УТВЕРЖДАЮ
Заведующий МКДОУ «Богучарский детский сад «Улыбка»
_____ Н.В.Татаренкова
Приказ от «01» 08 2018г. №26

Инструкция
по организации парольной защиты
в МКДОУ «Богучарский детский сад «Улыбка»

1. **Общие положения**.

1.1.Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.
Организационное и техническое обеспечение процессов генерации, использование и прекращение действия паролей во всех подсистемах АС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ПД.

1.2.Требования настоящей инструкции распространяется на всех сотрудников организации.

1.3.Бесконтрольность в определении и использовании паролей может повлечь риск несанкционированного доступа к информации организации, повлечь мошеннические и другие действия в информационных системах, которые могут нанести материальный вред и ущерб репутации организации.

2.Требования к паролям.

2.1.Пароли не должны основываться на каком-либо одном слове, выданном идентификаторе, имени, кличке, паспортных данных, номерах страховок и т.д.

2.2.Пароли не должны основываться на типовых шаблонах и идущих подряд на клавиатуре или в алфавите символов, например, таких, как: qwerty, 1234567, abcdefgh и т.д.

2.3 Пароли должны содержать символы как минимум из трех следующих групп:

- Строчные латинские буквы: abcd...xyz;
- Прописные латинские буквы: ABCD...XYZ;
- Цифры: 123...90;
- Специальные символы: !%()_+ и т.д.

2.4 Требования к длине пароля:
Для обычных пользователей - не менее 8 символов;
Для администраторов (локального\доменного) - не менее 15 символов;
Для сервисных идентификаторов, разделяемых ключей (shared keys) - не менее 14 символов;
Для SNMP Community Strings - не менее 10 символов.

2.5 Периодичность смены пароля:
Административные – каждые 60 дней;
Пользовательские– каждые 90 дней;
Сервисные – не реже двух раз в год;
Shared keys SNMP Community Strings - не реже одного раза в год.

2.6 Пароли не должны храниться и передаваться в незашифрованном виде по публичным сетям (локальная вычислительная сеть, интернет, электронная почта).

2.7 . В ходе работы не должны использоваться встроенные идентификаторы. Для них должны быть назначены пароли, отличные от установленных производителем. К ним предъявляются требования, аналогичные требованиям к сервисным паролям.

2.8 Пароли нельзя записывать на бумагу, в память телефона и т.д. Нельзя сообщать, передавать кому-либо пароль.

2.9.Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены о дисциплинарной ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2.10.При наличии технологической необходимости в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же сменить свой пароль.

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

2.12.Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться уполномоченными сотрудниками отдела информационных технологий немедленно после окончания последнего сеанса работы данного пользователя с системой.

2.13.В случае компрометации личного пароля пользователя АС должны быть немедленно предприняты меры в соответствии с п. 2.12 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

2.14.Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе (возможно вместе с персональными ключевыми дискетами и ЭЦП).

3. Требования к настройкам безопасности информационных систем

3.1 Учетная запись должна блокироваться после 5 неверных попыток доступа не менее, чем на 15 минут.

3.2.Запрещается использовать функции «Запомнить пароль» в любом программном обеспечении.