанные с наличием недокументированных (не декларированных) возможностей в системном программном обеспечении, используемом в ИС ПДн (угрозы 1-го типа);
- угрозы, связанные с наличием недокументированных (не декларированных) возможностей в прикладном программном обеспечении, используемом в ИС ПДн (угрозы 2-го типа);
- угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИС ПДн (угрозы 3-го типа).

Тип актуальных угроз безопасности персональных данных и необходимый уровень их защищенности определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда. Как установлено указанием Банка России от 10.12.2015 N 3889-У, угрозами безопасности персональных данных, актуальными при их обработке в используемой кооперативом информационной системе, являются в том числе:

- угроза несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных

данных, в том числе в ходе создания, эксплуатации, технического обслуживания и (или) ремонта, модернизации, снятия с эксплуатации информационной системы персональных данных;

- угроза воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;
- угроза использования методов социального инжиниринга к лицам, обладающим полномочиями в информационной системе персональных данных;
- угроза несанкционированного доступа к отчуждаемым носителям персональных данных;
- угроза утраты (потери) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в организации защиты персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в программном обеспечении информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных;
- угроза несанкционированного доступа к персональным данным лицами, не обладающими полномочиями в информационной системе персональных данных, с использованием уязвимостей, вызванных несоблюдением требований по эксплуатации средств криптографической защиты информации,

2.2. Угрозы утечки информации по техническим каналам

При обработке ПДн в ИС ПДн возможно возникновение угроз безопасности ПДн за счет реализации следующих технических каналов утечки информации:

- 1. Угрозы утечки акустической (речевой) информации, изображений лица.
- 2. Угрозы утечки видовой информации.
- 3. Угрозы утечки информации по каналам ПЭМИН.

2.2.1. Угрозы утечки акустической (речевой) информации

Источниками угроз утечки информации по техническим каналам являются физические лица, не имеющие доступа к ИС ПДн.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Носителем ПДн является пользователь ИС ПДн, осуществляющий голосовой ввод ПДн в ИС ПДн или акустическая система ИС ПДн воспроизводящая ПДн.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя при обработке ПДн, обусловлено наличием функций голосового ввода ПДн в информационную систему или функций воспроизведения ПДн акустическими средствами информационной системы.

Вывод: В ИС ПДн функции голосового ввода ПДн в ИС ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют, поэтому дальнейшее рассмотрение данной угрозы представляется ***нецелесообразным***.

2.2.2. Угрозы утечки видовой информации

Источником угроз утечки видовой информации являются физические лица, не имеющие доступа к информационной системе.

Среда распространения информативного сигнала – это физическая среда, по которой информативный сигнал может распространяться – однородная (воздушная).

Носителем ПДн являются технические средства ИС ПДн, создающие физические поля, в которых информация находит свое отражение в виде символов и образов.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ, входящих в состав ИС ПДн.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Вывод: Перехват ПДн в ИС ПДн может вестись портативной носимой аппаратурой (портативные аналоговые и цифровые фото- и видеокамеры, цифровые видеокамеры, встроенные в сотовые телефоны) – физическими лицами при их неконтролируемом пребывании в служебных помещениях или в непосредственной близости от них в условиях наличия визуального контакта.

Перехват (просмотр) ПДн осуществляется посторонними лицами путем их непосредственного наблюдения в служебных помещениях либо на расстоянии прямой видимости из-за пределов ИС ПДн с использованием оптических (оптикоэлектронных) средств.

2.2.3. Угрозы утечки информации по каналам ПЭМИН

Источником угроз утечки информации за счет ПЭМИН являются физические лица, не имеющие доступа к ИС ПДн.

Среда распространения информативного сигнала – неоднородная за счет перехода из одной среды в другую.

Носителем ПДн являются технические средства ИС ПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИС ПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническим средствами ИС ПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИС ПДн в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях технических средств ИС ПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИС ПДн.

Вывод: Количество субъектов, ПДн которых одновременно обрабатываются в информационной системе менее 1000. Соответственно, рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН, избыточно, так как утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и величиной ущерба для субъекта от полученной в результате регистрации ПЭМИН информации, следовательно, защита ПДн от данного вида угроз в дальнейшем рассматриваться не будет.

