

УТВЕРЖДЕНО:

Заведующий МБДОУ д/с № 7

Н. А. Кузьмина

Приказ от «30» 05.2017 №50



## **ИНСТРУКЦИЯ по организации парольной защиты**

### **1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. 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 дошкольного образовательного учреждения (далее - ДОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

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

### **2. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ**

2.1. 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.

2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра дистанционного образования.

2.3. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями

исполнителей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

### **3. ВВОД ПАРОЛЯ**

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.).

### **4. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ**

4.1. Смена паролей проводится регулярно, не реже одного раза в три месяца.

4.2. 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.

4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения 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.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

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

### **5. ХРАНЕНИЕ ПАРОЛЯ**

5.1. 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.

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

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

### **6. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ**

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 4.3 или п. 4.4 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

### **7. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ**

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.2. Ответственность за организацию парольной защиты в структурных подразделениях ДОУ возлагается на системного администратора.

7.3. Работники ДОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ДОУ, должны быть ознакомлены с инструкцией под роспись.