МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ Г. МУРМАНСКА № 38

СОГЛАСОВАНО:
Председатель ОСТК
С.Г.Щур
Протокол от «01» 12 2017г. № 9

УТВЕРЖДЕНО:
приказом заведующего
МБДОУ г. Мурманска 38
приказ «01» 12 2017 № 68/3

ПОЛОЖЕНИЕ
О ПАРОЛЬНОЙ ЗАЩИТЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМЦИИ В МБДОУ Г. МУРМАНСКА 38

1.Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (ИС) МБДОУ г. Мурманска 38 (далее Оператора), а также контроль за действием Пользователей и лиц, ответственных при работе с паролями.

2. Организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей во всех ИС и контроль за действиями Пользователей и лиц, ответственных при работе с паролями возлагается на сотрудников, работающих с автоматизированными информационными системами (АИС) или иного уполномоченного лица – администраторов парольной защиты.

3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не 8 символов;
- в числе символов пароля 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, дата рождения и т.п.), а также общепринятые сокращения (ЭВМ, ЛВС, USER);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль Пользователь не имеет права сообщать никому.

4. 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.

5. В случае, если формирование личных паролей

пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников отдела АИС (или иного соответствующего подразделения (или уполномоченного лица) Оператора). Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников отдела АИС (или иного соответствующего подразделения (или уполномоченного лица) Оператора) с паролями других сотрудников подразделений Оператора.

6. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых сотрудников (Пользователей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей передавать на хранение заведующему Учреждения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте.

Опечатанные конверты с паролями Пользователей должны храниться в сейфе. Для опечатывания конвертов должна применяться печать Оператора.

7.Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал (или в иные установленные Оператором сроки).

8.Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченным лицом Оператора) немедленно после окончания последнего сеанса работы данного Пользователя с системой.

9.Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

10.В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 7 или п. 8 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

11.Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у заведующего Учреждением в опечатанном печатью конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).

12.Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на заведующего Учреждением, периодический контроль – возлагается на уполномоченное лицо Оператора – администраторов парольной защиты.