ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ КРЫМ «АЛУПКИНСКАЯ САНАТОРНАЯ ШКОЛА-ИНТЕРНАТ»

РАССМОТРЕНО
на заседании педагогического совета
от 02.11.2022 г.
протокол № 2

УТВЕРЖДАЮ
Директор ГБОУ РК «Алупкинская санаторная школа-интернат»
_____ А.Ю. Смирнова
Приказ № 323 от 03.11. 2022 г.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ В ГБОУ РК «АЛУПКИНСКАЯ САНАТОРНАЯ ШКОЛА-ИНТЕРНАТ» (новая редакция)

1. Общие положения

Данное положение разработано в соответствии с ФЗ-149 “Об информации, информационных технологиях и о защите информации” Российской Федерации.

Пароли являются важным элементом информационной безопасности. Они обеспечивают защиту учетных записей пользователей. Неправильно выбранный пароль может стать причиной неавторизованного доступа к конфиденциальной информации или нарушения работоспособности информационных систем ГБОУ РК «Алупкинская санаторная школа-интернат» (далее школа-интернат).

Все, имеющие доступ к информационным системам школы-интернат, ответственны за принятие соответствующих (как описано ниже) мер по созданию и защите пароля.

2. Цель

Целью положения является введение стандартов по созданию стойких паролей, их защите и срокам действия.

3. Область действия

Положение распространяется на всех пользователей информационных систем школы-интернат, которые имеют учетные записи или назначены ответственными за таковые. А также на сотрудников, хранящих конфиденциальную информацию школы-интернат и имеющие доступ к системам защиты финансовых операций.

4. Содержание

4.1. Рекомендации

4.1.1. Создание

Пароли используются для многочисленных целей. Наиболее распространенные из них: вход на компьютер, электронная почта, заставка экрана, локальный маршрутизатор и т.д. Поскольку пароли используются многократно (за редким исключением систем с одноразовыми паролями) пользователи должны знать требования по созданию стойких паролей.

Характеристики слабого пароля:

- содержит менее 8 символов;
- слово из словаря;
- повседневно используемое слово, например, имена или фамилии друзей, коллег, актеров или сказочных персонажей, клички животных;
- компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;
- вариации наименования компании или торговой марки;
- день рождения или другая персональная информация, например, адрес, номер телефона и т.п.
- регулярные последовательности символов и цифр, например, 111222, abcde, qwerty и т.п.
- что-либо из вышеперечисленного в обратном написании;
- что-либо из вышеперечисленного с добавлением цифр в начале или конце.

Характеристики стойкого пароля:

- содержит прописные и строчные буквы;
- содержит цифры и символы;
- более 8 символов длиной;
- не является словом ни на одном из языков, диалектов, жаргонов, слэнгов;
- не основывается на персональной информации;
- не записан в бумажной или электронной форме.

Пароль должен хорошо запоминаться. Один из способов - создание пароля на основе названия песни или запоминающейся фразы.

Например, "Это элементарно Ватсон!", "2Элмнт_В!".

4.1.2. Защита паролей

Для учетных записей пользователей компании запрещено использовать тот же самый пароль, что и для других информационных систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.). По возможности не используйте один и тот же пароль для различных корпоративных систем. Также необходимо использовать различные пароли в операционных системах Unix и Windows.

Запрещено сообщать пароль кому бы то ни было, включая административный персонал и секретарей. Все пароли являются конфиденциальной информацией компании.

Список запрещенных действий с паролями:

- никому не сообщайте пароль по телефону;
- не указывайте пароль в сообщениях электронной почты;
- не сообщайте пароль вашему руководству (исключение делается для первичного пароля);
- не сообщайте принципы создания пароля (например, "на основе моей фамилии");
- не сообщайте пароль в электронных опросах и незнакомых формах авторизации;
- не сообщайте пароль членам семьи и родственникам;
- не передавайте пароль коллегам на время вашего отпуска.

На компьютере должна быть включена защищенная паролем заставка, активирующаяся через 10 минут бездействия пользователя. Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер.

Если кто-либо требует сообщить ваш пароль, сошлитесь на данный документ или направьте в службу информационной безопасности компании. Не записывайте пароли на бумагу. Не сохраняйте пароли в файлах на каком-либо носителе (например, флэшка, мобильный телефон и т.п.) без шифрования.

При компрометации учётной записи пользователя, ответственный системный администратора отключает её до выяснения всех обстоятельств.

Пользователи, работающие с системами электронной подписи несут особую ответственность за сохранность и недоступность систем ЭЦП. Они должны заботиться о сохранности средств ЭЦП, не допускать посторонних лиц к средствам ЭЦП, не передавать их в чужие руки и т.д.

Для системных учетных записей учет неправильных попыток ввода пароля может быть отключен.

Пароль должен изменяться не менее одного раза в 42 дня, для системных учетных записей раз в три месяца. Рекомендованный интервал смены пароля 30 дней. Если вы подозреваете, что ваш пароль стал известен кому-либо немедленно измените его и сообщите об этом ответственному за информационную безопасность.

Службой информационной безопасности проводится периодическая проверка паролей на стойкость методами последовательного перебора и перебора по словарю. Если в ходе проверки удастся получить ваш пароль, ваша учетная запись будет заблокирована и вам будет необходимо изменить пароль для дальнейшей работы.

5. Ответственность

Все сотрудники школы-интерната несут ответственность за нарушение данной политики. Ответственный за информационную безопасность выявляет и передает в отдел кадров все факты нарушения данной политики для принятия соответствующих мер.