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

ПРИКАЗ

от «16» декабря 2025 г. № 313

Липецк

Об организации режима безопасности помещений, принадлежащих муниципальному учреждению «Дом культуры «Матыра»

В целях исполнения Постановления Правительства РФ от 01 ноября 2013 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и 11риказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания я организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительственных данных для каждого из уровней защищенности»

П Р И К А З Ы В А Ю:

1. Ввести в муниципальном учреждении «Дом культуры «Матыра» режим обеспечения безопасности помещений, в которых размещены компоненты информационных систем, в том числе используемые СКЗИ, носители ключевой, аутентифицирующей и парольной информации СКЗИ.

2. Утвердить перечень лиц, имеющих право доступа в помещения, в которых размещены компоненты информационных систем, доступ к которым осуществляется с автоматизированных рабочих мест сотрудников муниципального учреждения «Дом культуры «Матыра», в том числе производится обработка персональных данных и используются средства криптографической защиты информации, носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации (Приложение №1).

3. Режим обеспечения безопасности помещений осуществлять в соответствии с документом «Порядок доступа сотрудников муниципального учреждения «Дом культуры «Матыра» в помещения, в которых размещены средства защиты информации, в том числе производится обработка персональных данных и используются средства криптографической защиты информации, носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации» (Приложение №2).

6. Контроль за исполнением настоящего Приказа возложить на заместителя директора Шокорова Д.А.

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

Приложение № 1

к Приказу от «16» декабря 2025 г № 313

Перечень лиц, имеющих право доступа в помещения, в которых размещены компоненты информационных систем, доступ к которым осуществляется с автоматизированных рабочих мест сотрудников муниципального учреждения «Дом культуры «Матыра», в том числе производится обработка персональных данных и используются средства криптографической защиты информации, носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации

№ п/п	ФИО	Должность
1.	Черепахина Лилия Леонидовна	Директор
2.	Шокоров Дмитрий Александрович	Заместитель директора
3.	Тильпо Егор Геннальевич	Заместитель директора
4.	Ларина Людмила Анатольевна	Секретарь руководителя
5.	Стасёв Владимир Александрович	Звукорежиссер
6.	Путилин Алексей Геннадьевич	Звукорежиссер
7.	Алферов Иван Викторович	Заведующий информационным отделом
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

Приложение № 2

к Приказу от «16» декабря 2025 г № 313

Порядок доступа сотрудников муниципального учреждения «Дом культуры «Матыра» в помещения, в которых размещены средства защиты информации, в том числе производится обработка персональных данных и используются средства криптографической защиты информации, носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации

1. Общие положения

1.1. Настоящий Порядок разработан в соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и Приказом ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.2. Целью настоящего Порядка является обеспечение безопасности информации (в том числе персональных данных) путем создания условий, затрудняющих несанкционированный доступ к аппаратным, программным средствам защиты, машинным носителям, средствам криптографической защиты информации, носителям ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации.

1.3. Кабинеты, расположенные по адресу: г. Липецк, ул. Энергостроителей, 5а, 2 этаж, каб. №2.1, 2.2, в которых производится обработка персональных данных, установлены технические средства защиты информации, хранятся машинные носители информации, установлены средства криптографической защиты информации или хранятся ключевые документы к ним, в настоящем Порядке именуются – Помещения.

2. Организация доступа в Помещения

2.1. Для Помещений, указанных в п.1.3 настоящего Порядка, организуется режим обеспечения безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания посторонних лиц.

2.2. В Помещения допускаются сотрудники, указанные в «Перечне лиц, имеющих право доступа в помещения...» (далее – Перечень).

2.3. Сотрудники, не внесенные в список Перечня (далее – лица, не имеющие право доступа в Помещения), являются посторонними лицами и могут находиться в Помещениях только в присутствии лиц, имеющих права доступа в Помещения.

2.4. Сторонние лица, не являющиеся сотрудниками Организации, имеют право пребывать в Помещениях только в присутствии лиц, имеющих право доступа в Помещения, и в течение ограниченного количества времени, необходимого для решения вопросов, связанных с осуществлением основной деятельности, выполнением возложенных законодательством РФ функций, полномочий и обязанностей и (или) осуществлением полномочий в рамках заключенных договоров.

