

**Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа №3»**

Утверждаю
Директор МБОУ СОШ №3
_____ М.А.Садыкова

ПОЛОЖЕНИЕ

**о парольной защите при обработке персональных данных
и иной конфиденциальной информации**

1. Общие положения

1.1. Введение:

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия пользователей и обслуживающего персонала при работе с паролями

1. 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 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.

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.

2. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на сотрудников, ответственных за организацию работы АИС в школе. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

3. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей сообщать руководителю их новые значения.
4. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал.
5. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться сотрудниками, отвечающими за работу АИС немедленно после окончания последнего сеанса работы данного Пользователя с системой.
6. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.
7. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.
8. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и

3. Роли и ответственность

Пользователи:

- 3.1 Исполняют требования положения и несут ответственность за ее нарушение.
- 3.2 Информировывают администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.

4. Администратор парольной защиты:

- 4.1 Принимает обращения пользователей по вопросам парольной защиты (например, блокировка учетных записей, нарушение положения и др.), ведет их учет.
- 4.2 Организует консультации пользователей по вопросам использования парольной защиты.
- 4.3 Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.
- 4.5 Отвечает за безопасное хранение паролей встроенных административных учетных записей.