

**Муниципальное дошкольное образовательное учреждение
детский сад №3 «Солнышко»**

171540, Тверская область, Кимрский муниципальный округ, с. Горицы, ул. Садовая, д.15,
тел (848236)71139, E-mail: solnyshkogorizi@yandex.ru

БИК 012809106, ИНН 6927005761, КПП 692701001. ОГРН 1026901670949,
ОКАТО 28528000, расч/счет: 63234643285280003600 ОТДЕЛЕНИЕ ТВЕРЬ БАНКА РОССИИ/УФК
по Тверской области г. Тверь

УТВЕРЖДАЮ
Приказ №14 «9» января 2025г.
МДОУ детский сад №3 «Солнышко»
и.о. заведующего от _____ Забурдаева Е.С.

Приложение №9
к приказу №14 от 09.01.2025г.

**Инструкция
по применению парольной защиты и личных идентификаторов в информационной
системе персональных данных в
Муниципальном дошкольном образовательном учреждении детский сад №3
«Солнышко»**

1. Общие положения

1.1. Настоящая инструкция определяет требования к порядку использования, генерации, смены и прекращения действия паролей и личных идентификаторов пользователей информационной системы персональных данных (далее – ИСПДн) Муниципального дошкольного образовательного учреждения детский сад №3 «Солнышко» (далее – Учреждение) и устанавливает ответственность сотрудников Учреждения, эксплуатирующих и сопровождающих ИСПДн, за их выполнение, а также к контролю действий пользователей при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на администратора безопасности информации ИСПДн.

1.3. Пароли для всех учетных записей пользователей ИСПДн должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
- максимальное действие пароля - не более чем 90 дней;
- пароль не должен повторяться;
- пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

1.4. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

1.5. При первичной регистрации пользователя в ИСПДн пароль ему назначает администратор безопасности информации.

1.6. Пользователи ИСПДн обязаны хранить свой личный пароль втайне от других и не передавать любым способом пароль третьим лицам.

1.7. Пользователь ИСПДн лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.

1.8. Привязку идентификатора к пользователю (учетной записи) выполняет администратор безопасности информации.

1.9. Пользователи ИСПДн получают свой идентификатор у администратора безопасности информации.

1.10. Пользователь ИСПДн обязан хранить свой личный идентификатор в недоступных для других сотрудников хранилищах.

1.11. Пользователю ИСПДн запрещается передавать свой личный идентификатор.

1.12. В случае утери личного идентификатора, пользователь ИСПДн должен немедленно доложить об этом администратору безопасности информации.

1.13. При наличии технологической необходимости использования имен и паролей сотрудников в их отсутствие (например, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.), пароли данных сотрудников должны быть незамедлительно изменены администратором безопасности информации.

1.14. Полная плановая смена паролей пользователей должна проводиться регулярно, но не реже одного раза в год.

1.15. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена, а её идентификатор должен быть сдан администратору безопасности информации после окончания последнего сеанса работы данного пользователя в ИСПДн.

1.16. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности информации.

1.17. В случае компрометации личного пароля или утери личного идентификатора пользователя администратором безопасности информации должны быть немедленно предприняты меры в соответствии с п. 1.18 настоящей Инструкции.

1.18. Администратор безопасности информации должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.

Доведение Инструкции до сотрудников Учреждения. в части их касающейся осуществляется администратором безопасности информации ИСПДн под роспись в Листе ознакомления с данной инструкцией