Редреева Светлана Викторовна

Подписано цифровой подписью: Редреева Светлана Викторовна
Дата: 2021.07.06 21:13:46 +07'00'

Утверждено
Приказом от 07.02.2018г. № 9
Заведующий МБДОУ д/с № 6 «Березка
_____ С.В. Редреева

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных ДОУ

г. Топки

Общие положения

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на информационных системах персональных данных (далее – информационные системы) муниципального бюджетного дошкольного образовательного учреждения – детский сад № 6 «Березка» (далее – ДОУ), а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в защищаемой АС и контроль действий пользователей при работе с паролями возлагается на администратора безопасности информационных систем (далее – администратор безопасности).

Персональные пароли должны соответствовать следующим требованиям:

длина пароля должна быть не менее *шести* символов;

в числе символов пароля 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 (ФИО, наименование информационной системы и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в *четырёх* позициях.

Пользователь не имеет права сообщать его персональный пароль никому.

Хранение пользователем АС значений своих паролей на бумажном носителе допускается только в опечатанном личной печатью пенале или конверте (возможно вместе с персональным электронным идентификатором, при его наличии) в сейфе у администратора безопасности.

Повседневный контроль действий исполнителей при работе с паролями, соблюдением порядка их смены, хранения и использования, а также периодический контроль возлагается на администратора безопасности.

Процедуры смены паролей

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.

Внеплановая смена личного пароля или отключение учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую должность внутри Учреждения и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя в информационной системе согласно письменного указания непосредственного руководителя данного пользователя.

Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу или другие обстоятельства) администратора безопасности.

В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п. 0 или п. 0 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля. По каждому случаю компрометации личного пароля пользователя проводится служебное расследование комиссией Учреждения.

Ответственность

Администратор безопасности несет ответственность за повседневный контроль действий пользователей при работе с паролями, соблюдения порядка их смены, хранения и использования, а также периодический контроль.

Пользователь информационных систем ДОУ несет ответственность за соблюдение конфиденциальности его персональной парольной информации.

Пользователи информационных систем ДОУ должны быть предупреждены об ответственности за разглашение парольной информации.

С инструкцией ознакомлен(а):

Администратор безопасности информационных систем персональных данных .