2.3. Угрозы НСД

Угрозы НСД в ИС ПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

- угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИС ПДн;
- угрозы, связанные с реализацией протоколов сетевого взаимодействия;
- угрозы внедрения (в том числе по сети) вредоносных программ (программно-математического воздействия).

2.3.1. Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИС ПДн.

Данные угрозы могут быть реализованы нарушителем в случае получения физического доступа к ИС ПДн или, по крайней мере, к средствам ввода информации в ИС ПДн. При этом можно выделить следующие угрозы:

1. Угрозы, реализуемые в ходе загрузки операционной системы.

Эти угрозы безопасности информации направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИС ПДн.

Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

2. Угрозы, реализуемые после загрузки операционной среды, независимо от того, какая прикладная программа запускается пользователем.

Эти угрозы, как правило, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) или какой-либо прикладной программой общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах по ключевым словам и копирования;
- специальными программами просмотра и копирования записей в базах данных;
- программами быстрого просмотра графических файлов, их редактирования или копирования;
- программами поддержки возможностей реконфигурации программной среды (настройки ИС ПДн в интересах нарушителя) и др.

Кроме того, к данным угрозам необходимо отнести угрозы утечки информации путем копирования ее на съемные носители.

3. Угрозы, реализуемые после загрузки операционной среды, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз представляет собой угрозы внедрения вредоносных программ.

2.3.2. Угрозы, связанные с реализацией протоколов сетевого взаимодействия.

Можно выделить следующие угрозы, реализуемые с использованием протоколов сетевого взаимодействия, реализуемые внутри распределенной сети:

1. Угрозы «Анализа сетевого трафика».

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль, а также конфиденциальная информация.

2. Угрозы сканирования сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИС ПДн и анализе ответов от них с целью выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбора идентификаторов и паролей пользователей.

3. Угрозы выявления паролей.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4. Угрозы навязывания ложного маршрута сети.

Данная угроза отсутствует в силу того, что сеть является локальной.

5. Угрозы внедрения ложного объекта сети.

Данная угроза отсутствует в силу того, что сеть является локальной.

6. Угрозы типа «Отказ в обслуживании».

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИС ПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода может служить: направленный шторм эхо-запросов по протоколу OCMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИС ПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускании каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICPM-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связанности между техническими средствами ИС ПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "Nuke", "UDP-bomb") или имеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"(, что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличии ошибок а программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИС ПДн, передача с одного адреса точного количества запросов на подключение технических средств в составе ИС ПДн, какое максимально может "вместить" трафик (направленный "шторм запросов") что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИС ПДн из-за невозможности системы заниматься ничем, кроме обработки запросов.

7. Угрозы удаленного запуска приложений.

Угроза заключается в стремлении запустить на хосте ИС ПДн различные предварительно внедренные вредоносные программы: программы-закладки,

вирусы, "сетевые шпионы", основная цель которых – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой прикладных процессов и др.

Выделяются три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений-серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов например, тексты JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля переполнение буфера). Настройка системных регистров иногда удается переключать процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широкого известного "вируса Морриса".

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, "троянскими" программами типа Back Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т.п.). В результате их использования удается добиться удаленного контроля над станциями сети.

2.3.3. Угрозы внедрения по сети вредоносных программ (программно-математического воздействия).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями

или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИС ПДн, в процессе его разработки, сопровождения, модификации и настройки.

Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС ПДн с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС ПДн.

Вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения и разнообразных сетевых технологий, обладают широким спектром возможностей и могут действовать во всех видах программного обеспечения.

Наличие в ИС ПДн вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

2.4. Источники угроз безопасности ПДн

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Источниками угроз НСД в ИС ПДн могут быть:

- нарушитель;

- носитель вредоносной программы;
- аппаратная закладка.

2.5. Категории нарушителей безопасности ПДн

Целью возможного нарушителя является нарушение характеристик безопасности защищаемых объектов путем модификации, разрушения или блокирования программных и технических средств, хищения и ознакомления с защищаемой информацией, а также навязывания ложной информации, или побуждения к принятию неверных решений.

Контролируемой зоной является территория офиса, включая помещения общего доступа, предназначенные для работы с клиентами, и помещение, в котором расположен сервер.

АРМ, расположенные в помещениях общего доступа, находятся под постоянным визуальным наблюдением работников Института, в связи с этим доступ посторонних лиц к АРМ ограничен.

