Утверждено:
Директор школы
_____ Г.В.Лазирская

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ И ПАРОЛЬНОЙ ЗАЩИТЫ В МОАУСОШ № 4 г.Новокубанска

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее ИСПД) МОАУСОШ № 4 г.Новокубанска; контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями; контроль системы с использованием антивирусной программы.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПД, контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями и антивирусной защитой возлагается на администратора информационной безопасности.

1. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

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;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- 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;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях;
- 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 администратора информационной безопасности.

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 видеокамерам и т.п.).

1. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

1.1. Смена паролей должна проводиться регулярно, не реже одного раза в 3 месяца.

1.2. 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.

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

1.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п.3.1 настоящей инструкции, и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

1.5. Администратор информационной безопасности ведёт "Журнал принудительной смены личных паролей", в котором он отмечает причины внеплановой смены паролей пользователей.

1.6. Временный пароль, заданный администратором информационной безопасности при регистрации нового пользователя, следует изменить при первом входе в систему.

2. ХРАНЕНИЕ ПАРОЛЯ

2.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

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

2.3. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора информационной безопасности, или руководителя подразделения в опечатанном личной печатью пенале.

3. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

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

4. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ АНТИВИРУСНОЙ И ПАРОЛЬНОЙ ЗАЩИТЫ

4.1. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4.2. Ответственность за организацию парольной и антивирусной защиты в подразделении возлагается на ответственных за информационную безопасность в подразделениях, периодический контроль – возлагается на администратора информационной безопасности.

Введено в действие с 01.01.2017г. пр. от 30.12.2016г. №