УТВЕРЖДАЮ

Директор МБОУ СОШ №26

_____ Н.А.Шишкин

«12» сентября 2018 г.

Инструкция
по организации парольной защиты в МБОУ СОШ №26

г.Ставрополь
2018 г.

I. Общие положения

1. Инструкция по организации парольной защиты (далее - Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах образовательного учреждения (далее - ОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее - ИС) ОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора ОУ или лаборанта.

II. Правила формирования паролей

1. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, $, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abed и т. д.), общепринятые сокращения (ЭВМ, ЛВС, USER, и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственных лиц.

III. Ввод пароля

1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

IV. Порядок смены личных паролей

1. Смена паролей проводится регулярно, не реже одного раза в пол года.

2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

3. Срочная (внеплановая) полная смена паролей производится в случае прекраще-

ния полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 5 (IV) Инструкции.

5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

V. Хранение пароля

1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.

2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

VI. Действия в случае утери и компрометации пароля

1. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 9 или 10 (IV) Инструкции.

VII. Ответственность при организации парольной защиты

1. 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 информации о пароле.

2. Ответственность за организацию парольной защиты в структурных подразделениях ОУ возлагается на системного администратора.

3. Работники ОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ОУ, должны быть ознакомлены с инструкцией.

С инструкцией ознакомлены: