Приложение № 5__

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

по регистрации, выявлению и реагированию на инциденты

Липецк 2025

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»).

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)).

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»).

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»).

Инцидент (информационная безопасность) - одно или несколько нежелательных или неожиданных событий в области информационной безопасности, которые со значительной степенью вероятности могут привести к нарушению операционной деятельности и поставить под угрозу информационную безопасность [ИСО/МЭК 27035-1].

1. Общие положения

1.1. Настоящая инструкция разработана на основании следующих нормативных документов:

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

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

1.2. Инструкция по регистрации, выявлению и реагированию на инциденты информационной безопасности определяет общие функции, ответственность, права и обязанности ответственных за управление инцидентами информационной безопасности лиц.

1.2. . Все сотрудники МУ «ДК «Матыра» должны немедленно уведомлять администратора безопасности о выявленных слабых местах и инцидентах. Пользователи не должны использовать имеющиеся уязвимости.

1.3. После получения уведомления, а также в случае самостоятельного обнаружения инцидента информационной безопасности (далее – ИБ) администратор безопасности должен отреагировать на инцидент и принять меры по:

- Анализу инцидента ИБ.
- Предотвращению развития инцидента ИБ.
- Устранению инцидента ИБ.
- Восстановлению безопасности после инцидента ИБ.
- Регистрации инцидента ИБ, проведении внутреннего расследования (при необходимости).
- Формирование рекомендаций по результатам инцидента ИБ по повышению уровня ИБ.

1.4. Информация об инцидентах ИБ, приведших к нарушению безопасности ИС, должна быть задокументирована администратором безопасности.

1.5. В МУ «ДК «Матыра» должна осуществляться периодическая проверка эффективности действий по реагированию на инциденты ИБ.

2. Регистрация событий информационной безопасности

2.1. События безопасности, подлежащие регистрации, должны определяться с учетом способов реализации угроз безопасности. К событиям безопасности, подлежащим регистрации, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты конфиденциальной информации (в т.ч. ПДн), указывающие на возможность нарушения конфиденциальности, целостности или доступности конфиденциальной информации (в т.ч. ПДн), доступности компонентов ГИС, нарушения процедур, установленных организационно-

распорядительными документами, а также на нарушение штатного функционирования средства защиты информации.

2.2.Состав и содержание информации по каждому событию, включенному в список регистрации должны идентифицировать источник, время и результат события

2.3.К событиям безопасности в МУ «ДК «Матыра», которые подлежат регистрации, относятся:

— события безопасности, имеющие отношение к возможности реализации угроз безопасности конфиденциальной информации (в т.ч. ПДн), описанных в модели угроз безопасности ГИС;

— разглашение конфиденциальной информации, либо угроза такого разглашения;

— компрометация учетных записей или паролей

— вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки операционной системы;

— компрометация учетных записей или паролей;

— подключение съемных машинных носителей информации и вывод конфиденциальной информации (в т.ч. ПДн) на съемные машинные носители;

— вирусная атака или вирусное заражение;

— нарушение или сбой в работе системы резервного копирования;

— попытки удаленного доступа;

2.4. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

2.5.Порядок сбора, записи и хранения информации о событиях безопасности

2.5.1.Настройку журналов регистрации событий информационной безопасности в программном обеспечении ИС и СЗИ осуществляет администратор безопасности (Приложение 2).

2.5.2.Администратор информационной безопасности должны **не реже 1 раза в неделю** просматривать журналы регистрации событий безопасности.

2.5.3.Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись в память технических средств ИС и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение **1 месяца**.

2.5.4.Информация о событиях безопасности в ГИС, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана), должна фиксироваться администратором информационной безопасности при её обнаружении в журнале событий безопасности.

2.5.5.Администратор безопасности должен исследовать наиболее часто повторяющиеся события безопасности, выяснять причины их возникновения и устранять эти причины.

3. Выявление инцидентов информационной безопасности

3.1.Основными источниками информации об Инцидентах ИБ являются:

- факты, выявленные отделом, а также другими сотрудниками организации;

- результаты работы средств мониторинга ИБ, результаты проверок и аудита (внутреннего или внешнего);

- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

- обращения субъектов персональных данных с указанием Инцидента ИБ;

- другие источники информации.

3.2. Выявление и учет инцидентов организует администратор безопасности на основе получения о предполагаемом инциденте, проводит первоначальный анализ полученных данных. В процессе анализа администратор безопасности проводит проверку наличия в выявленном факте нарушений.

3.3. Если администратор информационной безопасности определяет текущее событие безопасности как инцидент, то он незамедлительно принимает в установленном порядке меры для устранения последствий инцидента в рамках своих полномочий.

3.4. При выявлении инцидента осуществляют оповещение пользователей об инциденте. Форму и порядок оповещения устанавливает администратор безопасности.

4. Порядок реагирования на инциденты

4.1. При реагировании на инциденты осуществляют анализ инцидента, устраняют причины и последствия инцидента, формируют перечень мероприятий по предотвращению инцидента в будущем.

4.2. Анализ инцидента организует администратор безопасности с привлечением специалистов отдела информационных технологий и пользователей-непосредственных участников инцидента.

4.3. Анализ проводит комиссия, состав которой определяет администратор информационной безопасности.

4.4. Анализ инцидента оформляется Актом расследования инцидента информационной безопасности (Приложение А).

4.5. Устранение причин и последствий инцидента осуществляет администратор информационной безопасности и/или совместно с администраторами системными по установленным правилам и в установленные сроки.

4.6. Перечень мероприятий, направленных на предотвращение инцидента в будущем, формирует, утверждает директор МУ «ДК «Матыра» и организует выполнение администратор информационной безопасности. Форма перечня мероприятий не регламентируется.

Приложение А

Акт «___»
об инциденте информационной безопасности

Инцидент зафиксирован

_____

(дата, ф.и.о.работника)

В инциденте зафиксированы следующие работники

_____

(ф.и.о. работника (-ов))

_____

Описание инцидента

_____

_____

_____

Причины инцидента

_____

_____

_____

Меры, принятые для устранения причин, последствий инцидента

_____

_____

_____

Фамилия И.О. «___»_____

Форма журнала
учета инцидентов информационной безопасности

№ п/п	№ акта	Дата совершения инцидента	Краткое описание инцидента	Сроки устранения инцидента	Ф.И.О. Подпись