ОБЛАСТНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР КОМПЕТЕНЦИЙ АПК ЛИПЕЦКОЙ ОБЛАСТИ»
(ОБУ «ЦЕНТР КОМПЕТЕНЦИЙ АПК ЛИПЕЦКОЙ ОБЛАСТИ»)

П Р И К А З

«05» июня 2019 г. № 7 -од

г. Липецк

О мерах по защите персональных данных

В соответствии с требованиями Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» и главы 14 Трудового кодекса Российской Федерации, в целях обеспечения безопасности персональных данных, обработка которых осуществляется в ОБУ «Центр компетенций АПК Липецкой области» (далее – учреждение), приказываю:

1. Утвердить «Положение об обработке и защите персональных данных в областном бюджетном учреждении «Центр компетенций АПК Липецкой области» (приложение 1), которое ввести в действие с 01.07.2019 г.

2. Утвердить «Положение о защите персональных данных в информационных системах персональных данных, используемых в областном бюджетном учреждении «Центр компетенций АПК Липецкой области» (приложение 2), которое ввести в действие с 01.07.2019 г.

3. Утвердить «Инструкцию ответственного за организацию обработки персональных данных» (приложение 3).

4. Возложить на главного специалиста отдела информатизации и технического обеспечения учреждения Чурсину Е.В. обязанности и ответственность за организацию обработки персональных данных в учреждении, в том числе обязанности:

осуществлять внутренний контроль за соблюдением всеми работниками законодательства Российской Федерации о персональных данных, требований Положения, утверждённого настоящим приказом, включая требований к защите персональных данных, а также контроль за обеспечением надлежащего хранения дел, документов и иных носителей, содержащих персональные данные;

доводить до сведения работников учреждения 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.

5. Возложить на начальника отдела информатизации и технического обеспечения учреждения Тарана П.В. обязанности и ответственность за обеспечение технической защиты персональных данных, обработка которых осуществляется с использованием аттестованных автоматизированных рабочих мест, а также в создаваемых и функционирующих в учреждении информационных системах.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.И. Явных

Визы:
Е.В. Чурсина
П.В. Таран
А.Н. Королёв

Приложение 1
к приказу ОБУ «Центр компетенций
АПК Липецкой области»
от «05» июня 2019 г. № 7-ОД

ПОЛОЖЕНИЕ

об обработке и защите персональных данных в областном бюджетном учреждении «Центр компетенций АПК Липецкой области»

I. Общие положения

1.1. Настоящее Положение определяет политику областного бюджетного учреждения «Центр компетенций АПК Липецкой области» (далее -Оператор или учреждение соответственно) в сфере обработки и защиты персональных данных, а также цели, содержание и правила их обработки, меры и процедуры по обеспечению защиты от несанкционированного доступа, выявлению и предотвращению нарушений законодательства Российской Федерации о защите персональных данных и устранению последствий таких нарушений (далее - Положение).

1.2. Основанием для разработки настоящего Положения являются Конституция Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», другие федеральные законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения в сфере обработки и защиты персональных данных.

1.3. Обработка Оператором персональных данных осуществляется:

с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;

с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», настоящим Положением, в целях: обеспечения прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, обеспечения исполнения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по работе, обеспечения личной безопасности работников, контроля количества и

качества выполняемой ими работы и обеспечения сохранности имущества, предоставления информационных и консультационных услуг гражданам и юридическим лицам, относящимся к сельхозтоваропроизводителям Липецкой области, а также иным гражданам, выражающим намерение осуществлять деятельность в сфере сельского хозяйства.

1.4. Обработка Оператором персональных данных основывается на следующих основных принципах:

законности целей и способов обработки персональных данных, добросовестности и справедливости в деятельности Оператора;

достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

обработки только персональных данных, которые отвечают целям их обработки;

соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой;

обеспечения точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных;

хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

II. Порядок и условия обработки персональных данных

2.1. До начала обработки персональных данных Оператор приказом учреждения назначает ответственного (ответственных) за организацию обработки и защиты персональных данных, утверждает перечень лиц, имеющих доступ к персональным данным соответствующей категории, в соответствии с ч. 3 ст. 22 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Липецкой области направляет уведомление об обработке (намерении осуществлять обработку) персональных данных.

2.2. Работники Оператора, непосредственно осуществляющие обработку персональных данных, до начала работы и получения допуска к персональным данным должны быть ознакомлены под подпись с положениями законодательства Российской Федерации о персональных

данных, в том числе с настоящим Положением и другими локальными актами учреждения по вопросам обработки персональных данных.

2.3. При обработке персональных данных Оператор применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

2.4. Контроль за соблюдением работниками Оператора требований законодательства Российской Федерации и положений локальных актов Оператора осуществляется в соответствии с Положением о внутреннем контроле Оператора при обработке персональных данных, который заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

2.5. Аудит соблюдения Оператором требований законодательства Российской Федерации и положений локальных нормативных актов Оператора осуществляется в соответствии с Положением Оператора об аудите при обработке персональных данных.

2.6. Опубликование или обеспечение иным образом неограниченного доступа к настоящему Положению, иным документам, определяющим политику Оператора в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных осуществляются в соответствии с Положением Оператора о раскрытии информации.

2.7. При осуществлении сбора персональных данных с использованием информационно-телекоммуникационных сетей Оператор до начала обработки персональных данных обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

2.8. Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в том числе в случае реализации Оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

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

5) обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

6) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», при условии обязательного обезличивания персональных данных;

7) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

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

2.9. Оператор и его работники, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и по достижении целей обработки или в случае утраты необходимости в их достижении они подлежат уничтожению в порядке, предусмотренном Положением о хранении персональных данных у Оператора.

2.11. Взаимодействие с федеральными органами исполнительной власти, исполнительными органами государственной власти и органами местного самоуправления Липецкой области по вопросам обработки и защиты персональных данных субъектов, персональные данные которых обрабатываются Оператором, осуществляется в рамках законодательства Российской Федерации.

2.12. Персональные данные работников Оператора, а также граждан, претендующих на заключение трудового договора и трудоустройство в учреждение, подлежащие обработке и защите в соответствии с настоящим Положением, могут включать следующие сведения:

фамилию, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);

число, месяц, год рождения;

место рождения;

информацию о гражданстве (в том числе предыдущие гражданства, иные гражданства);

вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

адрес места жительства (адрес регистрации, фактического проживания);

номер контактного телефона или сведения о других способах связи;

реквизиты страхового свидетельства государственного пенсионного страхования;

идентификационный номер налогоплательщика;

реквизиты страхового медицинского полиса обязательного медицинского страхования;

реквизиты свидетельства государственной регистрации актов гражданского состояния;

семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);

сведения о трудовой деятельности;

сведения о воинском учете и реквизиты документов воинского учета;

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

сведения об ученой степени;

информацию о владении иностранными языками, степень владения;

медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на государственную гражданскую службу или ее прохождению;

сведения о месте прохождении государственной или муниципальной службы, в том числе дате, основании поступления на государственную или муниципальную службу, наименовании последней замещаемой должности, времени и основании увольнения с государственной или муниципальной службы (в отношении бывших государственных или муниципальных служащих, поступающих на работу в учреждение);

информация о наличии или отсутствии судимости;

информация об оформленных допусках к государственной тайне;

государственные награды, иные награды и знаки отличия;

сведения о профессиональной переподготовке и (или) повышении квалификации;

информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

сведения о доходах, об имуществе и обязательствах имущественного характера;

номер лицевого счета;

номер банковской карты;

фотографию;

2.13. иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 2.12. настоящего Положения.

2.14. Обработка персональных данных и биометрических персональных данных работников учреждения и граждан, претендующих на поступление на работу в учреждение, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 1.3. настоящего Положения, в соответствии с пунктом 2 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных», Федерального закона «О противодействии коррупции», Трудового кодекса Российской Федерации.

2.15. Обработка специальных категорий персональных данных работников учреждения и граждан, претендующих на поступление на работу в учреждение, осуществляется без согласия указанных лиц в рамках целей, определенных пунктом 1.3. настоящего Положения, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации.

2.16. Обработка персональных данных работников учреждения и граждан, претендующих работу в учреждении, осуществляется при условии получения согласия указанных лиц в следующих случаях:

1) при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации о государственной гражданской службе;

2) при трансграничной передаче персональных данных;

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

2.17. В случаях, предусмотренных пунктом 2.16. настоящего Положения, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

2.18. Обработка персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.19. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных работников учреждения, граждан, претендующих на работу в учреждении, лиц, обратившихся в учреждение за получением услуг, в том числе персональных данных субъектов МСП, содержащихся в информационных системах (базах данных, реестрах и др.), создаваемых в учреждении, осуществляется путем:

1) получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые работнику кадров учреждения);

2) копирования оригиналов документов;

3) внесения сведений в учетные формы (на бумажных и электронных носителях);

4) формирования персональных данных в ходе кадровой работы;

5) внесения персональных данных в информационную систему, используемую работником кадров учреждения.

2.20. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от работников учреждения, граждан, претендующих на работу в учреждении, а также лиц, обратившихся в учреждение за получением услуг.

2.21. В случае возникновения необходимости получения персональных данных работников учреждения и лиц, претендующих на работу в учреждение, у третьей стороны, следует известить об этом работника учреждения заранее, получить их письменное согласие и сообщить им о целях, предполагаемых источниках и способах получения персональных данных.

