Приложение 3
к приказу от _____№____

УТВЕРЖДАЮ
Директор
МАОУ СОШ № 45
города Тюмени
_____ О.А. Филиппова
«09» _____ 2018 г.

ИНСТРУКЦИЯ
по организации парольной защиты в МОУ СОШ № 45 города Тюмени

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в автоматизированной системе (АС) объекта информатизации, а также контроль за действиями пользователей при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС и контроль за действиями пользователей при работе с паролями возлагается на администратора защиты.
2. Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:
   - длина пароля должна быть не менее 6 символов;
   - в числе символов пароля *обязательно должны присутствовать* буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
   - символы паролей для рабочих станций, на которых установлено средство защиты информации от НСД, должны вводиться в режиме латинской раскладки клавиатуры;
   - 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.);
   - при смене пароля новое значение должно отличаться от предыдущего;
   - пользователь не имеет права сообщать личный пароль другим лицам.

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.

3. При наличии, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, 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

администратору защиты или руководителю подразделения, эксплуатирующего технические средства. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у пользователей).

4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.
5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором защиты немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.
6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора защиты.
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. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора защиты.