Управление образованием
Администрации города Юрги

Муниципальное бюджетное
дошкольное образовательное
учреждение
«Детский сад компенсирующего вида
№ 28 «Ромашка»

УТВЕРЖДАЮ

_____Заведующий МБДОУ
«ДСКВ №28 «Ромашка» Е.А. Ковалева
Приказ № 210 **от** 14.09.2018г**.**

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ДЕТСКИЙ САД КОМПЕНСИРУЮЩЕГО ВИДА № 28 "РОМАШКА"
Дата: 2022.02.15 14:46:31 +07'00'

Инструкция
по организации парольной защиты в МБДОУ «ДСКВ №28 «Ромашка»

1. Общие положения

1.1. Инструкция по организации парольной защиты (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»; постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных».
1.2. Инструкция по организации парольной защиты (далее – Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах муниципального дошкольного образовательного учреждения «Детский сад компенсирующего вида №28 «Ромашка» (далее – Учреждение), а также контроль за действиями пользователей при работе с паролями.

2. Правила формирования паролей

2.1. Личные пароли генерируются и распределяются централизованно с учетом следующих требований:
-пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, $, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abcd и т. д.), общепринятые сокращения (ЭВМ, ЛВС, 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 старого не менее чем в шести позициях.
- при создании паролей личных учетных записей пользователей возможно использование специализированного программного обеспечения.
2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного за защиту персональных данных в Учреждении.
2.3. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте передать на хранение ответственному за информационную безопасность Учреждения.

3.Ввод пароля

3.1.При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).
3.2. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.
3.3. Разблокирование учетной записи осуществляется Ответственным для учетных записей Пользователя для АРМ и для ИСПДн соответственно.
3.4. После 10 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, централизованно не реже одного раза в три месяца.
4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.
4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5. Хранение пароля

5.1. Опечатанные конверты с паролями сотрудников должны храниться в сейфе, к которому исключён доступ других сотрудников и третьих лиц. Все конверты с паролями в обязательном порядке фиксируются в «Журнале учёта паролей пользователей информационной системы персональных данных».
5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.
5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия в случае утери и компрометации пароля.

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

7. Ответственность при организации парольной защиты.

7.1. Владельцы паролей должны быть ознакомлены под расписку 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 Учреждении возлагается на ответственного за безопасность персональных данных.
7.3. Работники ДОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ДОУ, должны быть ознакомлены с Инструкцией под расписку.