2.22. Запрещается получать, обрабатывать и приобщать к личному делу работника учреждения персональные данные, не предусмотренные пунктом 2.12 настоящего Положения, в том числе касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

2.23. При сборе персональных данных работник кадров учреждения, осуществляющий сбор (получение) персональных данных непосредственно от работников учреждения, граждан, претендующих на работу в учреждении, обязан разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

2.24. Передача (распространение, предоставление) и использование персональных данных работников учреждения, граждан, претендующих на работу в учреждении, а также лиц, обратившихся в учреждение за получением услуг, осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

III. Условия и порядок обработки персональных данных субъектов малого и среднего предпринимательства в сфере сельского хозяйства в связи с их обращением в учреждение за оказанием услуг

3.1. Обработка Оператором персональных данных физических лиц, относящихся к субъектам малого и среднего предпринимательства в сфере сельского хозяйства (далее – субъекты МСП), осуществляется в целях предоставления указанным субъектам следующих услуг, предусмотренных «Стандартом деятельности центров компетенций в сфере сельскохозяйственной кооперации и поддержки фермеров», утверждённым проектным комитетом по национальному проекту «Малый бизнес и поддержка индивидуальной предпринимательской инициативы (протокол от 21 марта 2019 г. № 1):

1) организация приема граждан, обеспечение своевременного и в полном объеме рассмотрения устных и письменных обращений граждан по вопросам, относящимся к компетенции Оператора;

2) организация обучения граждан, ведущих личные подсобные хозяйства (далее ЛПХ), руководителей, членов и участников крестьянско-фермерских хозяйств (далее – КФХ), сельскохозяйственных производственных и потребительских кооперативов (далее – СПК и СПоК соответственно), сельского населения основам законодательства и основам ведения предпринимательской деятельности в сфере сельскохозяйственного производства;

3) оказание услуг в области финансовой и производственной деятельности, в том числе:

организация взаимодействия с финансовыми организациями с целью содействия субъектам МСП и СХК в подготовке документации, необходимой для последующего направления в кредитные и лизинговые организации с целью получения заемного финансирования, в том числе с применением механизма льготного кредитования сельскохозяйственных товаропроизводителей, реализуемого Минсельхозом России, Минэкономразвития России, продуктов АО "Корпорация "МСП" и ее дочерних обществ;

4) по вопросам финансового планирования (бюджетирование, налогообложение, бухгалтерские услуги), в том числе:

сопровождение КФХ и СПоК, получивших государственную поддержку в рамках направлений, реализуемых Минсельхозом России, в части формирования необходимого пакета отчетных документов;

содействие субъектам МСП и СХК в подборе сельскохозяйственной техники и оборудования для осуществления ими эффективной деятельности, внедрения инновационных технологий в сельском хозяйстве;

содействие в подборе квалифицированных кадров, проведение консультаций по вопросам применения трудового законодательства Российской Федерации (в том числе по оформлению необходимых документов для приема на работу, разрешений на право привлечения иностранной рабочей силы и др.);

5) оказание услуг по планированию деятельности, в том числе:

содействие в организации предпринимательской деятельности в сельском хозяйстве для физических лиц;

проведение консультаций с субъектами МСП и СХК по вопросам приобретения прав на земельные участки из земель сельскохозяйственного назначения и их оформления в собственность и/или аренду;

6) оказание услуг по подготовке и оформлению документов:

необходимых для регистрации, реорганизации и ликвидации предпринимательской деятельности в органах Федеральной налоговой службы; для участия субъектов МСП и СХК в программах государственной поддержки, реализуемых на муниципальном, региональном и федеральном уровнях, мероприятиях федерального проекта (включая разработку бизнес-

плана, составление финансово-экономического обоснования планируемого к реализации проекта, оказание содействия в подготовке проектно-сметной и разрешительной документации); для получения патентов и лицензий, необходимых для ведения деятельности субъектов МСП и СХК (формирование патентно-лицензионной политики, патентование, разработка лицензионных договоров, определение цены лицензий и др.);

разработка и распространение типовой документации, в том числе учредительных документов для организации и развития предпринимательской деятельности в области сельского хозяйства всех видов и форм собственности; методической литературы и периодических изданий по вопросам организации предпринимательской деятельности в области сельского хозяйства;

7) оказание юридических услуг, в том числе:

правовое обеспечение деятельности субъектов МСП и СХК (составление и юридическая экспертиза договоров, соглашений, учредительных документов, должностных регламентов и инструкций, обеспечение представительства в судах общей юрисдикции, арбитражном и третейском судах, составление направляемых в суд документов (исков, отзывов и иных процессуальных документов);

обеспечение представления интересов субъекта МСП в органах государственной власти и органах местного самоуправления при проведении мероприятий по контролю и др.);

8) оказание услуг в области маркетинга, продвижения и сбыта сельскохозяйственной продукции, в том числе:

