Министерство образования Саратовской области
государственное автономное профессиональное образовательное учреждение
Саратовской области
«Энгельсский промышленно-экономический колледж»
(ГАПОУ СО «ЭПЭК»)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 341688004EAE5FB242C0CB02F4F47955
Владелец: КУКУШКИН МИХАИЛ АЛЕКСАНДРОВИЧ
Действителен: с 04.03.2022 до 04.06.2023

УТВЕРЖДЕНО:
Приказом ГАПОУ СО «ЭПЭК»
от «02» 11. 2022 г. № 264 АХД
Директор ГАПОУ СО «ЭПЭК»
_____ М.А. Кукушкин

ПОЛОЖЕНИЕ

о парольной защите при обработке персональных данных и иной конфиденциальной информации государственного автономного профессионального образовательного учреждения Саратовской области «Энгельсский промышленно-экономический колледж»

(ГАПОУ СО «ЭПЭК»)

Энгельс 2022 г

Данное положение о парольной защите при обработке персональных данных и иной конфиденциальной информации (далее-Положение) государственного автономного профессионального образовательного учреждения Саратовской области «Энгельсский промышленно-экономический колледж» (далее-Оператор) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (учетных записей Пользователей) в информационных системах (далее-ИС) ответственного лица по безопасности ИС, а также контроль за действиями Пользователей и обслуживающего персонала при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИС и контроль за действиями Пользователей и обслуживающего персонала при работе с паролями возлагается на ответственное лицо по безопасности ИС.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИС самостоятельно с учетом следующих требований:

-длина пароля должна быть не менее 8 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 (имена, фамилии, наименования АРМ 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 6 позициях;

-личный пароль Пользователей не имеет права сообщать никому.

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

3. В случае, если формирование личных паролей Пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных приказом по Колледжу работников. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

4. При наличии технологической необходимости (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) использования имен и паролей некоторых работников (Пользователей) в их отсутствие, такие работники обязаны сразу же после смены своих паролей передавать на хранение руководителю своего подразделения их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте. Опечатанные конверты с паролями Пользователей должны храниться в сейфе.

5. Полная плановая смена паролей Пользователей должна проводиться регулярно, не реже одного раза в квартал (или в иные установленные ответственным лицом по безопасности сроки).

6. Внеплановая смена личного пароля или удаление учетной записи Пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) ответственным лицом по безопасности немедленно после окончания последнего сеанса работы данного Пользователя с системой.

7. Внеплановая полная смена паролей всех Пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного лица по безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля Пользователей ИС должны быть немедленно предприняты меры в соответствии с пунктом 6 или пунктом 7 настоящего Положения в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение Пользователем своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте.

10. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль –возлагается на ответственное лицо по безопасности.