Принято:
Решением Педагогического совета
ГБОУ СОШ №1 «ОЦ» им.
В. И. Фокина с. Большая Глушица
Протокол от 31.08.15 № 1

Утверждено:
приказом директора
ГБОУ СОШ №1 «ОЦ» им.
В. И. Фокина с. Большая Глушица
от 01.09.15 № 277-од
Директор школы
Уколова С.М. Уколова

Политика паролей государственного бюджетного общеобразовательного учреждения Самарской области средней общеобразовательной школы №1 «Образовательный центр» имени Героя Советского Союза В.И. Фокина с. Большая Глушица муниципального района Большеглушицкий Самарской области, используемых для входа в Автоматизированную систему управления региональной системой образования (АСУ РСО)

Пароль - это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты информации от несанкционированного доступа (***Несанкционированный доступ*** - доступ к закрытой для публичного использования информации со стороны лиц, не имеющих разрешения на доступ к этой информации.). В большинстве информационных систем комбинация «имя пользователя - пароль» используется для удостоверения пользователя.

Политика распространяется на всех пользователей информационных систем, которые имеют учетные записи или назначены ответственными за таковые. А также на сотрудников хранящих конфиденциальную информацию организации.

Характеристики слабого (ненадежного) пароля:

- содержит менее 8 символов;

- слово из словаря;
- повседневно используемое слово, например, имена или фамилии друзей, коллег, актеров или сказочных персонажей, клички животных;
- компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;
- вариации наименования компании или торговой марки;
- день рождения или другая персональная информация, например, адрес, номер телефона и т.п.;
- регулярные последовательности символов и цифр, например, 111222, abcde, qwerty и т.п.;
- что-либо из вышеперечисленного в обратном написании;
- что-либо из вышеперечисленного с добавлением цифр в начале или конце.

Пример слабого пароля: ***ABCD1***

Характеристики стойкого пароля:

- содержит прописные(A-Z) и строчные буквы(a-z);
- содержит цифры и символы;
- более 8 символов длиной;
- не является словом ни на одном из языков, диалектов, жаргонов, слэнгов;
- не основывается на персональной информации;
- не записан в бумажной или электронной форме.

Пример стойкого пароля: ***Rh4yi39f8***

Защита паролей

Для учетных записей пользователей запрещено использовать тот же самый пароль, что и для других информационных систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.). По возможности не используйте один и тот же пароль для различных корпоративных систем. Также необходимо использовать различные пароли в операционных системах Linux и Windows.

Запрещено сообщать пароль кому бы то ни было, включая административный персонал и секретарей. Все пароли являются конфиденциальной информацией.

Список запрещенных действий с паролями:

- никому не сообщайте пароль по телефону;
- не указывайте пароль в сообщениях электронной почты;
- не сообщайте пароль вашему руководству (исключение делается для первичного пароля);
- не сообщайте принципы создания пароля (например, "на основе моей фамилии");
- не сообщайте пароль в электронных опросах и незнакомых формах авторизации;
- не сообщайте пароль членам семьи и родственникам;
- не передавайте пароль коллегам на время вашего отпуска.

Общие рекомендации при работе на компьютере при обработке конфиденциальной информации в т.ч. персональных данных.

1) На компьютере должна быть включена защищенная паролем заставка, активирующаяся через 10 минут бездействия пользователя. Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер.

2) При работе в АСУ РСО, экран монитора должен быть скрыт от посторонних глаз. Если помещение с ПК находится на 1 этаже здания, на окнах должны быть установлены шторы, жалюзи и т.п.

3) Никто из посторонних не должен находится за спиной во время работы с персональными данными в АСУ РСО.

4) Не записывайте пароли на бумагу. Не сохраняйте пароли в файлах на каком-либо носителе (например, флэшка, мобильный телефон и т.п.) без шифрования.

5) Пароль должен изменяться не менее одного раза в 42 дня, для системных учетных записей раз в три месяца. Рекомендованный интервал

смены пароля 30 дней. Если вы подозреваете, что ваш пароль стал известен кому-либо - немедленно измените его.

Ответственность

Согласно ст. 24 Федерального закона «О персональных данных» на лиц, виновных в нарушении его требований, возлагается гражданская, уголовная, административная, дисциплинарная и иная предусмотренная законодательством РФ ответственность.