содействие сельскохозяйственным потребительским кооперативам в размещении мобильных торговых объектов;

привлечение к участию субъектов МСП в выставочно-ярмарочных и конгрессных мероприятиях, бизнес-миссиях, других мероприятиях;

организация деловых контактов с представителями регионального бизнес-сообщества с целью выстраивания партнерских взаимоотношений с субъектами МСП и СХК;

содействие в разработке маркетинговой стратегии и планов, рекламной кампании, дизайна, разработке и продвижении бренда, организация системы сбыта продукции, в том числе с использованием Портала Бизнес-навигатора МСП АО "Корпорация "МСП";

содействие в регистрации учетной записи (аккаунта) субъекта МСП, СХК на торговых площадках, в том числе организованных для закупки товаров и услуг для государственных и муниципальных нужд, а также продвижении продукции субъекта МСП на торговой площадке;

содействие организации поставок сельскохозяйственной продукции на экспорт;

формирование и ведение базы данных о зарегистрированных на территории Липецкой области сельскохозяйственных потребительских кооперативах, реестра действующих на территории Липецкой области субъектов МСП с СХК, в том числе являющихся получателями

государственной поддержки, показателей их финансовой, производственной и хозяйственной деятельности.

Оператором предоставляются иные услуги субъектам МСП и СХК в соответствии с законодательством Российской Федерации.

3.2. Персональные данные граждан, обратившихся в учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

3.3. В рамках рассмотрения обращений граждан подлежат обработке следующие персональные данные заявителей:

фамилия, имя, отчество (последнее при наличии);

почтовый адрес;

адрес электронной почты;

указанный в обращении контактный телефон;

иные персональные данные, указанные заявителем в обращении (жалобе), а также ставшие известными в ходе личного приема или в процессе рассмотрения поступившего обращения.

3.4. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов, обратившихся в учреждение для получения услуг, осуществляется путем:

получения оригиналов необходимых документов (заявлений);

заверения копий документов;

внесения сведений в учетные формы (на бумажных и электронных носителях);

внесения персональных данных в прикладные программные подсистемы учреждения.

3.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путем получения персональных данных непосредственно от субъектов персональных данных (заявителей).

3.6. При предоставлении услуг Оператору запрещается запрашивать у субъектов персональных данных и третьих лиц, а также обрабатывать персональные данные в случаях, не предусмотренных законодательством Российской Федерации.

3.7. При сборе персональных данных уполномоченное должностное лицо Оператора, осуществляющее получение персональных данных непосредственно от субъектов персональных данных, обратившихся за предоставлением услуг, обязано разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить персональные данные.

3.8. Передача (распространение, предоставление) и использование персональных данных заявителей (субъектов персональных данных) Оператором осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

IV. Порядок обработки персональных данных субъектов персональных данных в информационных системах

4.1. Обработка персональных данных в учреждении осуществляется на аттестованных под обработку персональных данных автоматизированных рабочих местах в следующих информационных системах:

1) Единая информационная система Липецкой области по бюджетному (бухгалтерскому) учёту и отчётности («1С: Предприятие 8»);

2) Система электронного документооборота администрации Липецкой области (СЭД-Дело Web);

3) База данных о зарегистрированных на территории Липецкой области сельскохозяйственных потребительских кооперативах;

4) Реестр действующих на территории Липецкой области субъектов МСП и СХК, в том числе являющихся получателями государственной поддержки, показателей их финансовой и производственной деятельности.

4.2. Информационные системы, указанные в п.4.1. настоящего Положения, содержат персональные данные работников учреждения, лиц, претендующих на поступление на работу в учреждение, а также граждан (заявителей), обратившихся в целях получения услуг и включают:

1) персональный идентификатор;

2) фамилию, имя, отчество субъекта персональных данных;

3) вид документа, удостоверяющего личность субъекта персональных данных;

4) серию и номер документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

почтовый адрес субъекта персональных данных;

контактный телефон, факс (при наличии) субъекта персональных данных;

адрес электронной почты субъекта персональных данных;

ИНН субъекта персональных данных.

4.3. Информационная система «1С: Предприятие 8» и прикладные программные подсистемы «АКСИОК» и «1С Бухгалтерия», содержат персональные данные работников учреждения и физических лиц, являющихся сторонами гражданско-правовых договоров, и включает:

фамилию, имя, отчество субъекта персональных данных;

дату рождения субъекта персональных данных;

место рождения субъекта персональных данных;

серию и номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

почтовый адрес субъекта персональных данных;

телефон субъекта персональных данных;

ИНН субъекта персональных данных;

табельный номер субъекта персональных данных;

должность субъекта персональных данных;

номер приказа и дату приема на работу (увольнения) субъекта персональных данных.

