Приложение 17 к приказу № 198 от 01.09.2025 г.

Инструкция
по организации парольной защиты
в МОУ «Средняя школа № 8 имени Н.Г. Варламова»

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

1. Организационное и техническое обеспечение процессов генерации, использование и прекращение действия паролей во всех подсистемах АС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ПД.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать латинские буквы и цифры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, 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 3 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены о дисциплинарной ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. При наличии технологической необходимости в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же сменить свой пароль.

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

5. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками отдела информационных технологий немедленно после окончания последнего сеанса работы данного пользователя с системой.

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

7. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе (возможно вместе с персональными ключевыми дискетами и ЭЦП).