С точки зрения наличия возможности постоянного или разового доступа в контролируемую зону, в которой размещены технические средства ИС ПДн, все нарушители могут быть отнесены к следующим двум категориям:

-- категория I: внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещаются технические средства ИС ПДн, а также права легального физического доступа к техническим средствам ИС ПДн;

-- категория II: внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещаются технические средства ИС ПДн.

Под внешним нарушителем информационной безопасности рассматривается нарушитель, не имеющий непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

3. Описание ИС ПДн

3.1. ИС ПДн «Ведение бухгалтерского и кадрового учета» («1С: Предприятие», «1С: Бухгалтерия»).

3.1.1. Общее описание

Назначение системы: автоматизация бухгалтерского и налогового учета.

Пользователи: сотрудники кооператива, включая бухгалтерию, члены правления, председатель (заместитель председателя) Кооператива.

ИС ПДн является локальной и состоит из одной структурной единицы офис СКПК «_____» и относится к информационной системе, обрабатывающей

персональные данные сотрудников, членов, ассоциированных членов и контрагентов Кооператива.

Обработка информационных потоков ИС ПДн осуществляется в офисе, расположенном по адресу: _____

3.1.2. Обрабатываемые в системе персональные данные.

Категория субъектов ПДн	Перечень ПДн	Хранение ПДн	
		Объем (кол-во записей)	Место и форма хранения
Сотрудники, члены, ассоциированные члены Кооператива, бывшие сотрудники, члены, ассоциированные члены, кандидаты на трудоустройство, представители членов и ассоциированных членов	• фамилия, имя, отчество; • дата и место рождения; • адреса места жительства и регистрации; • контактный телефон; • гражданство; • образование; • профессия, должность; • стаж работы; • семейное положение, наличие детей; • серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе; • данные страхового свидетельства государственного пенсионного страхования; • ИНН; • табельный номер; • сведения о доходах; • сведения о воинском учете; • сведения о судимостях; • сведения о повышении квалификации, о профессиональной переподготовке; • сведения о наградах (поощрениях), почетных званиях; • сведения о социальных гарантиях; • сведения о состоянии здоровья, влияющие на выполнение трудовой функции.	Менее *100*	ПДн содержатся в БД ИС «*1С:Бухгалтерия*»
Члены семьи сотрудников,	• фамилия, имя, отчество; • дата и место рождения;	Менее *100*	ПДн содержатся в БД ИС

членов и ассоциированных членов	• серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе; • серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе; • серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе.		«*1С:Бухгалтерия*»

3.1.3. Описание технологии функционирования и архитектуры системы

Основными составляющими ИС ПДн являются:

- центральный узел обработки данных (сервер с базой данных 1С Бухгалтерия);
- автоматизированные рабочие места (АРМ) сотрудников бухгалтерии.

Центральный узел обработки данных представляет собой сервер с базой данных 1С Бухгалтерия, с установленной операционной системой *Microsoft Windows Server 2003 R2*. В качестве антивирусной защиты используется *Антивирус Касперского 9.1для Windows Server*. Всего в рассматриваемой ИС ПДн используется один центральный узел обработки данных, который расположен по адресу: _____.

АРМ сотрудников – основное оборудование, участвующее в обработке ПДн. С помощью этого оборудования осуществляется ввод персональных данных в ИС ПДн. На данных АРМ установлена операционная система *MS Windows XP Professional SP3* и средство антивирусной защиты *Антивирус Касперского 9.1 Windows Workstation*.

3.1.4. Описание механизмов и средств защиты

Регистрация событий: регистрируются такие события, как вход и выход пользователя, изменение документов.

Для аутентификации в системе используются локальные учетные записи.

Средствами ППО настроена и контролируется следующая парольная политика:

- минимальная длина пароля – 6 символов;
- пароль должен содержать как буквы, так и цифры;
- срок действия пароля неограничен;
- независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного ПО.

3.2. ИС ПДн «Ведение учета членов и ассоциированных членов кооператива»

3.2.1. Общее описание

Назначение системы: автоматизация оформления организуемых кооперативом операций финансовой взаимопомощи, формирование базы данных, используемые в целях статистического, бухгалтерского и налогового учета и анализа.