4.4. Автоматизированное рабочее место работника учреждения, на которого возложены функции кадровой работы, предполагает обработку персональных данных работников учреждения, предусмотренных пунктом 2.12. настоящего Положения.

4.5. Работникам учреждения, имеющим право осуществлять обработку персональных данных в информационных системах, перечисленных в п. 4.1. настоящего Положения, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями работников.

4.6. Информация может вноситься как в автоматическом режиме, при получении персональных данных с Единого портала государственных услуг или официального сайта учреждения, так и в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

4.7. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах, перечисленных в п. 4.1. настоящего Положения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:

1) определение угроз безопасности персональных данных при их обработке в информационных системах;

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

3) применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

7) восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных учреждения, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.

4.8. Структурное подразделение учреждения, на которого возложена обязанность и ответственность за обеспечение информационной безопасности в учреждении, организует и контролирует ведение учета материальных носителей персональных данных.

4.9. Уполномоченное должностное лицо учреждения, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных, должно обеспечивать:

1) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных и руководителя учреждения;

2) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

3) возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4) постоянный контроль за обеспечением уровня защищенности персональных данных;

5) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

6) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

7) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

8) разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.10. Структурное подразделение учреждения, ответственное за обеспечение функционирования информационных систем персональных данных, принимает все необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.

4.11. Обмен персональными данными при их обработке в информационных системах персональных данных учреждения

осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

4.12. Доступ работников учреждения к персональным данным, находящимся в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

4.13. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных уполномоченное должностное лицо учреждения незамедлительно принимает меры по установлению причин нарушений и их устранению.

V. Обработка персональных данных в рамках межведомственного информационного взаимодействия с применением единой системы межведомственного электронного взаимодействия

5.1. Оператор в соответствии с законодательством Российской Федерации осуществляет обработку персональных данных в рамках межведомственного электронного информационного взаимодействия в электронном виде с территориальными федеральными органами государственной власти, федеральными внебюджетными фондами, исполнительными органами государственной власти, органами местного самоуправления и государственными учреждениями Липецкой области с применением единой системы межведомственного электронного взаимодействия (далее - СМЭВ).

5.2. Оператор в рамках СМЭВ на основании поступивших межведомственных запросов направляет информацию, включающую персональные данные субъектов, обрабатываемые в учреждении, в следующие федеральные органы и учреждения:

1) Министерство сельского хозяйства Российской Федерации;

2) управление Федерального казначейства по Липецкой области;

3) территориальные органы управления Федеральной налоговой службы Российской Федерации по Липецкой области;

4) управление Роскомнадзора по Липецкой области;

5) управление Федеральной службы государственной статистики по Липецкой области;

6) ГУ- Отделение Пенсионного фонда Российской Федерации по Липецкой области»;

7) ГУ-Региональное отделение Фонда социального страхования Российской Федерации по Липецкой области;

8) ФКУ «Военный комиссариат Липецкой области;

9) АО «Корпорация МСП»;

VI. Сроки обработки и хранения персональных данных

6.1. Сроки обработки и хранения персональных данных работников учреждения, граждан, претендующих на поступление на работу в учреждение, лиц, определяются в соответствии с законодательством Российской Федерации. С учетом положений законодательства Российской Федерации, устанавливаются следующие сроки обработки и хранения персональных данных государственных служащих:

1) персональные данные, содержащиеся в приказах по личному составу работников учреждения (о приеме, о переводе, об увольнении, об установлении надбавок и других выплат), подлежат хранению в кадровом подразделении учреждения в течение двух лет, с последующим формированием и передачей указанных документов в государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течении 75 лет.

2) персональные данные, содержащиеся в личных делах и личных карточках работников учреждения, хранятся в кадровом подразделении учреждения в течение десяти лет, с последующим формированием и передачей указанных документов в государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течении 75 лет.

3) персональные данные, содержащиеся в приказах о поощрениях, материальной помощи работников учреждения, подлежат хранению в течение двух лет в кадровом подразделении учреждения с последующим формированием и передачей указанных документов в государственный архив в порядке, предусмотренном законодательством Российской Федерации, где хранятся в течении 75 лет.

4) персональные данные, содержащиеся в приказах о предоставлении отпусков, о краткосрочных внутрироссийских и зарубежных командировках, о дисциплинарных взысканиях, налагаемых на работников учреждения, подлежат хранению в кадровом подразделении учреждения в течение пяти лет с последующим уничтожением.

5) персональные данные, содержащиеся в документах претендентов на занятие вакантных должностей в учреждении, хранятся в кадровом подразделении в течении 3 лет со дня их поступления, после чего подлежат уничтожению.

6.2. Сроки обработки и хранения персональных данных, предоставляемых субъектами персональных данных в связи с получением представляемых учреждением услуг, указанных в пункте 3.1 настоящего Положения, определяются нормативными правовыми актами, регламентирующими порядок их сбора и обработки.

