Государственное бюджетное дошкольное образовательное учреждение детский сад № 74 присмотра и оздоровления Красногвардейского района Санкт-Петербурга

Согласовано
Председателем ПК ГБДОУ №74
_____ И.Г. Булавина
Протокол № _____
«04» 11 2013 г.

Утверждаю
Заведующий ГБДОУ № 74
_____ И.В. Васильева
Приказ № 105 от 14.11.2013
«05» ноября 2013 г.

Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации

Государственного бюджетного дошкольного образовательного учреждения детский сад №74 присмотра и оздоровления Красногвардейского района Санкт-Петербурга

2013

Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) организации (далее Оператора), а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. 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 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, 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.

2. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников отдела АИС. 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 с паролями других сотрудников подразделений Оператора.

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 сообщать руководителю их новые значения .

4. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал .

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 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 защитой ИС.
7. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).
8. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на сотрудников отдела АИС – администраторов парольной защиты.