

Утверждаю

Директор

МБУ ДО ЦРТДЮ

Максютов В.Т.

Приказ № \_\_\_\_\_ от \_\_\_\_\_ 2024г.

## ИНСТРУКЦИЯ

по организации парольной защиты  
на автоматизированных системах

**МБУ ДО ЦРТДЮ**

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на автоматизированных системах МБУ ДО ЦРТДЮ.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора безопасности информации.
2. Личный пароль должен генерироваться и распределяться централизованно либо выбираться пользователем автоматизированной системы самостоятельно с учетом следующих требований: длина пароля должна быть не менее 6 символов; числе символов пароля **обязательно должны присутствовать** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, \$, &, \*, % и т.п.); пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.); при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях; личный пароль пользователь не имеет права сообщать никому. Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
3. Плановая смена паролей пользователя должна проводиться регулярно, не реже одного раза в 3 месяца.
4. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

5. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

6. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в лично опечатанном владельцем пароля конверте.

7. Контроль, за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации.