«Утверждаю»
Директор школы
Е.С. Мириуца

ПРИЛОЖЕНИЕ 5 к приказу
№___ от_____
об организационных мерах для
защиты персональных данных

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированных системах МБОУ Великооктябрьская СОШ (АС), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах МБОУ Великооктябрьская СОШ и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора сети

1. Требования, выполнение которых обязательно при назначении паролей:
   1.1 Пароль должен состоять не менее чем из шести символов.
   1.2 В пароле должны присутствовать символы из следующих категорий:
   строчные буквы английского алфавита от "a" до "z" (всего 26 символов);
   прописные буквы английского алфавита от "A" до "Z";
   десятичные цифры от "0" до "9";
   символы, не принадлежащие к алфавитно-цифровому набору (всего 68 символов).
   1.3 Использование трех и более символов, набранных в одном регистре, идущих подряд на клавиатуре, недопустимо.
   1.4 Использование трех и более символов, набранных в одном регистре, идущих подряд в алфавитном порядке, недопустимо.
   1.5 Использование двух и более одинаковых символов, набранных в одном регистре, идущих подряд, недопустимо.
   1.6 Задание пароля, совпадающего с одним из трех последних паролей, недопустимо.
   1.7 Пароль не должен содержать букв русского алфавита.
   1.8 Пароли должны быть случайны, насколько это возможно, и не связаны каким-либо образом с конкретным пользователем, например, с его именем, датой его рождения и т.п.

2. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на сотрудников. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих сотрудников, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений МБОУ Великооктябрьская СОШ (исполнителей).

3. При наличии в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов

(пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного представителя службы обеспечения безопасности информации (лицо, ответственное за организацию обработки и защиты ПДн).

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц. Смена технологических пароля производится не реже, чем 1 раз в 360 дней.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа МБОУ Великооктябрьская СОШ должна производиться администратором немедленно после окончания последнего сеанса работы данного пользователя с системой.

6. Внеплановая смена технологических паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа МБОУ Великооктябрьская СОШ и другие обстоятельства) сотрудников, которым по роду работы были предоставлены эти пароли.

7. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

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

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора сети, периодический контроль – на лицо, ответственное за организацию обработки и защиты ПДн.