Приложение № 8
к Приказу от «16» декабря 2025 г. № 315

У Т В Е Р Ж Д А Ю

Директор
Муниципального учреждения
«Дом культуры «Матыра»
_____ Л.Л. Черепахина
«16» декабря 2025 г.

МП

ИНСТРУКЦИЯ

ответственного за организацию обработки персональных данных

Липецк 2025

1. Термины, определения и сокращения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Автоматизированная система (АС) – Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) – материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

2. Общие положения

2.1. Настоящая инструкция разработана на основании следующих нормативных документов:

- Федеральный закон от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июня 2006 № 152 «О персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Информационное сообщение Федеральной службы по техническому и экспортному контролю от 20 ноября 2012 г. N 240/24/4669 «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных»;
- Информационное сообщение Федеральной службы по техническому и экспортному контролю от 15 июля 2013 г. N 240/22/2637 «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и приказа ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"».

2.2. Инструкция определяет основные задачи, функции, обязанности и права Ответственного за организацию обработку персональных данных в информационных системах (далее – Ответственного) МУ «ДК «Матыра» (далее – Организация).

2.3. В своей деятельности Ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных в информационных системах (далее – ИС) и обеспечивает их выполнение.

2.4. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в Организации.

3. Задачи и функции Ответственного за организацию обработки персональных данных

3.1. Основными задачами Ответственного являются:

- разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты ПДн;
- доведение до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществление внутреннего контроля за соблюдением требований законодательства РФ и инструкций при обработке ПДн, в том числе требований к защите ПДн;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;
- заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) персональных данных;
- контроль эффективности защиты информации.

4. Обязанности Ответственного за организацию обработки персональных данных

4.1. Для реализации поставленных задач и возложенных функций Ответственный обязан:

4.1.2. Разработать перечень ПДн.

4.1.4. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ПЭВМ, на которых ведется обработка ПДн.

4.1.5. Своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на ПЭВМ.

4.1.6. Контролировать обеспечение защиты персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

4.1.7. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

4.1.8. Контролировать эффективность защиты персональных данных:

- Проводить работу по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам ПЭВМ.
- Проводить занятия с администраторами и пользователями ИС по правилам работы на ПЭВМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков выявленных при контроле эффективности защиты информации.

4.1.9. Организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования.

4.1.11. Участвовать в проведении внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных

4.2. Ответственному запрещается:

4.2.1. Использовать в своих и в чьих-либо личных интересах ресурсы ИС, предоставлять такую возможность другим.

4.2.2. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИС, блокировке, потери информации и предупреждения пользователей.

4.2.3. Допускать к работе на ПЭВМ и серверах посторонних лиц.

5. Права Ответственного за организацию обработки персональных данных

5.1. Ответственный имеет право:

- Получать доступ к программным и аппаратным средствам ИС, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИС и ПЭВМ пользователей.
- Требовать от пользователей ИС выполнения инструкций по обеспечению безопасности персональных данных в ИС.
- Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС.
- Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим отчетом Директору.

5.2. Лицо, ответственное за организацию обработки ПДн, несет ответственность за:

- Реализацию утвержденных в МУ «ДК «Матыра» документов, регламентирующих порядок обеспечения безопасности персональных данных.
- Программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним Директором и за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.
- Разглашение персональных данных и сведений ограниченного распространения, ставших известными ему по роду работы.
- Качество и последствия проводимых им работ по контролю действий пользователей при работе в ИС.

6. Проведение внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных.

6.1. Основными целями проведения внутреннего расследования являются:

- выявление предпосылок утраты персональных данных в результате нарушения порядка их обработки;
- выявления лиц из числа сотрудников МУ «ДК «Матыра» виновных в утрате персональных данных;
- определение ущерба в результате утраты персональных данных;
- проверка полноты и качества исполнения нормативных документов по работе со средствами защиты персональных данных;
- документальное подтверждение соответствия обработки, хранения и передачи персональных данных нормам и правилам, установленным федеральными правовыми и нормативными актами;

- определение фактического состояния системы защиты персональных данных.

