УТВЕРЖДЕНО
приказом заведующего
МБДОУ ДС № 26
№ _214/01-05__
от 01.07. 2014 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее ИСПД) МБДОУ ДС №26, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПД и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности.

1. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

Личные пароли должны генерироваться и распределяться централизованно, либо выбираться пользователями информационной системы 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, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;
- личный пароль пользователь не имеет права сообщать никому.

В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их

формирования и распределения возлагается на администратора информационной безопасности.

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать администратора информационной безопасности.

2. ВВОД ПАРОЛЯ

При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.).

3. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

3.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

3.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п.3.1 настоящей инструкции, и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

3.5. Администратор информационной безопасности ведёт "Журнал принудительной смены личных паролей", в котором он отмечает причины внеплановой смены паролей пользователей.

3.6. Временный пароль, заданный администратором информационной безопасности при регистрации нового пользователя, следует изменить при первом входе в систему.

4. ХРАНЕНИЕ ПАРОЛЯ

4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

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

4.3. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора информационной безопасности, или руководителя подразделения в опечатанном личной печатью пенале.

5. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п.3.3 или п.3.4 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

6. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

6.1. 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 парольной информации.

6.2. Ответственность за организацию парольной защиты в подразделении возлагается на ответственных за информационную безопасность в подразделениях, периодический контроль – возлагается на администратора информационной безопасности.