Приложение 15
к приказу МБОУ СОШ №3
от 07.04.2017 №181

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных Муниципального бюджетного общеобразовательного учреждения «Средняя общеобразовательная школа №3»

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в МБОУ СОШ №3, а также контроль за действиями пользователей при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

Личные пароли должны генерироваться и распределяться централизованно (на сервере) либо выбираться пользователями 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, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- личный пароль пользователь не имеет права сообщать никому, кроме ответственного за обеспечение безопасности персональных данных.

В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за обеспечение безопасности персональных данных.

Полная плановая смена паролей пользователей должна проводиться регулярно, например, не реже одного раза в месяц.

Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться ответственным за обеспечение безопасности персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

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

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.