УТВЕРЖДЕНА

приказом директора
ОГБУ «КЦСО ЕАО»
от «02» 07 2024 г. № 184

ИНСТРУКЦИЯ
по организации парольной защиты в областном государственном бюджетном учреждении «Комплексный центр социального обслуживания Еврейской автономной области»

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации и/или выбора, использования, хранения, смены и прекращения действия паролей (удаления учётных записей пользователей) на автоматизированных рабочих местах (далее – АРМ), входящих в состав информационной системы персональных данных (далее – ИСПДн) в областном государственном бюджетном учреждении «Комплексный центр социального обслуживания Еврейской автономной области» (далее – ОГБУ «КЦСО ЕАО»), а также контроль за действиями пользователей и обслуживающего персонала ИСПДн при работе с паролями. Парольная защита при работе в ИСПДн осуществляется с целью предотвращения несанкционированного доступа (далее – НСД) к конфиденциальной информации, содержащей персональные данные.

1. Организационное и техническое обеспечение процессов генерации и/или выбора, использования, хранения, смены и прекращения действия паролей (удаления учётных записей пользователей) в ИСПДн и на АРМ ОГБУ «КЦСО ЕАО», а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности, в его отсутствие – на ответственного за организацию обработки ПДн.

2. Требования настоящего Порядка являются неотъемлемой частью комплекса мер безопасности и защиты информации в Учреждении.

3. Требования настоящего Порядка распространяются на всех должностных лиц и сотрудников подразделений Учреждения, использующих в работе ИСПДн, а также всех видов программного обеспечения (ПО), эксплуатируемого в Учреждении.

4. Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам Учреждения формируются (выбираются) пользователями этих ресурсов с учётом следующих требований к качеству парольной информации:

№	Параметр качества пароля	Администратор	Пользователь
1	Минимальная длина пароля в символах	8	6
2	Содержание в пароле цифр и букв латинского алфавита в верхнем и нижнем регистрах	обязательно	обязательно
3	Содержание в пароле специальных символов (@, #, $, &, *, % и т.п.)	обязательно	рекомендуется
4	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, наименований АРМ и т.п.	нет	нет
5	Содержание в пароле общепринятых сокращений (ПЭВМ, ЛВС, USER, PASSWORD и т.п.)	нет	нет
6	Минимальное отличие нового пароля от предыдущего (в позициях)	4	4
7	Максимальный срок действия пароля	12 мес.	12 мес.

5. При организации парольной защиты запрещается: записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе, на обратной стороне клавиатуры и т.п.); хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги; сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

6. Хранение сотрудником (администратором, пользователем) личных паролей допускается только в личном сейфе (запираемом шкафу, ящике), либо в сейфе (запираемом шкафу, ящике) администратора, либо в сейфе (запираемом шкафу, ящике) руководителя структурного подразделения. При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

7. Каждый пользователь несёт ответственность за неразглашение личного пароля третьим лицам.

8. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

9. При наличии (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) технологической необходимости использования имён и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учётных записей) в запечатанном конверте передавать на хранение ответственному за организацию обработки ПДн.

10. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

11. Внеплановая смена личного пароля или удаление учётной записи пользователя АРМ в случае прекращения его полномочий (увольнение) должна производиться администратором информационной безопасности ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой.

12. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности ИСПДн, ответственного за организацию парольной защиты, ответственного за организацию обработки ПДн, и других сотрудников, которым по роду служебной деятельности были предоставлены полномочия по управлению парольной защитой в ОГБУ «КЦСО ЕАО».

13. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с пунктом 11 или пунктом 12 настоящей Инструкции, в зависимости от полномочий владельца скомпрометированного пароля.

14. Компрометация действующих паролей является нештатной ситуацией, о чём администратор информационной безопасности незамедлительно сообщает руководителю.

15. Владельцы паролей должны быть ознакомлены с требованиями настоящей инструкции и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации. Ознакомление сотрудников Учреждения с требованиями Порядка проводит администратор информационной безопасности ИСПДн под роспись в журнале или на самом документе.

16. Повседневный контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на заведующих отделениями, периодический контроль возлагается на администратора информационной безопасности ИСПДн, ответственного за организацию парольной защиты.