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

ПРИКАЗ

от «16» декабря 2025 г. № 318

Липецк

Об организации контроля (анализа) защищенности информации при ее обработке на автоматизированном рабочем месте пользователя государственной информационной системы «Система электронного документооборота Правительства Липецкой области и исполнительных органов государственной власти Липецкой области» в МУ ДК «Матыра»

В целях осуществления внутреннего контроля за обеспечением уровня защищенности информации, обрабатываемой с использованием средств автоматизации в государственных информационных системах, оператором которых назначено областное бюджетное учреждение «Информационно-технический центр», а также учета и контроля состава машинных носителей информации и средств защиты информации

П Р И К А З Ы В А Ю:

1. Утвердить и ввести в действие «Правила осуществления внутреннего контроля (мониторинга) за обеспечением уровня защищенности информации на автоматизированном рабочем месте пользователя государственной информационной системы «Система электронного документооборота Правительства Липецкой области и исполнительных органов государственной власти Липецкой области» (далее – АРМ ГИС «СЭД») МУ ДК «Матыра» (Приложение № 1).
2. Ответственному за защиту информации на АРМ ГИС «СЭД» и администратору информационной безопасности проводить систематические мероприятия по анализу защищенности АРМ ГИС «СЭД» и тестированию работоспособности системы защиты информации в порядке и с периодичностью, установленными в «Правилах осуществления внутреннего контроля (мониторинга)…» в части их касающейся.
3. Утвердить и ввести в действие следующие формы журналов:
   3.1. Журнал учета и выдачи машинных носителей информации (Приложение № 2);
   3.2. Журнал учета мероприятий по контролю защищенности информации (Приложение № 3);
   3.3. Журнал инструктажа пользователей (Приложение №4);
   3.4. Журнал учета выдачи паролей (Приложение № 5);
   3.5. Журнал учета конфиденциальной информации (Приложение № 6);
   3.6. Журнал учета инцидентов информационной безопасности (Приложение №7);
   3.7. Журнал учета хранилищ, ключей и оттисков печатей (Приложение №8).

4. Назначить ответственным за ведение журналов, указанных в пункте 3 настоящего приказа, администратора информационной безопасности Ларину Л.А. секретаря руководителя.

5. 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 № 318

Правила
осуществления внутреннего контроля (мониторинга) за обеспечением уровня защищенности информации в МУ ДК «Матыра»

1. Общие положения

1.1. Правила осуществления внутреннего контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся на АРМ ГИС «СЭД» (далее – Правила) определяют план и порядок проведения внутренних проверок организации защиты информации.

1.2. Целью внутренних проверок является определение соответствия организации защиты информации действующему законодательству РФ, а также локальным актам муниципального учреждения «Дом культуры «Матыра» по обеспечению защиты информации.

2. План проведения внутренних проверок

2.1. План содержит перечень внутренних проверок и определяет для каждой из них:

- название проверки;
- периодичность проведения проверки;
- ответственного исполнителя.

2.2. Общий срок проведения проверки не должен превышать 30 рабочих дней.

2.3. Информация о проведенной проверке, дата ее начала и окончания, а также ее результаты, фиксируется в «Журнале учета мероприятий по контролю защищенности информации…».

2.4. План проведения внутренних проверок приведен в Приложении к настоящим Правилам.

3. Порядок проведения внутренних проверок

3.1. **Порядок проведения контроля установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации**

В ходе проведения проверки необходимо:

3.1.1. Проверить соответствие версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации.

3.1.2. Проверить наличие отметок в эксплуатационной документации (формуляр, паспорт) об установке (применении) обновлений.

3.2. **Порядок проведения контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации**

В ходе проведения проверки необходимо:

3.2.1. Проверить работоспособность (неотключение) программного обеспечения и средств защиты информации.

3.2.2. Проверить правильность функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации.

3.2.3. Проверить соответствие настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации.

