Марченко Оксана Алексеевна
Подписан: Марченко Оксана Алексеевна
DN: OU=заведующий, O="МБДОУ ЦРР - д/с № 14 ""Росинка"" г. Ставрополя", CN=Марченко Оксана Алексеевна, E=dou_14@stavadm.ru
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2022.06.16 12:59:16+03'00'
Foxit PDF Reader Версия: 11.2.1

УТВЕРЖДАЮ:
Заведующий МБДОУ ЦРР – д/с № 14 «Росинка»

_____О. А. Марченко

Приказ № 28/1-ОД от 01.06.2021

ИНСТРУКЦИЯ

по организации парольной защиты в информационной системе персональныхданных МБДОУ ЦРР – д/с № 14 «Росинка»

1. Общие положения

1.1 Данная инструкция по организации парольной защиты в информационной системе персональных данных администрации Троицкого муниципального района (далее - Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее – ИСПДн) Муниципального бюджетного дошкольного образовательного учреждения центра развития ребёнка – детского сада № 14 «Росинка» города Ставрополя (далее - Учреждение), 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 ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

2. Правила формирования паролей

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

Длина пароля должна быть не менее 6 символов.

2.2. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

2.3. 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 сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

2.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

2.5. Личный пароль пользователь не имеет права сообщать никому. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственного заобеспечение безопасности персональных данных.

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 в6 месяцев.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за обеспечение безопасности персональных данных, 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 настоящей инструкции, и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

4.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

5. Хранение пароля

5.1. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5.2. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за обеспечение безопасности персональных данных.

6. Действия в случае утери или компрометации пароля

6.1. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты следующие меры:

- Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора безопасности информации.
- В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.7 или п.8 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.