Муниципальное бюджетное общеобразовательное учреждение «Центр образования № 49»

ПРИКАЗ

От 17 ноября 2021 г. **№67-4-а**

Об утверждении инструкции по организации парольной защиты в информационных системах МБОУ ЦО № 49

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными и методическими документами Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации, на основании Устава МБОУ ЦО № 49:

1. Утвердить инструкцию по организации парольной защиты в информационных системах МБОУ ЦО № 49 (приложение).
2. Контроль за исполнением настоящего приказа возложить на руководителя МБОУ ЦО № 49
3. Приказ вступает в силу со дня подписания.

Директор
МБОУ ЦО № 49 О.Е. Плошкина

Приложение
к Приказу МБОУ ЦО № 49
от «17» ноября 2021г. № 67-4-а

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах
МБОУ ЦО № 49

1. Инструкция по организации парольной защиты в информационных системах МБОУ ЦО № 49 (далее – ИС) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИС МБОУ ЦО № 49, а также контроль за действиями пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) и серверах в ИС МБОУ ЦО № 49, а также контроль за действиями пользователей при работе с паролями возлагается на лицо, ответственное за обеспечение защиты персональных данных, и администратора безопасности (далее – АБ).

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

3.1. Длина пароля должна быть не менее 6 символов;

3.2. В числе символов пароля необходимо использовать буквы в верхнем и/или нижнем регистрах и цифры, алфавит пароля не менее 70 символов;

3.3. 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.);

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

3.5. 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 АБ.

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

7. Полная плановая смена паролей пользователей должна проводиться регулярно, не более чем через 90 дней.

8. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае

достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут.

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

10. В случае прекращения полномочий (увольнение и другие обстоятельства) АБ должна производиться внеплановая полная смена паролей всех пользователей.

11. 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.

12. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у АБ или руководителя подразделения в опечатанном личной печатью (штампом организации) конверте.

Лист ознакомлений

№	ФИО	Должность	Дата	Подпись