Пользователи: сотрудники (работники) кооператива, члены правления, члены наблюдательного совета, председатель (заместитель председателя) Кооператива.

ИСПД относится к информационной системе, обрабатывающей ПДн иных лиц, не являющихся сотрудниками Кооператива.

3.2.2. Обрабатываемые в системе персональные данные:

Категория субъектов ПДн	Перечень ПДн	Хранение ПДн	
		Объем (кол-во записей)	Место и форма хранения
Члены (ассоциированные члены) Кооператива	• фамилия, имя и отчество (при наличии последнего); • дата и место рождения; • пол; • гражданство; • реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии); • почтовый адрес места жительства (регистрации) или места пребывания; • идентификационный номер налогоплательщика (при наличии); • информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии); • сведения о целях установления и предполагаемом характере деловых отношений с кооперативом, сведения о видах финансово-хозяйственной	Менее *1 000*	ПДн содержатся в БД ИС «*1С: Учёт в МФО*» («*Аудит-Эскорт»)*

	деятельности; • сведения о статусе индивидуального предпринимателя; • сведения о статусе плательщика налога на профессиональный доход (доход физических лиц от деятельности, при ведении которой они не имеют работодателя и не привлекают наемных работников по трудовым договорам, а также доход от использования имущества); • сведения о финансовом положении; • сведения о семейном положении и составе семьи; • сведения об имущественном положении как индивидуальном, так и совместном с супругом, доходах, задолженности, обязательствах (правах и обязанностях) имущественного характера; • сведения о деловой репутации; • сведения об источниках происхождения денежных средств и (или) иного имущества клиента; • сведения о бенефициарном владельце; • (в случае, если клиент имеет статус лица, указанного в п.п. 1 п. 1 ст. 7.3 Федерального закона № 115-ФЗ) должность клиента, наименование и адрес его работодателя; • степень родства либо статус (супруг или супруга) клиента по отношению к лицу, указанному в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ; • номера телефонов и факса (при наличии); • адрес электронной почты; • иная контактная информация (при наличии); • Справка об инвалидности; • Листок нетрудоспособности		
Родственники членов (ассоциированных членов) Кооператива	• фамилия, имя, отчество; • дата и место рождения; • адрес места жительства (адрес постоянной регистрации, адрес временной регистрации, адрес	Менее *1 000*	ПДн содержатся в БД ИС «*1С: Учет в МФО*»

	фактического места жительства); • серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе; • серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе; • справка о полученных физическим лицом доходах и удержанных суммах налога.		(«*Аудит-Эскорт»)*
Представитель / Выгодоприобретатель / Бенефициарный владелец членов (ассоциированных членов) Кооператива	• фамилия, имя и отчество (при наличии последнего); • дата и место рождения; • гражданство; • реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии); • адрес места жительства (регистрации) или места пребывания; • идентификационный номер налогоплательщика (при наличии); • информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии); • сведения, подтверждающие наличие у лица полномочий представителя клиента; • номера телефонов и факсов (при наличии);	Менее *1 000*	ПДн содержатся в БД ИС «*1С:Учет в МФО*» («*Аудит-Эскорт»)*
Поручители членов Кооператива	• фамилия, имя и отчество (при наличии последнего); • дата и место рождения; • пол; • гражданство; • реквизиты документа, удостоверяющего личность: серия (при наличии) и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (при наличии);	Менее *1 000*	ПДн содержатся в БД ИС «*1С: Учет в МФО*» («*Аудит-Эскорт»)*

	• почтовый адрес места жительства (регистрации) или места пребывания; • идентификационный номер налогоплательщика (при наличии); • информация о страховом номере индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования (при наличии); • сведения о целях установления и предполагаемом характере деловых отношений с кооперативом, сведения о видах финансово-хозяйственной деятельности; • сведения о статусе индивидуального предпринимателя; • сведения о статусе плательщика налога на профессиональный доход (доход физических лиц от деятельности, при ведении которой они не имеют работодателя и не привлекают наемных работников по трудовым договорам, а также доход от использования имущества); • сведения о финансовом положении; • сведения о семейном положении и составе семьи; • сведения об имущественном положении как индивидуальном, так и совместном с супругом, доходах, задолженности, обязательствах (правах и обязанностях) имущественного характера; • сведения о деловой репутации; • сведения об источниках происхождения денежных средств и (или) иного имущества клиента; • сведения о бенефициарном владельце; • (в случае, если клиент имеет статус лица, указанного в п.п. 1 п. 1 ст. 7.3 Федерального закона № 115-ФЗ) должность клиента, наименование и адрес его работодателя; • степень родства либо статус (супруг или супруга) клиента по		

