Рассмотрено и рекомендовано к утверждению на педагогическом совете № 1 от 21.08. 2018 г.

Согласовано.
Председатель поп: _____
/Умникова Н.Л./

Утверждаю. 21.08.2018г. пр. №88
Директор школы: _____
/Новикова О. Н./

ПОЛОЖЕНИЕ О ПАРОЛЬНОЙ ЗАЩИТЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

МУНИЦИПАЛЬНОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «ФЕДОРОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»

1.Общие положения

1.1. Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (ИС) МБОУ «Федоровская средняя общеобразовательная школа» (далее школа), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.
1.2. Данное Положение разработано в соответствии с Конституцией РФ, Федеральным законом «Об образовании в Российской Федерации» от 29.12.2012г. №273 –ФЗ, Федеральным законом РФ «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006г., Федеральным законом РФ» О персональных данных» №152-ФЗ от 27.07.2006г., Указом президента РФ «Об утверждении перечня сведений конфиденциального характера» №188 от 06.03.1997г., уставом школы.
1.3.Цель
Положение определяет требования школы к парольной защите информационных систем.
1.4.Область действия
Положение распространяется на всех пользователей и информационные системы (далее –ИС) ОУ, использующих парольную защиту.
1.5.Термины и определения
ИС – в данном случае любая информационная система, для работы с которой необходима аутентификация пользователя.
Пароль – секретный набор символов, используемый для аутентификации пользователя.
Пользователи –администраторы ИС и работники школы или сторонней организации, которым предоставлен доступ к ИС школы, а также корпоративный доступ к ресурсам сети Интернет.
Учетная запись –идентификатор пользователя, используемый для доступа к ИС.

2.Основные положения

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на сотрудников школы работающих с автоматизированными информационными системами.
2.2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % 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, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

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.

2.3. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на сотрудников школы работающих с автоматизированными информационными системами. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления сотрудников школы работающих с автоматизированными информационными системами с паролями других сотрудников школы.

2.4. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей передавать на хранение руководителю их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте. Опечатанные конверты с паролями Пользователей должны храниться в сейфе. Для опечатывания конвертов должны применяться личные печати владельцев паролей (при их наличии у Пользователей), либо печать школы.

2.5. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в год.

2.6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного Пользователя с системой.

2.7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

2.8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

2.9. Хранение Пользователем своих паролей на бумажном носителе допускается только в сейфе у руководителя школы в опечатанном печатью конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).
2.10. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителя школы, периодический контроль – возлагается на сотрудников школы работающих с автоматизированными информационными системами.

3.Роли и ответственность

3.1.Пользователи:
3.1.1.Исполняют требования положения и несут ответственность за ее нарушение.
3.1.2.Информируют администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.
3.2.Администратор парольной защиты:
3.2.1.Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных записей, нарушение положения и др.).
3.2.2.Организует консультации пользователей по вопросам использования парольной защиты.
3.2.3.Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.
3.2.4.Отвечает за безопасное хранение паролей встроенных административных учетных записей.