

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 2»
МУНИЦИПАЛЬНЫЙ ОБРАЗОВАТЕЛЬНЫЙ ОКРУГ СИМФЕРОПОЛЬ
РЕСПУБЛИКИ КРЫМ**

Принято на заседании
педагогического совета
Протокол № 12
От 30.08.2018 г.

УТВЕРЖДЕНО
Директор МБОУ «Средняя
общеобразовательная школа № 2»
В.А. Кухнина
Приказ № 429 от 31.08.2018 г.
«Об утверждении организационно-
распорядительной документации по обработке
персональных данных в МБОУ «СОШ № 2» г.
Симферополя»

**ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах
МБОУ «СОШ № 2» г. Симферополя**

1. Настоящая инструкция по организации парольной защиты в информационных системах МБОУ «СОШ № 2» г. Симферополя определяет порядок аутентификации работников с использованием паролей на автоматизированных рабочих местах (далее - АРМ), базах данных, сетевом и коммутационном оборудовании, средствах защиты информации, в том числе средствах криптографической защиты информации, входящих в состав информационных систем МБОУ «СОШ № 2» г. Симферополя (далее - ИС), а также контроль действий пользователей при работе с паролями и идентификаторами.

2. Применение парольной защиты необходимо для проведения аутентификации пользователя при доступе к ИС и является частью многофакторной системы аутентификации пользователей.

3. Аутентификация пользователей с использованием пароля должна применяться при доступе пользователей ко всем элементам ИС (АРМ, базы данных, сетевое и коммутационное оборудование, средства защиты информации, в том числе средства криптографической защиты информации).

4. Пароли должны отвечать следующим требованиям:

- длина пароля должна быть не менее 8-ми символов и не может превышать 16-ти символов;
- пароль должен содержать заглавные латинские символы, строчные латинские символы, цифры, специальные символы (например «, %, ! 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, АРМ, и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

5. Максимальное количество неуспешных попыток аутентификации до блокировки должно составлять 8 попыток.

6. Блокировка программно-технического средства или учетной записи после превышения количества неуспешных попыток аутентификации должна осуществляться на период времени от 10 до 30 минут.

7. Плановая смена паролей должна проводиться регулярно, но не реже одного раза в 60 дней.

8. Внеплановая полная смена паролей должна производиться в случае компрометации паролей, прекращения полномочий в связи с увольнением, переходом на другую работу внутри МБОУ «СОШ № 2» г. Симферополя, и других обстоятельствах лиц, осуществляющих администрирование ИС, баз данных, сетевого и коммутационного оборудования, средств защиты информации, в том числе средств криптографической защиты информации.

9. Администраторы информационной безопасности МБОУ «СОШ № 2» после плановой или внеплановой смены паролей должны предоставить информацию о паролях директору МБОУ «СОШ № 2» г. Симферополя или лицу его замещающему. При этом пароли на бумажном носителе помещаются в запечатанный непрозрачный конверт, на лицевой стороне которого указывается Ф.И.О. работника, осуществившего смену пароля, наименование элемента ИС, дата изменения. Хранение конвертов с паролями осуществляется в запираемом сейфе в помещении, исключающем несанкционированное нахождение в нем третьих лиц.

10. Администраторы информационной безопасности МБОУ «СОШ № 2» г. Симферополя несут персональную ответственность за реализацию и выполнение требований настоящей Инструкции.

11. Работники МБОУ «СОШ № 2» г. Симферополя несут персональную ответственность за все действия, совершенные под их учетными записями, если ими не доказан факт несанкционированного их использования и отсутствия нарушений ими требований нормативных актов в сфере защиты информации.

12. Работники МБОУ «СОШ № 2» г. Симферополя обязаны своевременно сообщать администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и сроков их действия.

13. При вводе пароля работники МБОУ «СОШ № 2» г. Симферополя обязаны придерживаться следующих правил:

– ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

- при вводе пароля необходимо отключить возможность системы автоматически сохранять пароли;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и т.п.).

14. Хранение работниками МБОУ «СОШ № 2» г. Симферополя паролей должно исключать ознакомление с ними посторонних лиц.

15. Работникам МБОУ «СОШ № 2» г. Симферополя запрещается:

- использовать один и тот же пароль для доступа к различным информационным ресурсам;

- сообщать пароль кому-либо, без письменного разрешения администратора информационной безопасности;

- при вводе пароля для доступа к информации, размещенной в информационных системах, запрещается использовать клавиатуры и другие средства ввода, подключенные к средствам вычислительной техники по беспроводным технологиям, в том числе по технологии Bluetooth или с использованием инфракрасных передатчиков;

- ввод пароля в области непосредственного действия диктофонов, камер видеонаблюдения, средств телефонной связи в состоянии вызова, других устройств визуальной или акустической регистрации ввода парольных данных;

- при вводе пароля запрещается произносить вслух набираемый текст или части парольной фразы;

- запрещается сообщать другим работникам личный пароль и регистрировать их в системе под своей учетной записью;

- запрещается передача паролей работникам МБОУ «СОШ № 2» г. Симферополя при помощи почтовых сообщений либо иным другим открытым способом через информационно-телекоммуникационную сеть «Интернет».

Пронумеровано, прошито и скреплено печатью

3/мпу /сссга

Директор МБОУ «СОШ №2»
Г. Симферополь

В. А. Кухнина

