Муниципальное бюджетное дошкольное образовательное учреждение детский сад№ 15 «Казачок»

Принято Советом Учреждения
Протокол № У
« & » ^ / 2017г

Утверждаю:_____
Заведующий МБДОУ,д/с№15
Звягинцева' ШЗЗ.

ПОЛОЖЕНИЕ
о парольной защите при обработке персональных данных и иной конфиденциальной информации в МБДОУ д/с № 15 «Казачок»

Данное Положение регламентирует организационно-техническое обеспечение процессов л-.рации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (ИС) МБДОУ детском саду № 15 «Казачок» (далее Оператора), _ акже контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИС и контроль за действиями 11 ьзователей и обслуживающего персонала при работе с паролями возлагается на .; грудников школы работающих с автоматизированными информационными системами (ЛИС или иного соответствующего подразделения (или уполномоченного лица) статора) - администраторов парольной защиты.

I Личные пароли должны генерироваться и распределяться централизованно либо - - ^играться пользователями ИС самостоятельно с учетом следующих требований: • длина пароля до лжна быть не менее 8 символов; • в числе символов пароля обязательно должны - . . пвовахь бу квы в верхнем и нижнем регистрах, цифры и специальные символы (@, = $.£.*. °о и т.п.); пароль не должен включать в себя легко вычисляемые сочетания с нгм волов имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения ЛВМ. ЛВС. USER и т.п.); • при смене пароля новое значение должно отличаться от л польщу тле го не менее чем в 6 позициях; • личный пароль Пользователь не имеет права с 'лгать никому. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за исл льзование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. 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 дру гих сотрудников подразделений Оператора.

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 .мены своих паролей передавать на хранение руководителю своего подразделения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте. Опечатанные конверты с паролями Пользователей должны храниться в сейфе. Для опечатывания конвертов должны применяться личные печати владельцев паролей

при их наличии у Пользователей), либо 2 печать отдела АИС (или иного соответствующего подразделения (или уполномоченного лица) Оператора).

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

- Внеплановая смена личного пароля или удаление учетной записи Пользователя ПС в .лучае прекращения его полномочий (увольнение, переход на другую работу и т.п.) д окна производиться сотрудниками отдела АИС (или иного соответствующего : дразаеления (или уполномоченного лица) Оператора) немедленно после окончания следнего сеанса работы данного Пользователя с системой.

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 полис мсчия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п. 6 или п. 7 настоящего Положения в зависимости от пшоночнн владельца скомпрометированного пароля.

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

. вседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и нс ль звания возлагается на руководителей подразделений, периодический контроль - ъ а: ае с я на сотрудников отдела АИС (или иного соответствующего подразделения (или -омоченного лица) Оператора) - администраторов парольной защиты.