	отношению к лицу, указанному в п.п. 1 п. 1 ст. 7.3 Федерального закона 115-ФЗ; • номера телефонов и факса (при наличии); • адрес электронной почты; • иная контактная информация (при наличии)		

3.2.3. Описание технологии функционирования и архитектуры системы

Основными составляющими ИС ПДн являются:

- центральный узел обработки данных (сервер с базой данных «1С-Бухгалтерия»);
- автоматизированные рабочие места (АРМ) сотрудников (бухгалтеров).

Центральный узел обработки данных представляет собой сервер с базой данных «1С Бухгалтерия», с установленной операционной системой «*Microsoft Windows Server 2003 R2»*. В качестве антивирусной защиты используется «*Антивирус Касперского 9.1 для Windows Server»*. Всего в рассматриваемой ИС ПДн используется один центральный узел обработки данных, который расположен по адресу: _____.

АРМ сотрудников – основное оборудование, участвующее в обработке ПДн. С помощью этого оборудования осуществляется ввод персональных данных в ИС ПДн. На данных АРМ установлена операционная система «*MS Windows _____»* и средство антивирусной защиты «*Антивирус Касперского 9.1 Windows Workstation _____»*.

3.2.4. Описание механизмов и средств защиты

Регистрация событий: регистрируются такие события, как вход и выход пользователя, изменение документов.

Для аутентификации в системе используются локальные учетные записи.

Средствами ППО настроена и контролируется следующая парольная политика:

- минимальная длина пароля – 6 символов;
- пароль должен содержать как буквы, так и цифры;
- срок действия пароля неограничен;
- независимо от количества неуспешных попыток ввода пароля в систему, блокировка учетной записи не осуществляется.

Обновление антивирусных баз и модулей производится ежедневно. Контроль целостности обновлений и программной части ведется встроенными средствами антивирусного программного обеспечения.

4. Модель угроз безопасности ПДн, обрабатываемых в ИС ПДн «Ведение учета членов и ассоциированных членов кооператива», обрабатываемых в ИС ПДн «Ведение бухгалтерского и кадрового учета»

4.1. Уровень исходной защищённости ИС ПДн

Документом ФСТЭК России «Методика актуализации угроз ПДн» вводится обобщенный показатель уровня исходной защищенности ИС ПДн, зависящий от технических и эксплуатационных характеристик ИС ПДн (коэффициент Y1).

В соответствии с заданными критериями оценки определяется уровень исходной защищенности ИС ПДн.

Технические и эксплуатационные характеристики ИС ПДн		Уровень защищенности
1. По территориальному размещению	локальная ИС ПДн, развернутая в пределах одного здания	Высокий
2. По наличию соединения с сетями общего пользования	ИС ПДн, имеющая одноточечный выход в сеть общего пользования	Средний
3. По встроенным (легальным) операциям с записями баз персональных данных	• чтение, поиск; • запись, удаление, сортировка; • модификация, передача	Низкий
4.По разграничению доступа к персональным данным	ИС ПДн, к которой имеют доступ определенные перечнем сотрудники (работники), члены, ассоциированные члены (их представители) кооператива, являющегося владельцем ИС ПДн, либо субъект ПДн	Средний
5. По наличию соединений с другими базами ПДн иных ИС ПДн	ИС ПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИС ПДн	Высокий
6. По уровню обобщения (обезличивания) ПДн	ИС ПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	Средний
7. По объему ПДн, которые предоставляются сторонним пользователям ИС ПДн без	ИС ПДн, предоставляющая часть ПДн	Средний

предварительной обработки		

По совокупности полученных результатов, уровень исходной защищенности ИС ПДн «Ведение бухгалтерского и кадрового учета» («1С: Бухгалтерия», «1С: Зарплата и кадры») оценивается как средний, поскольку не менее 70% характеристик ИС ПДн (85%) соответствуют уровню «средний» или «высокий».

