

Муниципальное бюджетное дошкольное образовательное учреждение детский сад общеразвивающего вида с приоритетным осуществлением художественно-эстетического развития детей Тунгокоченского района Забайкальского края

УТВЕРЖДАЮ

Заведующая МБДОУ

детский сад общеразвивающего вида

_____ Л.С.Куфарова

Приказ № 21-од от 01.04.2022 г

ПОЛОЖЕНИЕ

о парольной защите при обработке персональных данных и иной конфиденциальной информации в МБДОУ детский сад общеразвивающего вида

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах (далее - ИС) организации, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями в Муниципальном бюджетном дошкольном образовательном учреждении детский сад общеразвивающего вида с приоритетным осуществлением художественно-эстетического развития детей Тунгокоченского района Забайкальского края (далее – ДОУ).
- 1.2. Положение определяет требования ДОУ к парольной защите информационных систем. Область действия Положения распространяется на всех пользователей и информационные системы ДОУ, использующих парольную защиту.
- 1.3. Ознакомление всех работников ДОУ, использующих средства вычислительной техники, с требованиями положения проводит администратор, назначенный приказом руководителя ДОУ. При ознакомлении с Положением внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационная система (ИС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого

спектра угроз с целью обеспечения непрерывности бизнеса, минимизации рисков бизнеса и максимального увеличения возможностей бизнеса.

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

Пароль – секретный набор символов, используемый для аутентификации пользователя.

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

Ключевой носитель – электронный носитель (дискета, флэш- накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

3. ТРЕБОВАНИЯ К ПАРОЛЯМ

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, цифры и (или) специальные символы (@, #, \$, &, *, % и т.п.). Исключение составляют подсистемы ИС ДООУ, в которых использование подобных спецсимволов недопустимо;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (qwerty, pa\$\$w0rd, 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.

3.1. 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.

3.2. 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.

3.3. 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. 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.

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

3.5. При работе в корпоративной сети Интернет запрещается:

- Использовать интернет-контент, сохраняющий пароли;
- Оставлять открытым доступ к контенту, на котором были применены пароли или коды доступа.

3.6. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на администраторов, назначенных приказом руководителя ДОУ

.

4. ОТВЕТСТВЕННОСТЬ

4.1. Пользователи ИС ДОУ несут персональную ответственность за несоблюдение требований по парольной защите. Информировать администратора парольной защиты обо всех ставших им известных случаях нарушения настоящего положения.

4.2. Администратор парольной защиты:

- Принимает обращения пользователей по вопросам парольной защиты (например, блокировка четных записей, нарушение положения и др.).
- Организует консультации пользователей по вопросам использования 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.