УТВЕРЖДЕНА
приказом № 15 от 15.07.2010 г.
заведующий С.В. Ковалева

# ИНСТРУКЦИЯ
по организации парольной защиты на объектах информатизации муниципального дошкольного образовательного учреждения детского сада № 17, предназначенных для обработки информации ограниченного распространения

Данная Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на объектах информатизации , предназначенных для обработки информации ограниченного распространения, а также контроль за действиями пользователей при работе с паролями.

## ПОРЯДОК РАБОТЫ ПО ОБЕСПЕЧЕНИЮ ПАРОЛЬНОЙ ЗАЩИТЫ

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированной системы муниципального дошкольного образовательного учреждения детского сада № 17 (МДОУ детского сада № 17) и контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности.

2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее шести символов;
- в числе символов пароля обязательно должны присутствовать символы из следующих категорий: строчные буквы латинского алфавита, прописные буквы латинского алфавита, десятичные цифры;
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ADMIN, SECRET, USER и т.п.);
- использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;
- использование двух и более подряд одинаковых символов недопустимо;
- при смене пароля новое значение должно отличаться от предыдущего минимум в 6-ти символах;

- новый пароль не должен совпадать с одним из 10-ти предыдущих паролей;
- пользователь обязан сохранять в тайне свой личный пароль.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за разглашение парольной информации.

3. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в один квартал.

4. При смене пароля администратором безопасности производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя – предъявления стороннего идентификатора.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя объекта информатизации в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности 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 внутри предприятия и другие обстоятельства) администратора безопасности.

7. В случае компрометации (утеря, передача парольной информации) личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.4 или п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Хранение сотрудником (исполнителем) значений своих паролей на любом носителе не допускается.