Приложение № 4
к приказу от 01.09.2015 №110
Рассмотрено и принято в качестве локального акта школы
на Совете трудового коллектива, протокол от 19.05.2015 г. № 3

ИНСТРУКЦИЯ

по организации парольной защиты КАИС КРО

Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы № 403 Пушкинского района Санкт-Петербурга

Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в КАИС КРО, а также контроль за действиями пользователей и обслуживающего персонала при работе с паролями:

1 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах КАИС КРО и контроль действий пользователей и обслуживающего персонала ИС при работе с паролями возлагается на Администратора безопасности информации КАИС КРО.

2 Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС 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 легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), даты рождений, свое имя и имена близких людей, а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем на 4 символа;
- личный пароль пользователь не имеет права сообщать никому.

3 Владельцы паролей (пользователи ИС) должны быть ознакомлены под подпись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4 В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности информации КАИС КРО. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

Система централизованной генерации и распределения паролей должна исключать возможность ознакомления ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений КАИС КРО.

5 Личные пароли (вместе с именами соответствующих учетных записей) сотрудники передают на хранение ответственному за информационную безопасность. Опечатанные конверты с паролями исполнителей должны храниться в сейфе.

6 Хранение сотрудниками значений своих паролей на бумажном носителе допускается только в сейфе у ответственного за безопасность информации.

7 В случае возникновения нештатных ситуаций или технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, конверты вскрываются с разрешения руководителя.

8 После выхода отсутствующего сотрудника на работу он обязан сразу же произвести смену пароля и передать его новое значение в запечатанном конверте на хранение ответственному за безопасность информации.

9 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода.

10 Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться Администратором безопасности информации КАИС КРО, немедленно после окончания последнего сеанса работы данного пользователя с системой.

11 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу) Администратора безопасности информации и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем СЗИ КАИС КРО.

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

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