

УТВЕРЖДАЮ

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



«16» декабря 2025 г.

ИНСТРУКЦИЯ
по организации учета, использования и уничтожения машинных
носителей информации

Липецк 2025

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 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»).

Государственная информационная система (ГИС) – 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»).

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»).

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 июня 2006 № 152-ФЗ «О персональных данных»;

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

2.2. Настоящая инструкция по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации (далее- МНИ) в – МУ «ДК «Матыра».

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

2.4. Учет, хранение и выдачу машинных носителей информации (далее – МНИ) осуществляет Администратор информационной безопасности.

3. Цель и задачи защиты машинных носителей информации

3.1. Целью реализации защиты МНИ в Организации является снижение вероятности реализации угроз безопасности информации, направленных на:

- несанкционированный доступ к МНИ;
- несанкционированную запись информации на съемный носитель информации;
- внедрение в Организации вредоносного программного обеспечения о съемных МНИ.

3.2. Реализация процессов защиты МНИ в Организации достигается решением следующих задач:

- учет МНИ;
- управление физическим доступом к МНИ;
- контроль подключения съемных МНИ.

3.3. В качестве МНИ рассматриваются:

- съемные машинные носители (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки и иные аналогичные по функциональности устройства);
- встроенные в портативные или стационарные технические средства машинные носители информации (накопители на жестких дисках).

4. Порядок учета машинных носителей информации

4.1. Учету подлежат все используемые в Организации МНИ.

4.2. Учет МНИ включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации,

номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

4.3. Учет съемных МНИ должен осуществляться в «Журнале учета машинных носителей информации...». Форма журнала учета машинных носителей утверждается приказом директора МУ «ДК «Матыра».

4.4. Ведение журнала учета осуществляет Администратор информационной безопасности.

5. Порядок выдачи и возврата съемных машинных носителей информации

5.1. Учет выдачи и возврата МНИ должен осуществляться Администратором информационной безопасности с фиксацией действия в «Журнале учета машинных носителей информации...».

5.2. Персональную ответственность за сохранность полученных МНИ несет сотрудник Организации, получивший эти носители.

5.3. В случае утраты пользователем съемного МНИ, в журнале учета выдачи МНИ заносится отметка об утрате.

6. Хранение машинных носителей информации и порядок доступа к ним

6.1. Хранение машинных носителей должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

6.2. В целях недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

6.3. Доступ к МНИ, встроенным в корпус средств вычислительной техники (накопители на жестких дисках), должен осуществляться в соответствии с порядком доступа в помещения, в которых они размещены.

6.4. Ответственным за хранение съемных МНИ является пользователь съемного МНИ.

6.5. В случае утраты или порчи МНИ, содержащих конфиденциальную информацию, в т.ч. ПДН ставится в известность Администратор информационной безопасности.

7. Порядок списания машинных носителей информации и уничтожения (стирания) информации на них

7.1. Уничтожение информации с МНИ должно инициироваться пользователями и осуществляться средствами программного обеспечения.

7.2. Уничтожение МНИ пришедших в негодность, производится путем их физического разрушения.

7.3. Списание МНИ производится комиссией, назначаемой директором МУ «ДК «Матыра».

8. Ответственность

8.1. Ответственность за выполнение правил эксплуатации МНИ при выполнении непосредственных работ с носителями несет пользователь.

8.2. Контроль выполнения пользователями установленных правил эксплуатации МНИ, осуществляют ответственный за организацию обработки персональных данных и администратор информационной безопасности в рамках своих должностных обязанностей.

ЛИСТ ОЗНАКОМЛЕНИЯ

с инструкцией по организации учета, использования и уничтожения машинных носителей,
утвержденной Приказом (Приложение №4) от «16» декабря 2025 г. №315

№ п/п	Ф.И.О.	Подпись, дата
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		