

Принято на педагогическом совете
Протокол от 21.12.20 20 № 3

УТВЕРЖДЕНО
Приказом № 45 от 21.12.2020
Заведующего МАДОУ детский сад
«Аленушка» п.Шеманиха
Прусакова Н.Н.



Положение по организации парольной защиты

Муниципального автономного дошкольного образовательного учреждения
детского сада «Аленушка» п. Шеманиха

1. Общие положения

1.1. Положение по организации парольной защиты (далее - положение) призвано регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах Муниципального автономного дошкольного образовательного учреждения детского сада «Аленушка» п. Шеманиха (далее образовательного учреждения), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее - ИС) образовательного учреждения и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на заведующего образовательного учреждения.

2. Правила формирования паролей

2.1. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно 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, ^^e^^у, аЪсё и т. д.), общепринятые сокращения (ЭВМ, ЛВС, ШЕК 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.

2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственных лиц, назначенных заведующим образовательного учреждения.

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 или опечатанном пенале передать на хранение ответственному за информационную безопасность образовательного учреждения. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

2.4. 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. Порядок смены личных паролей

3.1. Смена паролей проводится регулярно, не реже одного раза в три месяца.

3.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) ответственное лицо должно немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

3.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

3.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 положения и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

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

4. Хранение пароля

4.1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или заведующего в опечатанном пенале.

4.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

4.3. Запрещается сообщать другим пользователям личный пароль и

регистрировать их в системе под своим паролем.

5. Действия в случае утери и компрометации пароля

5.1. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 3.3 или п. 3.4 настоящего положения в зависимости от полномочий владельца скомпрометированного пароля.

6. Ответственность при организации парольной защиты

6.1. 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.

6.2. Ответственность за организацию парольной защиты в образовательном учреждении возлагается на заведующего.

Работники образовательного учреждения и лица, имеющие отношение к обработке персональных данных в информационных системах образовательного учреждения, должны быть ознакомлены с положением