ДЕПАРТАМЕНТ КУЛЬТУРЫ И ТУРИЗМА АДМИНИСТРАЦИИ ГОРОДА ЛИПЕЦКА
МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ «ДОМ КУЛЬТУРЫ «МАТЫРА»

ПРИКАЗ

от «16» декабря 2025 г. № 314

Липецк

О назначении ответственного за обеспечение безопасности информации в муниципальном учреждении «Дом культуры «Матыра»

В целях исполнения требований Указа Президента России от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и принятыми в соответствии с ним нормативными правовыми актами,

П Р И К А З Ы В А Ю:

1. Ответственность за обеспечение безопасности информации возложить на заместителя директора Шокорова Д.А.
2. Утвердить Инструкцию ответственного за обеспечение безопасности информации (Приложение №1).
3. Ответственному за обеспечение безопасности информации в своей деятельности руководствоваться Инструкцией ответственного за обеспечение безопасности информации.
4. Контроль за исполнением настоящего Приказа оставляю за собой.

.

Директор
Муниципального учреждения
«Дом культуры «Матыра» Л.Л. Черепахина

Приложение № 1
к Приказу от «16» декабря 2025 г. №314

У Т В Е Р Ж Д А Ю

Директор МУ «ДК «Матыра»
_____ Л.Л. Черепахина
«16» декабря 2025 г.

МП

ИНСТРУКЦИЯ
Ответственного за обеспечение безопасности информации

Липецк 2025

Оглавление

1. Термины, определения и сокращения

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 информационной 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»).

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»).

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»).

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:

2.1.1. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2.1.2. Федеральный закон от 27 июня 2006 № 152-ФЗ «О персональных данных»;

2.1.3. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2.1.4. 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»;

2.2. Инструкция определяет основные задачи, функции, обязанности и права Ответственного за защиту информации в Организации (далее – Ответственного).

2.3. В своей деятельности Ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты информации в информационных системах, доступ к которым осуществляется с автоматизированных рабочих мест сотрудников Организации (далее – ОИ) 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 защиту информации

– обеспечивать организацию построения и эксплуатации СЗИ ОИ и, при необходимости, модернизацию (развитие) СЗИ ОИ;

–обеспечивать организацию, координацию и выполнение работ по защите информации на ОИ;

–осуществлять внутренний контроль за соблюдением пользователями ОИ требований к обеспечению безопасности информации;

–вносить предложения по подготовке и принятию правовых, организационных и технических мер защиты информации на ОИ;

–контролировать соблюдение требований законодательства Российской Федерации и организационно-распорядительных документов по защите информации на ОИ;

–обеспечивать поддержание в актуальном состоянии организационно-распорядительных документов по защите информации на ОИ;

–осуществлять проведение контрольных мероприятий по защите информации на ОИ;

–обеспечивать проведение расследований инцидентов информационной безопасности на ОИ, принимать участие в расследовании инцидентов в пределах своей компетенции;

–обеспечивать безопасное хранение заполненных форм регистрации событий ИБ или инцидентов ИБ;

–обеспечивать контроль сторонних организаций (подрядчиков) при привлечении последних для обслуживания, настройки и ремонта средств защиты информации из состава СЗИ ОИ;

–организовывать выполнение требований парольной защиты;

–осуществлять процесс управления конфигурацией СЗИ ОИ;

–организовывать контроль за соблюдением условий использования средств криптографической защиты информации, установленных эксплуатационной и технической документацией на средства криптографической защиты информации и Инструкции по обращению со средствами криптографической защиты информации из состава СЗИ ОИ;

–принимать планы по действиям персонала ОИ при возникновении нештатных ситуаций;

–составлять план контрольных мероприятий по обеспечению уровня защищенности информации;

–организовывать проведение обучения (инструктажа) пользователей правилам работы со средствами защиты информации, применяемыми на ОИ;

–предоставлять консультации и оказывать содействие пользователям ОИ, участвующим в процессах обработки и защиты информации, по вопросам обработки и защиты информации на ОИ;

–осуществлять взаимодействие с государственными органами Российской Федерации, регулирующими вопросы защиты информации (далее – регулирующие органы), в том числе координировать действия лиц, участвующих в процессах обработки и защиты информации на ОИ, при проведении проверок регулирующими органами, а также при обработке запросов указанных органов.

4. Обязанности Ответственного за защиту информации

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

4.1.1. Разрабатывать решения по:

–определению списка устройств, логических дисков, каталогов общего пользования на серверах с указанием состава допущенных к ним пользователей и режимом допуска;

–разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, использованию СЗИ при передаче конфиденциальных документов).

4.1.2. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ПЭВМ, на которых ведется обработка конфиденциальной информации, в том числе ПДн.

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

4.1.4. Контролировать обеспечение защиты конфиденциальной информации, в том числе персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

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

4.1.6.Контролировать обеспечение защиты конфиденциальной информации, в том числе 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 ОИ или средств защиты.

4.1.8. Контролировать эффективность защиты конфиденциальной информации, в том числе 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 ОИ 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. Осуществлять контроль за правильностью учета, хранения, приема и выдачи персональных идентификаторов ответственным исполнителям.

4.1.10. Участвовать в проведении внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты конфиденциальной информации, в том числе персональных данных.

4.2. Ответственному запрещается:

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

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

5. Права Ответственного за защиту информации

5.1 Ответственный имеет право:

5.1.1 Получать доступ к программным и аппаратным средствам ОИ, средствам их защиты, а также просмотру прав доступа к ресурсам на ПЭВМ пользователей.

5.1.2 Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ОИ.

5.1.3 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 Руководителю.