

«Утверждаю»
Директор МБОУ ООШ №18
им. Д.А. Шеметова пос.Заводской
МО Ейский район
_____ И.Л.Лущик
«01» сентября 2022 г.

ИНСТРУКЦИЯ

по организации парольной защиты доступа к информационным ресурсам, содержащим персональные данные

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) доступа к информационным ресурсам, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на ответственных сотрудников образовательной организации.

2.Личные пароли и имена входов на доступ к информационным ресурсам назначаются и распределяются централизованно. Пароли на доступ в информационные подсистемы распределяются централизованно либо выбираются пользователями подсистемы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 7 символов;
 - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, общепринятые наименования или сокращения, например, «ЭВМ», «User» и т.д.);
 - при смене пароля новое значение должно отличаться от предыдущих значений пароля;
 - личный пароль и имя входа пользователь должен хранить в секрете;
- Владельцы паролей и имен входов перед их получением должны заполнить типовую анкету и быть предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение пароля и имени входа в информационную подсистему.

3.В случае если формирование личных паролей имен входов осуществляется централизованно, ответственность за правильность их

формирования и распределения возлагается на ответственных сотрудников образовательной организации.

4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной подсистемы в случае прекращения его полномочий (увольнения, переход на другую работу внутри организации и т.п.)

должна производиться администраторами после окончания последнего сеанса работы данного пользователя соответствующей подсистемой.

5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) администратора, которому по роду работы были предоставлены полномочия по управлению парольной защитой доступа к информационной подсистеме.

6. В случае компрометации личного пароля пользователя информационной подсистемы, должны быть немедленно предприняты меры в соответствии с п. 5 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного сотрудника образовательной организации.