Муниципальное автономное общеобразовательное учреждение
«Средняя общеобразовательная школа № 14»
650040, г. Кемерово, ул. Дружбы, 7. E-mail: kemnov-school@yandex.ru
тел./факс: 8384-238-58-25

Приказ

10.01.2022 г. **№ 2/1**

«Об утверждении Положения по организации парольной защиты в информационных системах МАОУ «Средняя общеобразовательная школа № 14» г. Кемерово

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 2021 года № 1119 «Об утверждении требований к защите персональных данных при 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 МАОУ «Средняя общеобразовательная школа №14»

ПРИКАЗЫВАЮ:

1. Утвердить Положение по организации парольной защиты в информационных системах МАОУ «Средняя общеобразовательная школа № 14» (Приложение № 1).
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МАОУ
«Средняя общеобразовательная школа № 14» И.Е. Косарева

УТВЕРЖДАЮ:
Директор МАОУ ««Средняя
общеобразовательная школа №14»
_____И.Е. Косарева
«10 » января 2022 г.

Приложение № 1
к Приказу № 2/1 от 10.01.2022 г.
«Об утверждении Положения по организации
парольной защиты в информационных системах
МАОУ «Средняя общеобразовательная школа № 14»

Инструкция
по организации парольной защиты в информационной системе
«Электронная школа 2.0» МАОУ «Средняя общеобразовательная школа № 14»

1. Требования к организации парольной защиты

1.1. Формирование и учет паролей по доступу к личному кабинету гражданина Кемеровской области (далее – личный кабинет) в информационной системе «Электронная школа 2.0» осуществляется Конешовой С.С., заместителем директора по УВР (далее - администратор безопасности), назначенной приказом МАОУ «Средняя общеобразовательная школа № 14» как лицо, ответственное за сохранность логинов и паролей в информационной системе «Электронная школа 2.0».

1.2. Устанавливаемые пароли **пользователей** должны соответствовать следующим требованиям:

- длина пароля должна быть не менее 8 символов;
- пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы);
- использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;
- использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;
- новое значение пароля не должно совпадать с одним из четырех предыдущих значений;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учетной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

1.3. Устанавливаемые пароли для **администратора безопасности** должны соответствовать следующим требованиям:

- длина пароля должна быть не менее 8 символов;
- пароль должен содержать строчные и прописные буквы, а также небуквенные символы (цифры, знаки пунктуации, специальные символы);
- использование трех и более, подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;

– использование в качестве пароля одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов недопустимо;

– новое значение пароля не должно совпадать с одним из четырех предыдущих значений;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования автоматизированного рабочего места, имя учетной записи или какую-либо его часть, общепринятые сокращения (password, USER, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;

– запрещается регистрировать пользователей в ИС под своим паролем;

1.4. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом администратору безопасности и изменить пароль.

1.5. Восстановление забытого пароля пользователя осуществляется администратором безопасности.

1.6. Для предотвращения несанкционированного доступа в операционную систему должен быть реализован механизм блокировки учетной записи при трехкратном неправильном вводе пароля, разблокировку учетной записи производит администратор безопасности.

1.7. Пользователи и администраторы ИС обязаны:

– сохранять в тайне свой личный пароль;

– четко знать и строго выполнять требования настоящей Инструкции;

– своевременно сообщать лицу, ответственному за защиту информации в ИС, обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

1.8. При организации парольной защиты запрещается:

– умышленное и неумышленное несанкционированное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;

– запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками месте;

– сохранение паролей в браузерах и на АРМ пользователей.

– вход в систему с использованием чужих идентификаторов или паролей;

– сообщать посторонним лицам, в том числе сотрудникам МАОУ «Средняя общеобразовательная школа № 14», свои пароли, а также пересылать открытым текстом в электронных сообщениях.

2. Порядок применения парольной защиты

2.1. Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к личному кабинету.

2.2. Набор личного пароля следует проводить, предварительно убедившись в отсутствии лиц, которые могут его увидеть.

2.3. При временном отсутствии на рабочем месте следует произвести блокировку компьютера.

2.4. Смена личных паролей пользователей осуществляется администратором безопасности ИС.

Внеплановая смена (удаление) личного пароля любого пользователя производится в следующих случаях:

– по окончании срока действия пароля;

– в случае прекращения полномочий пользователя (увольнение);

– при обнаружении факта успешной попытки несанкционированного доступа к элементам ИС;

– при обнаружении факта компрометации пароля.

2.5. Внеплановая полная смена паролей всех пользователей, а также паролей по доступу к базовым системам ввода вывода компьютеров, настройкам сетевого оборудования, настройкам операционных систем по запуску специализированного программного обеспечения, предназначенного для обработки защищаемой информации, настройкам средств защиты информации, должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности ИС.

2.6. Скомпрометированные пароли выводятся из действия немедленно.

2.7. По каждому случаю, связанному с компрометацией действующих паролей, ответственным за защиту информации в ИС организуется и проводится служебная проверка.

2.8. Результаты служебной проверки в виде служебной записки предоставляются руководству МАОУ «Средняя общеобразовательная школа № 14». По результатам проверки лица, допустившие разглашение паролей, привлекаются к дисциплинарной ответственности.

2.9. 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.

2.10. Контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности ИС.