Согласно «Методики актуализации угроз ПДн» ФСТЭК России коэффициент исходной защищенности ИС ПДн «Ведение бухгалтерского и кадрового учета» («1С: Бухгалтерия», «1С: Зарплата и кадры») Y1=5.

4.2. Описание угроз безопасности ПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИС ПДн в складывающихся условиях обстановки.

Вероятность (Y2) определяется по 4 вербальным градациям этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
- средняя вероятность – объектные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);
- высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей для рассматриваемой ИС ПДн приведена в таблице 3. Притом итоговая оценка реализации определенной угрозы рассчитывается исходя из максимального показателя для какого-либо нарушителя.

Таблица 3

Угрозы 1-го типа			
Класс угроз	Источник Угроз	Нарушаемые свойства ИБ	Вероятность реализации
1. Угроза НСД с применением стандартных функций ОС	Внутренний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая
2. Угроза НСД с применением специально созданных для этого программ	Внутренний нарушитель Внешний	Нарушение конфиденциальности, целостности и доступности	низкая

	нарушитель	ПДн	
3. Угрозы типа «Отказ в обслуживании», в том числе использование известных уязвимостей в ПО	Внешний нарушитель	Нарушение доступности ПДн	низкая
4. Угрозы удаленного запуска приложений, в том числе: - распространение файлов, содержащих несанкционированный исполняемый код; - переполнение буфера приложений серверов; - использование возможностей удаленного управления системой	Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая
Угрозы 2-го типа			
5. Угроза НСД с применением стандартных функций ППО	Внутренний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	средняя
6. Угроза НСД с применением специально созданных для этого программ	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	средняя
7. Угрозы типа «Отказ в обслуживании», в том числе использование известных уязвимостей в ПО	Внешний нарушитель	Нарушение доступности ПДн	низкая
8. Угрозы удаленного запуска приложений	Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая
9. Угроза внедрения вредоносных программ с использованием съемных носителей, а также в связи с подключением стороннего оборудования	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая
Угрозы 3-го типа			
10. Угрозы утечки видовой информации	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности ПДн	низкая
11. Угрозы модификации базовой системы ввода/вывода (BIOS), перехвата управления загрузкой, перехвата или	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая

подбора паролей или идентификаторов			
12. Угроза НСД с применением стандартных функций ОС, СУБД, прикладной программы	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая
13. Угроза НСД с применением специально созданных для этого программ	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая
14. Угроза утечки информации путем преднамеренного копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать неучтенных копий документов с ПДн на принтерах	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности ПДн	средняя
15. Угроза «Анализа сетевого трафика»	Внутренний нарушитель, Внешний нарушитель	Нарушение конфиденциальности ПДн исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей	низкая
16. Угроза сканирования сети	Внешний нарушитель	Нарушение конфиденциальности: определение протоколов, доступных портов сетевых служб, идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей.	низкая
17. Угроза выявления паролей	Внешний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн: выполнение любого действия, связанного с получением НСД	низкая
18. Угроза внедрения по сети вредоносных программ	Внутренний нарушитель	Нарушение конфиденциальности, целостности и доступности ПДн	низкая

Применяемые защитные меры:

1. Используется лицензионное системное ПО надежных производителей.

2. На серверах, функционирующих под управлением ОС «Windows», устанавливаются обновления и патчи для системного ПО, сервисов и служб, которые закрывают известные и новые уязвимости.
3. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
4. Доступ в помещения, где расположены серверы, ограничен и контролируется.
5. Обеспечивается разграничение доступа пользователей к ИС ПДн.
6. Идентификация и аутентификация осуществляется по локальным учетным записям и паролям.
7. Средства отображения информации защищены от визуального просмотра.
8. Пользователи не обладают административными правами на серверах.
9. Пароли в открытом виде в ИС ПДн не хранятся.
10. При осуществлении взаимодействия с сетью Интернет используются средства межсетевого экранирования.
11. Права пользователей ограничены и не распространяются на установку ПО, а также отключение или изменение настроек СЗИ на серверах.

4.3. Определение актуальности угроз безопасности ПДн

По итогам оценки уровня исходной защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы.
Коэффициент реализуемости угрозы рассчитывается по формуле: Y=(Y1+Y2)/20, причем:

- если 0<= Y<= 0.3 , то возможность реализации угрозы признается низкой;
- если 0.3< Y<= 0.6, то возможность реализации угрозы признается средней;
- если 0.6 <Y <=0.8 , то возможность реализации угрозы признается высокой;
- если Y> 0.8, то возможность реализации угрозы признается очень высокой.

