

«УТВЕРЖДЕНО»

Заведующая МБДОУ ДСКВ № 25

«Пчёлка»



Г.И.Зимовец

## **ИНСТРУКЦИЯ**

### **по организации парольной защиты доступа к информационным ресурсам, содержащим персональные данные.**

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) доступа к информационным ресурсам локальной вычислительной сети муниципального бюджетного дошкольного образовательного учреждения детского сада комбинированного вида № 25 «Пчёлка» ст. Брюховецкой муниципального образования Брюховецкий район (ЛВС) и информационных подсистем, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями сотрудников при работе с паролями возлагается на администратора системы или ответственного по защите персональных данных учреждения.

2. Личные пароли и имена входов на доступ в ЛВС должны назначаться и распределяться централизованно. Пароли на доступ в информационные системы распределяются централизованно либо выбираются пользователями подсистемы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 7 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, общепринятые наименования или сокращения, например, «ЭВМ», «User» и т.д.);
- при смене пароля новое значение должно отличаться от предыдущих значений пароля;
- личный пароль и имя входа пользователь должен хранить в секрете;

Владельцы паролей перед их получением должны быть предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение пароля и имени входа в ЛВС или информационную подсистему.

3. В случае, если формирование личных паролей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора системы ответственного по защите персональных данных учреждения.

4. Внеплановая смена личного пароля или удаление учетной записи пользователя ЛВС в случае прекращения его полномочий (увольнения, переход на другую работу внутри организации и т.п.) должна производиться администратором после окончания последнего сеанса работы данного пользователя с ЛВС или соответствующей системой.

5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) администратора, которому по роду работы были предоставлены полномочия по управлению парольной защитой доступа к ЛВС или информационной подсистеме.

6. В случае компрометации личного пароля пользователя ЛВС или информационной подсистемы должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного по защите персональных данных учреждения.