Приложение № 4
к приказу ГБОУ гимназии № 1 г. Новокуйбышевска
от 31.12.2019 г. № 104/07 -од
«Об утверждении локальных актов»

УТВЕРЖДЕНО
приказом ГБОУ гимназии №1
г. Новокуйбышевска
от 31.12.2019 г. № 104/07-од

Директор
Л.Г. Слепцова

Инструкция
по организации парольной защиты

1. Общие положения

1.1. Настоящая Инструкция по организации парольной защиты (далее – Инструкция) устанавливает порядок и правила генерации, использования паролей в информационных системах в государственном бюджетном общеобразовательном учреждении Самарской области гимназии № 1 им. Н.И. Ферапонтова города Новокуйбышевска городского округа Новокуйбышевск Самарской области (далее – образовательная организация) и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих АС, за ее выполнение.

1.2. Требования настоящей Инструкции распространяются на всех сотрудников образовательной организации, эксплуатирующих и сопровождающих АС.

1.3. Бесконтрольность в определении и использовании паролей может повлечь риск несанкционированного доступа к информации образовательной организации, повлечь мошеннические и другие действия в информационных системах, которые могут нанести материальный вред и ущерб репутации образовательной организации.

2. Требования к паролям

2.1. Пароли не должны основываться на каком-либо одном слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок, номере телефона и т.д.

2.2. Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов, например, таких, как: qwerty, 1234567, abcdefgh и т.д.

2.3. Пароли должны содержать символы как минимум из трех следующих групп:

- строчные латинские буквы: abcd...xyz;
- прописные латинские буквы: ABCD...XYZ;
- цифры: 123...90;
- специальные символы: !%() _+ и т.д.

2.4 . Требования к длине пароля:

- для обычных пользователей - не менее 6 символов;
- для администраторов - не менее 8 символов;

2.5 Периодичность смены пароля:

- административные – каждые 60 дней;
- пользовательские– каждые 90 дней;

2.6. Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (*локальная вычислительная сеть, интернет, электронная почта*).

2.7. Пароли нельзя записывать на бумагу, в память телефона и т.д. Нельзя сообщать, передавать кому-либо пароль.

2.8 В ходе внутреннего аудита администратором информационной безопасности не реже двух раз в год возможна проверка соответствия пароля требованиям данной инструкции в присутствии пользователя: пользователь называет свой пароль, а проверяющий осуществляет ввод пароля и его проверку. После такой проверки требуется обязательная и немедленная смена пароля.

2.9. Пароли сервисных идентификаторов должны входить в процедуру управления паролями УА, включающую хранение их в защищенном месте периодическую смену (*1 раз в год*).

3. Ответственность

3.1 Виновные в нарушении условий настоящей Инструкции несут ответственность в соответствии с законодательством Российской Федерации, трудовым договором, должностной инструкцией.