Утверждено:
приказом от 04.04.2019г. № 05
заведующий МБДОУ детский сад №12
«Рябинка» _____ С.А.Степанова

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных ДОУ

г. Топки

1. Общие положения

1.1. 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 №12 «Рябинка» (далее – ДОУ), а также контроль действий пользователей и обслуживающего персонала системы при работе с паролями.

1.2. 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).

1.3. 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.

1.4. Пользователь не имеет права сообщать его персональный пароль никому.

1.5. 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.

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

2. Процедуры смены паролей

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

2.2. 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.

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

2.4. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п. 2.2 или п. 2.3 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля. По каждому случаю компрометации личного пароля пользователя проводится служебное расследование комиссией Учреждения.

3. Ответственность

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

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

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

С инструкцией ознакомлен(а):

Администратор безопасности информационных систем персональных данных .

_____