Приложение №2
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 организации парольной защиты

Липецк 2025

Термины и определения

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»).

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»).

1. Общие положения

1.1. Настоящая инструкция разработана на основании следующих нормативных документов:

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

1.1.2. Федеральный закон от 27 июня 2006 № 152 «О персональных данных».

1.2. Инструкция устанавливает основные правила парольной защиты и регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей, а также контроль за действиями пользователей системы при работе с паролями.

1.3. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах (далее - ИС) и контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями возлагается на Администратора информационной безопасности.

1.4. Требования настоящей Инструкции распространяются на всех сотрудников МУ «ДК «Матыра» (далее – Организация), использующих в работе средства вычислительной техники и должны применяться для всех средств вычислительной техники, эксплуатируемой в Организации.

2. Организация парольной защиты

2.1. Установку первичного пароля производит Администратор информационной безопасности при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на Администраторе информационной безопасности.

2.2. При создании первичного пароля, администратор информационной безопасности обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

2.3. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

2.4.Полная плановая смена паролей проводится не реже одного раза в 3 месяца.

2.5.Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую должность и т.п.) должна производиться Администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя.

2.6. Устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) пользователя, равное 7, после чего учетная запись блокируется.

2.7. Разблокирование учетной записи осуществляется Администратором информационной безопасности.

2.8. После 15 минут бездействия (неактивности) происходит автоматическое блокирование сеанса доступа в автоматизированное рабочее место пользователя (далее – АРМ) или учетной записи.

3. Требования к формированию паролей

3.1. Пользователи при формировании паролей должны руководствоваться следующими требованиями:

3.1.1. Длина пароля должна быть не менее 12 символов.

3.1.2. В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:

- буквы в верхнем регистре;
- буквы в и нижнем регистре;
- цифры;
-специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, *, % и т.п.).

3.2. Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

3.3. Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.

3.4. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

3.5. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

3.6. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

3.7. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

4. Правила ввода паролей

4.1. Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ должны руководствоваться следующими правилами:

4.1.1. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

4.1.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

4.1.3. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля), Пользователю необходимо уведомить Администратора информационной безопасности соответственно для проведения процедуры генерации нового пароля.

5. Обязанности

5.1. Пользователи обязаны:

5.1.1. Четко знать и строго выполнять требования настоящей инструкции по парольной защите.

5.1.2 Своевременно сообщать Администратору информационной безопасности об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ.

5.1.3. Ознакомиться под роспись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6. Ответственность

6.1. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ.