УТВЕРЖДАЮ
Заведующий МБДОУ
«ЦРР-детский сад № 188»
_____Г.И.Лифанова
приказ от 29.01.2018 № 13-О

Инструкция
по организации парольной защиты
в муниципальном бюджетном дошкольном образовательном учреждении
«Центр развития ребенка — детский сад № 188»

1. Общие положения

1.1. Инструкция по организации парольной защиты (далее — Инструкция), регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных муниципального бюджетного дошкольного образовательного учреждения «Центр развития ребенка — детский сад № 188» (далее — Учреждение), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах и контроль за действиями пользователей и обслуживающего персонала при работе с паролями возлагается на системного администратора Учреждения.

1.3. Настоящая инструкция оперирует следующими основными понятиями:

1.3.1. **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) *(ст. 3 ФЗ РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных»);*

1.3.2. **информационная система персональных данных** (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»);*

1.3.3. **пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам;

1.3.4. **пользователь** – сотрудник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных;

1.3.5. **компрометация пароля** – раскрытие, обнаружение или утеря пароля.

2. Правила формирования паролей

2.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в пароле обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия и т.д.), повторяющуюся комбинацию из нескольких символов (например, «11111», «ddddd»), комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «123456», «zxcvbn»), общепринятые сокращения (например, «ЭВМ», «USER» и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от предыдущего не менее чем в четырех позициях символов.

2.2. Пользователям допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанных в произвольном порядке со специальными символами (например, коЖЗгсф-7).

2.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

2.4. Для обеспечения возможности использования имен и паролей некоторых пользователей в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.) такие пользователи обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) передавать заведующему Учреждением.

Опечатанные конверты с паролями пользователей должны храниться в сейфе. Для их опечатывания используется печать Учреждения.

После возвращения пользователя, в отсутствие которого была использована его парольная информация, производится внеплановая смена пароля.

3. Ввод пароля

При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

4. Порядок смены личных паролей

4.1. Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) его учетная запись должна быть немедленно удалена сразу после окончания его последнего дня работы.

4.3. Срочная (внеплановая) полная смена паролей всех пользователей производится в случае прекращения полномочий (увольнение, переход на другую работу, другие обстоятельства) администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 Инструкции.

4.5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

5. Хранение пароля

5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и других носителях информации, в том числе на предметах.
5.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
5.3. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля, сейфе либо в сейфе заведующего Учреждением в опечатанном конверте.

6. Действия в случае компрометации пароля

В случае компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 4.2. или п. 4.3. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность пользователей при работе с парольной защитой

7.1. 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 информации о пароле.
7.2. Ответственность за организацию парольной защиты в организации возлагается на системного администратора.
7.3. Работники Учреждения и лица, имеющие отношение к обработке персональных данных в информационных системах Учреждения, должны быть ознакомлены с Инструкцией под расписку.