6.2. Работник, по вине которого произошло нарушение, обязан по требованию Ответственного представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный вправе увеличить указанный срок, а также поставить перед работником перечень вопросов, на которые работник обязан ответить.

6.3. В целях внутреннего расследования все работники МУ «ДК «Матыра», по первому требованию Ответственного, должны предъявить для проверки все числящиеся за ними материалы, содержащие персональные данные, представить устные или письменные объяснения, в том числе об известных им фактах разглашения персональных данных, утраты документов и изделий, содержащих персональные данные.

6.4. В случае давления на работника со стороны других работников или третьих лиц (просьб, угроз, шантажа и др.) по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом Ответственному.

6.5. Для проведения внутреннего расследования Директор формирует комиссию из опытных и квалифицированных работников в составе не менее трех человек.

6.6. До вынесения решения, членам комиссии запрещается разглашать сведения остальным работникам МУ «ДК «Матыра» о ходе проведения внутреннего расследования и ставших известными им в связи с этим обстоятельствах.

6.7. В процессе проведения внутреннего расследования выясняются:

- перечень разглашенных сведений, составляющих персональные данные;
- причины разглашения персональных данных;
- круг лиц, виновных в разглашении персональных данных;
- размер причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с персональными данными;
- иные обстоятельства.

6.8. По результатам расследования, комиссией составляется акт, с отражением в нем лиц, виновных в разглашении персональных данных, размера причиненного ущерба МУ «ДК «Матыра», наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

6.9. На основании акта комиссия выносит решение о:

- применении мер дисциплинарного воздействия к работнику;
- информировании регулятора о факте нарушения;
- информировании правоохранительных органов;
- информировании субъектов персональных данных.

7. Организация режима безопасности помещений, где осуществляется работа с персональными данными

7.1. Ограничение доступа посторонних лиц в помещения, предназначенные для осуществления профессиональной деятельности, связанной с эксплуатацией ИС, предусматривает следующие:

- Исключение возможности бесконтрольного проникновения в эти помещения посторонних лиц, включая работников других структурных подразделений.
- После окончания рабочего дня двери помещений, в которых эксплуатируется ИС, закрываются на ключ и опечатывается персональным пломбиром. Все помещения имеют разные

замки. Дубликаты ключей хранятся в запираемом шкафу у Ответственного. В случае выхода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ.

- Уборка помещения производится в присутствии одного из сотрудников, работающего в этом помещении.
- Доступ работников в помещения подразделения по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.
- Строгое ограничение доступа посторонних лиц к серверам, а также сетевому оборудованию.
- Защита мест хранения носителей (USB flash-накопитель, CD, НЖМД) от беспрепятственного доступа посторонних лиц.

8. Приостановление обработки персональных данных

8.1. При выявлении недостоверных персональных данных или неправомерных действий с ними при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных необходимо осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных (приостановки предоставления персональных данных пользователям ИС), с момента такого обращения или получения такого запроса на период проверки.

8.2. В случае подтверждения факта недостоверности персональных данных на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов требуется уточнить персональные данные и снять их блокирование.

8.3. В случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, необходимо устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, необходимо уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязана уведомить субъект персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

8.4. В случае достижения цели обработки персональных данных необходимо незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъект персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также указанный орган.

8.5. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных требуется прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Организацией и субъектом персональных данных. Об уничтожении персональных данных необходимо уведомить субъект персональных данных.

8.6. В случае прекращения полномочий работника Администратором информационной безопасности приостанавливается предоставление ему персональных данных, а также немедленно производиться смена пароля после окончания последнего сеанса работы данного пользователя с системой.

Зам. директора — (должность)

(подпись)

Шохоров Д. А. — (ФИО)

«16» 12 2015 г.