Приложение № 9
к приказу МОУ СШ № 6
от «30» 08 2018 г. № 57/1-0

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных в МОУ СШ № 6

1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее - ИСПДн) МОУ СШ № 6 (далее - Школа»), а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн Школы и контроль действий исполнителей и обслуживающего персонала ИСПДн при работе с паролями возлагается на ответственного за обеспечение безопасности ПДн, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДн 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 и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- 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 уполномоченных сотрудников. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников Школы.

6. 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 передавать на хранение ответственному за информационную безопасность подразделения. Опечатанные конверты с паролями исполнителей должны храниться в недоступном месте.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.

8. Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение), должна производиться ответственным за обеспечение

безопасности ПДн немедленно после окончания последнего сеанса работы данного пользователя с системой.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Школы и другие обстоятельства ответственного за информационную безопасность и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

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

11. Повседневный контроль действий исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за информационную безопасность.