6.3. Персональные данные граждан, обратившихся в учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, хранятся в учреждении в течении пяти лет.

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

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

6.6. Контроль за хранением и использованием материальных носителей персональных данных, не допускающий несанкционированное использование, уточнение, распространение и уничтожение персональных данных, находящихся на этих носителях, осуществляется начальниками соответствующих отделов учреждения.

6.7. Срок хранения персональных данных, внесенных в информационные системы персональных данных учреждения, указанные в пункте 4.1 настоящего Положения, должен соответствовать сроку хранения бумажных оригиналов.

VII. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

7.1. Структурным подразделением учреждения, ответственным за документооборот и архивирование, осуществляется систематический контроль и выделение документов, содержащих персональные данные, с истекшими сроками хранения, подлежащих уничтожению.

7.2. Вопрос об уничтожении выделенных документов, содержащих персональные данные, рассматривается на заседании экспертной комиссии, состав которой утверждается приказом учреждения.

По итогам заседания составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел, проверяется их комплектность, акт подписывается председателем и членами экспертной комиссии и утверждается директором учреждения.

7.3. Оператором в порядке, установленном законодательством Российской Федерации, определяется подрядная организация, имеющая необходимую производственную базу для обеспечения установленного порядка уничтожения документов. Должностное лицо учреждения, ответственное за архивную деятельность, сопровождает документы, содержащие персональные данные, до производственной базы подрядчика и присутствует при процедуре уничтожения документов (сжигание или другой способ уничтожения).

7.4. По окончании процедуры уничтожения подрядчиком и должностным лицом учреждения, ответственным за архивную деятельность, составляется соответствующий акт об уничтожении документов, содержащих персональные данные.

7.5. Уничтожение по окончании срока обработки персональных данных на электронных носителях производится путем механического нарушения целостности носителя, не позволяющего произвести считывание или восстановление персональных данных, или удалением с электронных носителей методами и средствами гарантированного удаления остаточной информации.

VIII. Рассмотрение запросов субъектов персональных данных или их представителей

8.1. Граждане, и другие субъекты персональных данных из числа сельхозтоваропроизводителей, обратившиеся с заявлением о предоставлении государственной поддержки, а также работники учреждения, в отношении которых осуществляется обработка персональные, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных в учреждении;

2) правовые основания и цели обработки персональных данных;

3)применяемые в учреждении способы обработки персональных данных;

4) наименование и место нахождения учреждения, сведения о лицах (за исключение работников учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с учреждением или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения в учреждении;

7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством Российской Федерации в области персональных данных;

8) информацию об осуществленной или предполагаемой трансграничной передаче данных;

9) наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных.

10) иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

8.2. Лица, указанные в пункте 8.1 настоящего Положения (далее - субъекты персональных данных), вправе требовать от Оператора уточнения их 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.

8.3. Сведения, указанные в подпунктах 1 - 10 пункта 8.1 настоящего Положения, должны быть Оператором предоставлены субъекту персональных данных 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.

8.4. Сведения, указанные в подпунктах 1 - 10 пункта 8.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом структурного подразделения учреждения, осуществляющего обработку соответствующих персональных данных при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

2) сведения, подтверждающие участие субъекта персональных данных в правоотношениях с Оператором, либо сведения, иным образом подтверждающие факт обработки персональных данных в учреждении, 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.

8.5. В случае, если сведения, указанные в подпунктах 1 - 10 пункта 8.1 настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8.6. Субъект персональных данных вправе обратиться повторно к Оператору или направить повторный запрос в целях получения сведений, указанных в подпунктах 1 - 10 пункта 8.1 настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 8.5 настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 9.4 настоящего Положения, должен содержать обоснование направления повторного запроса.

8.7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям,

предусмотренным пунктами 8.5 и 8.6 настоящего Положения. Такой отказ должен быть мотивированным.

8.8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

IX. Лицо, ответственное за организацию обработки персональных данных в учреждении

9.1. Должностное лицо учреждения, ответственное за организацию обработки персональных данных назначается приказом учреждения из числа руководителей структурных подразделений или иных работников в соответствии с распределением обязанностей.

9.2. Ответственный за обработку персональных данных в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Положением.

9.3. Ответственный за обработку персональных данных обязан:

1) обеспечивать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в учреждении 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) обеспечить осуществление внутреннего контроля за соблюдением работниками учреждения требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

3) доводить до сведения работников учреждения положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

4) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в учреждении;

5) в случае нарушения работниками учреждения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

9.4. Ответственный за обработку персональных данных вправе иметь доступ к информации, касающейся обработки персональных данных в учреждении и включающей:

1) цели обработки персональных данных;
категории обрабатываемых персональных данных;

2) категории субъектов, персональные данные которых обрабатываются;
правовые основания обработки персональных данных;

3) перечень действий с персональными данными, общее описание используемых в учреждении способов обработки персональных данных;

4) описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

5) дату начала обработки персональных данных;

6) срок или условия прекращения обработки персональных данных;

7) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

8) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

9) привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в учреждении, иных работников с возложением на них соответствующих обязанностей и закреплением ответственности.