3.2.4. В случае возникновения необходимости восстановить работоспособность, правильное функционирование, а также параметры настройки программного обеспечения и средств защиты информации, в том числе с использованием резервных копий и (или) *дистрибутивов.*

3.3. **Порядок проведения контроля состава технических средств, программного обеспечения и средств защиты информации**

В ходе проведения проверки необходимо:

3.3.1. Проверить соответствие состава программного обеспечения, технических средств и средств защиты информации приведенному в локальных документах и эксплуатационной документации.

3.3.2. Исключить из состава несанкционированно установленные (удаленные) технические средства, программное обеспечение и средства защиты информации.

3.3.3. Проверить выполнение условий и сроков действия сертификатов соответствия на средства защиты информации

3.3.4. В случае возникновения необходимости принять меры, направленные на устранения выявленных недостатков.

3.4. **Порядок проведения контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей**

В ходе проведения проверки необходимо:

3.4.1. Проверить соблюдение пользователями и ответственными лицами правил генерации и смены паролей пользователей.

3.4.2. Проверить соответствие заведенных и удаленных учетных записей пользователей локальным документам.

3.4.3. Осуществить проверку реализации правил разграничения доступа и полномочий пользователей в соответствии с утвержденной матрицей доступа.

3.4.4. Провести контроль наличия документов, подтверждающих разрешение изменения учетных записей пользователей, их параметров, правил разграничения доступа, установленных полномочий пользователей.

3.4.5. В случае возникновения необходимости принять меры, направленные на устранения выявленных недостатков.

3.5. **Порядок проведения проверки соблюдения режима защиты информации**

В ходе проведения проверки необходимо:

3.5.1. Определить соблюдают ли работники, участвующие в процессе обработки защищаемой информации, принятые меры по защите информации.

3.5.2. Произвести контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена.

3.5.3. Произвести контроль соблюдения Порядка доступа сотрудников, а также сторонних лиц в помещения.

3.5.4. Осуществить проверку наличия машинных носителей информации.

3.5.5. Проверить наличие и ведение журналов, используемых для контроля (анализа) защищенности информации.

3.5.6. Произвести контроль над выполнением резервного копирования и архивирования информации ограниченного доступа.

3.6. **Порядок проведения анализа и пересмотра существующих мер по обеспечению защиты информации**

В ходе проведения проверки необходимо:

3.6.1. Определить изменения в базовой конфигурации, проверить наличие данных о внесении изменений в документацию на систему защиты информации.

3.6.2. Провести анализ произведенных изменений на предмет возникновения дополнительных угроз безопасности защищаемой информации.

3.6.3. В случае выявления новых источников угроз провести уточнение и дополнение модели угроз безопасности.

3.6.4. Провести соотношение выявленных угроз безопасности с реализованными мерами по защите информации, в случае необходимости применить дополнительные меры по защите

информации.

3.6.5. По результатам анализа изменённой модели угроз и выбора необходимых дополнительных мер по защите информации – принять решение об обновлении либо модернизации системы защиты информации.

3.6.6. Сообщить Ответственному за защиту информации о необходимости переаттестации или проведении дополнительных аттестационных испытаний.

3.7. **Порядок проведения проверки наличия и актуальности внутренней нормативной документации по защите информации**

В ходе проведения проверки необходимо:

3.7.1. Проверить наличие соответствующих действующему законодательству РФ организационно-распорядительных документов, регламентирующих правила и процедуры, защиты информации (далее – организационно-распорядительные документы по защите информации).

3.7.2. Проверить наличие доказательств ознакомления работников с организационно-распорядительными документами по защите информации.

3.7.2.1. Принять решение о необходимости актуализации организационно-распорядительных документов по защите информации.

3.8. **Проверка целостности и функционирования средств криптографической защиты информации.**

3.8.1. Проверить работоспособность средств криптографической защиты информации.

3.8.2. Проверить целостность средств криптографической защиты информации.

