

Приложение
к приказу МБОУ «ЦО №32»
от «20» 04 2023 г. № 39-202

Инструкция
по организации парольной защиты
в информационных системах МБОУ «ЦО №32»

1. Инструкция по организации парольной защиты в информационных системах МБОУ «ЦО №32» регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах МБОУ «ЦО №32», а также контроль за действиями пользователей при работе с паролями.
2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) информационных систем МБОУ «ЦО №32» и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение защиты персональных данных в информационных системах МБОУ «ЦО №32» (далее Ответственный).
3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АРМ самостоятельно с учетом следующих требований:
 - 3.1. Длина пароля должна быть не менее 7 символов;
 - 3.2. В числе символов пароля необходимо использовать буквы в верхнем и/или нижнем регистрах и цифры;
 - 3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.);
 - 3.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3-х позициях;
 - 3.5. Личный пароль пользователь не имеет права сообщать никому.
4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного.

6. Для генерации стойких значений паролей могут применяться специальные программные средства.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 180 дней.

8. Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя в случае прекращения его полномочий (увольнение и т. п.) должна производиться Ответственным немедленно после окончания последнего сеанса работы данного пользователя с системой.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Ответственного.

10. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 8 или п. 9 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

11. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного или руководителя подразделения в опечатанном личной печатью (штампом организации) конверте.