9.5. Ответственный за обработку персональных данных в учреждении несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных и их защиту от несанкционированного доступа в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Приложение 2

к приказу ОБУ «Центр компетенций
АПК Липецкой области»
от «05» июня 2019 года №7-ОД
«О мерах по защите персональных
данных»

Положение о защите персональных данных в информационных системах персональных данных, используемых в областном бюджетном учреждении «Центр компетенций АПК Липецкой области»

1. Общие положения

1.1.Положение о защите персональных данных в информационных системах персональных данных (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах на протяжении всего цикла их эксплуатации в областном бюджетном учреждении «Центр компетенций АПК Липецкой области» (далее – учреждение).

Меры по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн), принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, обрабатываемых в ИС.

Меры по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, реализуются в рамках системы защиты в соответствии с требованиями к защите информации, установленными нормативно-правовыми актами, приведенными в п. 2 настоящего Положения, и направлены на нейтрализацию актуальных угроз безопасности персональных данных, обрабатываемых в ИСПДн.

1.2.Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий защиты ПДн, обрабатываемых в ИСПДн .

2. Нормативные ссылки

Положение разработано с учетом требований следующих нормативных правовых актов:

- Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной Обработке персональных данных»;
- Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.Выбор мер по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн

В соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» базовый набор мер, необходимых для обеспечения 4-го уровня защищенности, включает в себя меры, приведенные в таблице 1 настоящего Положения.

Таблица 1.

Условное обозначение меры	Содержание мер защиты информации
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	

Условное обозначение меры	Содержание мер защиты информации
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
II. Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях

Условное обозначение меры	Содержание мер защиты информации
	безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности
VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XII. Защита технических средств (ЗТС)	
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

Проведена адаптация базового набора мер с учетом структурно-функциональных характеристик ИСПДн, информационных технологий и особенностей функционирования информационной системы. Из базового набора мер исключены следующие меры, приведенные в таблице 2.

Таблица 2.

Условное обозначение меры	Содержание мер защиты информации	Причина исключения из базового набора мер
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В ИС нет внешних пользователей
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Удаленный доступ через внешние информационно-телекоммуникационные сети не осуществляется
УПД.14	Регламентация и контроль использования в информационной	Технологии беспроводного доступа не используются

Условное обозначение меры	Содержание мер защиты информации	Причина исключения из базового набора мер
	системе технологий беспроводного доступа	
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Мобильные технические средства не используются

Для нейтрализации всех актуальных угроз безопасности ИС проведено уточнение полученного набора мер путем его дополнения с учетом не выбранных ранее мер.

С целью снижения риска неработоспособности технических средств и программных средств обработки информации использованы меры ОДТ.3, ОДТ.4, ОДТ.5.

Более подробное описание выбранных мер по защите информации, обрабатываемой в ИС, а также способ их реализации приведены в таблице 4.

Знаком «+» обозначены меры по обеспечению безопасности персональных данных, которые включены в базовый набор мер для 4-го уровня защищенности.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», были добавлены при уточнении адаптированного базового набора мер.

Таблица 3.

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	СЗИ от НСД
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	СЗИ от НСД
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	Применение организационно-технических мер
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	СЗИ от НСД
II. Управление доступом субъектов доступа к объектам доступа (УПД)			

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	СЗИ от НСД
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	СЗИ от НСД
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	СКЗИ
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	СЗИ от НСД
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	СЗИ от НСД
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	СЗИ от НСД
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).	+	СЗИ от НСД СКЗИ
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	СЗИ от НСД
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	СЗИ от НСД

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	СЗИ от НСД
РСБ. 7	Защита информации о событиях безопасности	+	СЗИ от НСД
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	+	Антивирус
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	Антивирус
VIII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	Применение организационных мер
X. Обеспечение доступности персональных данных (ОДТ)			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование		Применение организационных мер
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных		Применение организационных мер
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала		Применение организационных мер
XII. Защита технических средств (ЗТС)			
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам	+	Применение организационно-технических мер

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровень защищенности ПДн	Способ реализации мер защиты информации
		4	
	обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены		
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	Применение организационных мер
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	СКЗИ

3. Реализация мер по обеспечению безопасности персональных данных в ИСПДн «АСП»

3.1. Для реализации технических мер по обеспечению безопасности персональных данных в ИСПДн необходимо осуществить выбор, установку и настройку средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, в соответствии с установленным уровнем защищенности персональных данных и с учетом типа актуальных угроз.

