

Утверждено
приказом по МАДОУ ЦРР –
детский сад №23 «Сказка»
№ 7/1 от 09.01.2019 г

ПОЛОЖЕНИЕ
о парольной защите при обработке
персональных данных и иной
конфиденциальной информации в МАДОУ
ЦРР - детский сад №23 «Сказка»

1. ОБЩИЕ ПОЛОЖЕНИЯ

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 Муниципальном автономном дошкольном образовательном учреждении Центре развития ребёнка - детский сад №23 «Сказка» (далее – МАДОУ). Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

Цель: Положение определяет требования МАДОУ к парольной защите информационных систем. Область действия Положения распространяется на всех пользователей и информационные системы (далее – ИС) МАДОУ, использующих парольную защиту.

2. 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 Общества или сторонней организации, которым предоставлен доступ к ИС Общества, а также корпоративный доступ к ресурсам сети Интернет. Учетная запись – идентификатор пользователя, используемый для доступа к ИС.

3. ПОЛОЖЕНИЯ

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; 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. 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. 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, отвечающими за работу ИС немедленно после окончания последнего сеанса работы данного Пользователя с системой. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у

руководителя в опечатанном конверте. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на заместителя заведующего.

4. РОЛИ И ОТВЕТСТВЕННОСТЬ

Пользователи: исполняют требования положения и несут ответственность за ее нарушение. Информировать администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения. Администратор парольной защиты: принимает обращения пользователей по вопросам парольной защиты. Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования. Отвечает за безопасное хранение паролей встроенных административных учетных записей.