МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ДЕТСКИЙ САД № 24 «ДРУЖБА»
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОЙ ОКРУГ ЯЛТА
РЕСПУБЛИКИ КРЫМ
(МБДОУ № 24)

ПРИКАЗ

от 09.01.2024 **№ 18**

г. Ялта

О назначении ответственного за защиту информации в МБДОУ № 24

В соответствии с федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 27.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:
1. Назначить Швец Татьяну Васильевну, старшего воспитателя, ответственным за защиту информации (администратором безопасности информационной системы) в МБДОУ № 24.
2. Возложить на старшего воспитателя Швец Татьяну Васильевну, функции по организации защиты информации в МБДОУ № 24.
3. Утвердить Перечень информационных систем и информации ограниченного доступа, эксплуатируемых в МБДОУ № 24 (приложение № 1).
4. Утвердить Инструкцию по организации парольной защиты в информационной системе (приложение № 2).
5. Делопроизводителю Свиридовой Н.В. довести настоящий приказ до сведения лиц касающихся.
5. Контроль за исполнением данного приказа оставляю за собой.

Заведующий Е.Г. Скокина

С приказом ознакомлены:

Приложение № 2
к приказу от «19» января 2024 г. № 18

ИНСТРУКЦИЯ
по организации парольной защиты в информационной системе

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационной системе (наименование ИС), а также контроль над действиями пользователя при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора безопасности ИС.
2. Личный пароль должен выбираться и генерироваться пользователем ИС самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее шести символов;
- в числе символов пароля ***обязательно должны присутствовать*** буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего;
- личный пароль пользователь не имеет права сообщать никому.

Владелец пароля должен быть ознакомлен под роспись с перечисленными выше требованиями и предупрежден об ответственности за использование пароля, не соответствующего данным требованиям, а также за разглашение парольной информации.

3. При возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передать руководителю подразделения. Опечатанные конверты с паролями исполнителей должны храниться в сейфах руководителя подразделения.
4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.
5. Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться Администратором информационной безопасности ИС немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.
6. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) Администратора информационной безопасности ИС.
7. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры в соответствии с п.5 или п.6 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.
8. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в сейфе руководителя.
9. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора информационной безопасности ИС.