Приложение
к Правилам осуществления внутреннего
контроля (мониторинга) за обеспечением
уровня защищенности информации
АРМ ГИС «СЭД»

План проведения внутренних проверок

Проверка	Периодичность	Методика (программа) проверки	Ответственный исполнитель
Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	1 раз в 3 месяца	Пункт 3.1 настоящих Правил	Администратор информационной безопасности
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	1 раз в 3 месяца	Пункт 3.2 настоящих Правил	Администратор информационной безопасности
Контроль состава технических средств, программного обеспечения и средств защиты информации	1 раз в 3 месяца	Пункт 3.3 настоящих Правил	Администратор информационной безопасности
Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей	1 раз в полгода	Пункт 3.4 настоящих Правил	Ответственный за защиту информации
Проверка соблюдения режима защиты информации	1 раз в полгода	Пункт 3.5 настоящих Правил	Ответственный за защиту информации
Анализ и пересмотр существующих мер защиты информации	1 раз в год	Пункт 3.6 настоящих Правил	Администратор информационной безопасности
Проверка наличия и актуальности внутренней нормативной документации по защите информации	1 раз в год, а также перед проверками регуляторов	Пункт 3.7 настоящих Правил	Ответственный за защиту информации
Проверка работоспособности и целостности (в том числе пломбы установленные на СКЗИ не повреждены)	Не реже одного раза в месяц/случае нарушения работоспособности СКЗИ, нарушении конфиденциальности информации	Пункт 3.8 настоящих Правил	Ответственный за СКЗИ

Приложение №2
к Приказу от «16» декабря 2025 г № 318

ЖУРНАЛ
учета и выдачи машинных носителей информации
(форма)

№ п.п.	Учетный номер носителя	Вид носителя	Заводской номер носителя	Фамилия и инициалы владельца	Дата и роспись в получении	Дата и номер акта уничтожения
1	2	3	4	5	6	7

Приложение №3
к Приказу от «16» декабря 2025 г № 318

ЖУРНАЛ
учета мероприятий по контролю защищенности информации
(форма)

№ п/п	Мероприятие	Дата	Фамилия И.О. исполнителя	Результат	Подпись исполнителя
1	2	3	4	5	6

Приложение №4
к Приказу от «16» декабря 2025 г № 318

ЖУРНАЛ
инструктажа пользователей
(форма)

№ п/п	Дата проведения инструктажа	ФИО инструктируемого	Должность инструктируемого	ФИО инструктирующего	Подпись	
					Инструктирующего	Инструктируемого
1	2	3	4	5	6	

Приложение №6
к Приказу от «16» декабря 2025 г № 318

ЖУРНАЛ
учета конфиденциальной информации
(форма)

Порядковый регистра-ционный номер и гриф секретности	Дата подписи	Номер поступившего документа	Откуда документ поступил или кем подготовлен (подразделение, фамилия)	Вид и краткое содержание документа	Количество поступивших, подготовленных экземпляров, листов и отметка о движении (передаче, отправке)						Отметка о местонахождении, направлении или уничтожении документа	Дата проверки наличия документа
					Количество экземпляров	Номера экземпляров	Количество листов		Кому передан, резолюция, куда направлен документ, отметка о взятии на контроль и об исполнении	Расписка в получении и дата		
							Основного документа	Приложения				
1	2	3	4	5	6	7	8	9	8	9	10	11

Приложение №7
к Приказу от «16» декабря 2025 г № 318

ЖУРНАЛ
учета инцидентов информационной безопасности
(форма)

№ п/п	Краткое описание инцидента	ФИО, должность сотрудника, обнаружившего инцидент, дата и время обнаружения	Дата и время пресечения несанкционированного воздействия	Дата, время доведения информации об инциденте в отдел информационной безопасности Правительства липецкой области, ФИО и должность сотрудника принявшего информацию	ФИО и подпись системного администратора/администратора безопасности
1	2	3	4	5	6

Приложение №8
к Приказу от «16» декабря 2025 г № 318

ЖУРНАЛ
учета хранилищ, ключей и оттисков печатей
(форма)

№ п/п	Наименование хранилища, печати, штампа, ключа	Номер хранилища, печати, штампа, ключа	Дата и подпись лица в получении	Отметка о возврате	Примечание
1	2	3	4	5	6