3.2. Организационные меры по обеспечению безопасности персональных данных в ИСПДн необходимо реализовать путем утверждения инструкций, регламентирующих функции, задачи и обязанности ответственных лиц и иных пользователей, инструкций, определяющих правила и процедуры управления системой защиты информации информационной системы, выявления инцидентов безопасности обработки персональных данных, осуществления резервного копирования информации, содержащей персональные данные, а также определения правил разграничения доступа субъектов доступа к объектам доступа.

3.3. Для контроля за соблюдением мер по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, необходимо разработать документы, определяющие правила и процедуры проведения внутреннего

контроля (анализа) защищенности персональных данных, в том числе контроля за обеспечением уровня защищенности персональных данных, содержащихся в ИСПДн.

Приложение 3
к приказу ОБУ «Центр компетенций
АПК Липецкой области»
от «05» июня 2019 года № 7-ОР
«О мерах по защите персональных
данных»

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных в областном бюджетном учреждении «Центр компетенций АПК Липецкой области» (далее – ответственный и учреждение соответственно) назначается приказом директора учреждения.

1.2. Настоящая инструкция определяет основные задачи, обязанности и права Ответственного за организацию обработку персональных данных.

1.3. В своей деятельности ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам обработки и защиты персональных данных и обеспечивает их выполнение.

2. Задачи Ответственного

Основными задачами ответственного являются:

– разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты персональных данных;

– определение перечня работников учреждения, допущенных к работе с персональными данными;

– доведение до сведения работников учреждения, допущенных к работе с персональными данными, положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– осуществление внутреннего контроля за соблюдением учреждением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов;

– заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) персональных данных в уполномоченный орган по защите прав субъектов персональных данных.

3. Обязанности Ответственного

1.4. Для реализации поставленных задач ответственный обязан:

1.4.1. Руководствоваться положениями законодательства Российской Федерации о персональных данных, а также локальными актами по вопросам обработки и защиты персональных данных.

1.4.2. Информировать работников, допущенных к работе с персональными данными, о политике информационной безопасности в учреждении и степени ответственности при работе с персональными данными.

1.4.3. Контролировать наличие подписей всех работников, допущенных к работе с персональными данными, об ознакомлении с организационно-распорядительными документами по обработке и защите персональных данных.

1.4.4. Осуществлять контроль за процессами обработки персональных данных работниками, допущенными к обработке персональных данных.

1.4.5. Осуществлять контроль взаимодействия с субъектами персональных данных уполномоченных сотрудников с использованием утвержденных типовых форм.

1.4.6. Соблюдать или контролировать соблюдение единого и обязательного порядка приема и рассмотрения обращений и запросов субъектов персональных данных (или их законных представителей) в части реализации прав субъекта, определенных в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных», и принятия мер по данным обращениям и запросам.

1.4.7. Осуществлять контроль соблюдения сотрудниками и иными лицами порядка доступа в помещения учреждения, в которых осуществляется обработка персональных данных.

1.4.8. С периодичностью, установленной в Правилах осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в учреждении, обеспечивать:

– контроль выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», и соблюдения прав субъектов персональных данных;

– 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»;

– контроль наличия и актуальности внутренней нормативной документации по обработке и защите персональных данных.

1.4.9. Требовать прекращения обработки персональных данных, как в целом, так и для отдельных лиц, в случае выявления нарушений установленного режима обработки или обеспечения безопасности персональных данных.

1.4.10. Участвовать в проведении внутреннего расследования по фактам разглашения персональных данных, нарушения требований обеспечения

информационной безопасности, несанкционированного доступа, утраты, порчи персональных данных и технических компонентов информационной системы.

4. Права Ответственного

1.5. Ответственный имеет право:

1.5.1. Требовать от работников учреждения, допущенных к работе с персональными данными, выполнения требований документов, определяющих порядок обработки персональных данных в учреждении.

1.5.2. Осуществлять оперативное вмешательство в работу лиц, не соблюдающих установленный порядок обработки персональных данных.

1.5.3. Контролировать действия лица, назначенного ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных, и администратора безопасности системы защиты информации информационных систем персональных данных в соответствии с инструкциями указанных ответственных лиц.

1.6. Лицо, ответственное за организацию обработки персональных данных, несет ответственность за:

1.6.1. Реализацию утвержденных документов, регламентирующих порядок обработки и защиты персональных данных.

1.6.2. Прием и обработку запросов и обращений субъектов персональных данных (или их законных представителей), всех промежуточных запросов и ответов, окончательных ответов на запросы и обращения, а также за своевременность предоставления и направления ответов.

1.6.3. Качество и последствия проводимых им работ по организации обработки и защиты персональных данных.

1.6.4. Разглашение персональных данных, ставших известными ему по роду работы.
