Приложение №11
УТВЕРЖДЕНО
приказом директора МАОУ СОШ №2
от 26.07.2023 № 52

ПОЛОЖЕНИЕ

об организации парольной защиты в информационных системах в образовательном процессе в муниципальном автономном общеобразовательном учреждении

«Средняя общеобразовательная школа №2»

1. Общие положения

1.1 Положение по организации парольной защиты в информационных системах МАОУ СОШ №2 регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах МАОУ СОШ №2, а также контроль за действиями пользователей при работе с паролями.

1.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) информационных систем МАОУ СОШ №2 и контроль за действиями пользователей при работе с паролями возлагается на ответственного за обеспечение защиты информации в информационных системах МАОУ СОШ №2 (далее – Ответственный).

2. Требования к организации парольной защиты в информационных системах

2.1 Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями АРМ самостоятельно с учетом следующих требований:

2.2 Длина пароля должна быть не менее 7 символов;

2.3 В числе символов пароля необходимо использовать буквы в верхнем и/или нижнем регистрах, цифры и специальные символы;

2.4 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.);

2.5 При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3-х позициях;

2.6 Личный пароль пользователь не имеет права сообщать никому.

2.7 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.

2.8 В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного.

2.9 Для генерации стойких значений паролей могут применяться специальные программные средства.

2.10 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 90 дней.

2.11 Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя в случае прекращения его полномочий (увольнение и т. п.) должна производиться Ответственным немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.12 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Ответственного.

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

2.14 Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного или начальника в опечатанном личной печатью (штампом организации) конвертами Школы.