



УТВЕРЖДАЮ

Заведующая МБДОУ ЦРР «Д/с №21 «Кэнчээри»

Савинова Ж.Н.

Приказ №03 от 03.03.2019г.

ПОЛОЖЕНИЕ

О парольной защите при обработке персональных данных Иной конфиденциальной информации в МБДОУ ЦРР «Д/с № 21 «Кэнчээри»

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) организации, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в МБДОУ ЦРР - «Д/с № 21 «Кэнчээри» (далее – ОУ)

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действий паролей во всех ИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на сотрудников ОУ работающих с автоматизированными информационными системами (АИС или иного соответствующего подразделения (или уполномоченного лица) Оператора) – администратор парольной защиты.
2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:
 - длина пароля должна быть не менее 8 символов;
 - в числе символов пароля обязательно присутствовать буквы в верхних и нижних регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
 - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.)
 - при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
 - личный пароль Пользователь не имеет права сообщать никому.

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.

3. 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 руководителю своего подразделения их новые значения (вместо 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 печать отдела АИС (или иного соответствующего подразделения (или уполномоченного лица) Оператора).
4. Полная плановая смены паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал (или в иные установленные Оператором сроки).

5. 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 сотрудниками отдела АИС (или иного соответствующего подразделения (или уполномоченного лица) Оператора) немедленно после окончания последнего сеанса работы данного Пользователя с системой.
6. 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 защиты ИС.
7. В случае компрометации личного пароля Пользователя ИС должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.
8. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном личной печатью конверте.
9. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на сотрудников ДОУ, периодический контроль – возлагается на сотрудников отдела АИС (или иного соответствующего подразделения (или уполномоченного лица) Оператора) – администраторов парольной защиты, руководителя ДОУ.

Термины и определения

ИС – в данном случае любая информационная система, для работы с которой необходима аутентификация пользователя.

Пароль – секретный набор символов, используемый для аутентификации пользователя.

Пользователи – администраторы ИС и работники ДОУ или сторонней организации, которым предоставлен доступ к ИС ДОУ, а также корпоративный доступ к ресурсам сети Интернет.

Учетная запись – идентификатор пользователя, используемый для доступа к ИС.