



АДМИНИСТРАЦИЯ ЛЕЖНЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
ИВАНОВСКОЙ ОБЛАСТИ

МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДЕТСКИЙ САД ОБЩЕРАЗВИВАЮЩЕГО ВИДА «СКАЗКА»

155120, Ивановская область, поселок Лежнево, улица 3-я Свердлова, дом 5а,
тел. 8 (49357) 2-27-63, e-mail: dou.skazka@yandex.ru,
ОГРН 1023701649025/ ИНН 3715004425/ КПП 371501001

ПРИНЯТО

УТВЕРЖДАЮ

Педагогическим Советом

Заведующий

Протокол № 4

 М.В. Першина

от «10» апреля 20 19 г.

Приказ № 40-09
«14» апреля 20 19 г.



**ПОЛОЖЕНИЕ
О ПАРОЛЬНОЙ ЗАЩИТЕ
ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
И ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.**

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. «Положение о парольной защите при обработке персональных данных и иной конфиденциальной информации» (далее - Положение) в МКДОУ д/с общеразвивающего вида «Сказка» (далее - ДОО), регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (ИС) ДОО, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в ДОО.

1.2. Парольная защита требует соблюдения ряда правил, изложенных в настоящем Положении.

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

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ИС.

2.1. 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 ДОО или сторонней организации, которым предоставлен доступ к ИС ДОО, а также корпоративный доступ к ресурсам сети Интернет.

2.2. Учетная запись - идентификатор пользователя, используемый для доступа к ИС.

3. ПОЛОЖЕНИЯ.

3.1. 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;
- 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.

3.2. 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.

3.3. 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.

3.4. 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 работниками, отвечающими за работу ИС немедленно после окончания последнего 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 работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

3.5. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

3.6. 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.

4.1. Пользователи:

4.1.2. Исполняют требования положения и несут ответственность за ее нарушение.

4.1.3. Информировать администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.

4.2. Администратор парольной защиты:

4.2.1. Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных записей, нарушение положения и др.).

4.2.2. Организует консультации пользователей по вопросам использования парольной защиты. Контролирует действия Пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования.

4.2.3. Отвечает за безопасное хранение паролей встроенных административных учетных записей.