2.5. Помещения должны быть оборудованы надежно запираемыми шкафами (ящиками, хранилищами) индивидуального пользования. Ключи от указанных хранилищ должны

храниться у ответственного за организацию работ со средствами криптографической защиты информации.

2.6. При утрате ключа от хранилища или от входной двери в Помещение, замок требуется заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если переделать замок от хранилища не представляется возможным, такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачены ключи, до изменения его секрета устанавливается ответственным за организацию работ со средствами криптографической защиты информации.

2.7. Доступ в Помещение разрешается только в рабочее время.

2.8. В течение рабочего времени лица, имеющие право доступа в Помещение, утвержденные Перечнем лиц, имеющих доступ в помещение (форма представлена в Приложении А):

- При оставлении последним Помещения закрывают дверь Помещения на ключ (при этом запрещается оставлять ключ в замке Помещения);
- Не покидают Помещение, если в нем находятся лица, не внесенные в соответствующий Перечень;
- При обнаружении фактов нарушения режима безопасности Помещения ставят в известность Ответственного за обеспечение безопасности информации;
- При посещении Помещения посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию Помещений и их инженерно-технических средств ставят в известность об этом Ответственного за обеспечение безопасности информации.

2.9. Доступ в Помещения в нерабочее время возможен только по письменной заявке сотрудника, согласованной с Ответственным за обеспечение безопасности. Данные заявки хранятся у Ответственного за обеспечение безопасности информации.

2.10. Доступ в Помещения при возникновении нештатной ситуации в нерабочее время осуществляется в присутствии Ответственного за обеспечение безопасности информации с составлением акта на вскрытие (далее – акт).

В акте необходимо указать:

- фамилии, имена, отчества лиц, принимавших участие во вскрытии Помещения;
- причины вскрытия Помещения;
- дату и время вскрытия Помещения;
- кто был допущен (должность и фамилия) в Помещение для ликвидации последствий нештатной ситуации;
- как осуществлялась охрана вскрытого Помещения в этот период;
- какое имущество, в каком количестве, куда эвакуировано из вскрытого Помещения и как осуществлялась его охрана;
- кто из должностных лиц и когда был информирован по указанному факту происшествия;
- другие сведения.

Акт подписывается лицами, вскрывшими Помещение.

Вскрытие сейфов с машинными носителями, содержащими информацию, осуществляется сотрудниками, отвечающими за их сохранность.

2.11. При обслуживании Помещения (уборка или различный ремонт Помещения, инженерно-технического оборудования):

- обслуживающий персонал находится в Помещении только в присутствии лиц, имеющих право доступа в Помещение;
- ключи от замков дверей Помещения обслуживающему персоналу и другим лицам, не имеющим права доступа в Помещение, без согласования с Ответственным за обеспечение безопасности информации не выдаются;
- сотрудники, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонентов ПЭВМ и машинных носителей информации;

- сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении сотрудников, имеющих право доступа в Помещения;

- капитальный или иной ремонт может проводиться и без присмотра, однако при этом в обязательном порядке ПЭВМ и машинные носители информации должны быть вынесены из ремонтируемого Помещения в другие контролируемые Помещения, и по окончании ремонта должны быть сменены замки.

2.12. Лица, имеющие право доступа в Помещения, несут ответственность за нерегламентированное пребывание в Помещениях сотрудников, не имеющих права доступа в Помещения.

3. Контроль соблюдения порядка доступа в Помещения

3.1. Контроль выполнения сотрудниками требований настоящего Порядка осуществляется ответственным за обеспечение безопасности информации.

3.2. Ответственный за обеспечение защиты информации установления факта нарушения сотрудником настоящего Порядка проводит с ним разъяснительную работу, а в случае неоднократного нарушения уведомляет директор МУ «ДК «Матыра».

3.3. Порядок и режим охраны должен предусматривать периодический контроль состояния технических средств охраны и пожарной сигнализации, если таковые имеются