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

- низкая опасности – если реализация угрозы может привести к незначительны негативным последствиям для субъектов персональных данных;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИС ПДн представителей членов (ассоциированных членов) СКПК «_____»

существуют следующие актуальные угрозы (таблица 7). Отнесение угрозы к актуальной производится по правилам, приведенным в таблице.

Таблица 7

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Наименование угрозы	**Тип угрозы**	**Актуальность**	
		Вероятность реализации	*Показатель опасности*
1. Угроза НСД с применением стандартных функций ОС	Нарушение конфиденциальности, целостности и доступности ПДн	неактуальная	
		низкая	средняя
2. Угроза НСД с применением специально созданных для этого программ	Нарушение конфиденциальности, целостности и доступности ПДн	неактуальная	
		низкая	низкая
3. Угрозы типа «Отказ в обслуживании», в том числе использование известных уязвимостей в ПО	Нарушение доступности ПДн	неактуальная	
		низкая	низкая
4. Угрозы удаленного запуска приложений	Нарушение конфиденциальности, целостности и доступности ПДн	неактуальная	
		низкая	низкая
5. Угроза НСД с применением стандартных функций ППО	Нарушение конфиденциальности, целостности и доступности ПДн	**актуальная**	
		средняя	средняя
6. Угроза НСД с применением специально созданных для этого программ	Нарушение конфиденциальности, целостности и доступности ПДн	**актуальная**	
		средняя	средняя
7. Угрозы типа «Отказ в обслуживании», в том числе использование известных	Нарушение доступности ПДн	неактуальная	
		низкая	низкая

уязвимостей в ПО			
8. Угрозы удаленного запуска приложений	Нарушение конфиденциальности, целостности и доступности ПДн	неактуальная	
		низкая	низкая
9. Угроза внедрения вредоносных программ с использованием съемных носителей, а также в связи с подключением стороннего оборудования	Нарушение конфиденциальности, целостности и доступности ПДн	**актуальная**	
		низкая	средняя
10. Угрозы утечки видовой информации	Нарушение конфиденциальности ПДн	**актуальная**	
		низкая	средняя
11. Угрозы модификации базовой системы ввода/вывода (BIOS), перехвата управления загрузкой, перехвата или подбора паролей или идентификаторов	Нарушение конфиденциальности, целостности и доступности ПДн	низкая	средняя
12. Угроза НСД с применением стандартных функций ОС, СУБД, прикладной программы	Нарушение конфиденциальности, целостности и доступности ПДн	**актуальная**	
		низкая	средняя
13. Угроза НСД с применением специально созданных для этого программ	Нарушение конфиденциальности, целостности и доступности ПДн	**актуальная**	
		низкая	средняя
14. Угроза утечки информации путем преднамеренного копирования доступных ПДн на неучтенные (в том числе отчуждаемые) носители, а также печать неучтенных копий документов с ПДн на принтерах	Нарушение конфиденциальности ПДн	**актуальная**	
		средняя	средняя
15. Угроза «Анализа сетевого трафика»	Нарушение конфиденциальности ПДн: исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей	**актуальная**	
		низкая	низкая
16. Угроза сканирования сети	Нарушение конфиденциальности: определение протоколов, доступных портов сетевых служб, идентификаторов	**актуальная**	
		низкая	средняя

	соединений, активных сетевых сервисов, идентификаторов и паролей пользователей.		
17. Угроза выявления паролей	Нарушение конфиденциальности, целостности и доступности ПДн: выполнение любого действия, связанного с получением НСД	**актуальная**	
		низкая	средняя
18. Угроза внедрения по сети вредоносных программ	Нарушение конфиденциальности, целостности и доступности ПДн	**актуальная**	
		низкая	средняя

Методические материалы и формы (бланки) документов *не содержат* правовых норм или общеобязательных правил, конкретизирующих нормативные предписания, и не являются нормативным правовым актом. Мнение Центра развития кооперативов имеет *информационно-разъяснительный* характер по вопросам применения законодательства Российской Федерации и не препятствует руководствоваться нормами законодательства в понимании, отличающемся от толкования, изложенного в настоящем методическом материале.