Приложение к приказу 126-О от 25.10.2023

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ РАБОЧЕЙ СТАНЦИИ

по организации парольной защиты

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями пользователей при работе с паролями возлагается на заместителя начальника управления образования либо специалиста на которого, согласно приказу начальника управления образования возложены обязанности по защите информации.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ (сокращенно автоматизированное рабочее место) и т.д.), а также общепринятые сокращения (ЭВМ (сокращенно электронно-вычислительная машина), ЛВС (сокращенно локальная вычислительная сеть), USER (сокращенное общепринятое пользователь) и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому.

В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры по смене паролей в зависимости от полномочий владельца скомпрометированного пароля.

Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у заместителя начальника управления образования, либо у ответственного за информационную безопасность или у начальника управления образования в опечатанном личной печатью пенале.