Автономная некоммерческая организация дополнительного профессионального образования
«РЕГИОНАЛЬНЫЙ ЦЕНТР ПЕРЕПОДГОТОВКИ КАДРОВ УПРАВЛЕНИЯ»

УТВЕРЖДАЮ
Директор АНО ДПО «РЦПКУ»

_____ А.К. Семенов
«01» 07 2020 г.

ПОЛОЖЕНИЕ

о парольной защите при ОПД и иной
конфиденциальной информации в АНО ДПО «РЦПКУ»

г. Липецк

1.1. Данное Положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационной системе АНО ДПО «РЦПКУ» (далее - Организация), меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации Организации.

1.3. Требования настоящего Положения распространяются на всех работников, использующих в работе средства вычислительной техники.

1.4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах Организации и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на руководителя Организации. Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора локальной вычислительной сети (далее - администратор ЛВС) Организации.

1.5. Ознакомление всех работников Организации, использующих средства вычислительной техники, с требованиями Положения проводит руководитель. При ознакомлении с Положением внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации.

2. Термины и определения

Информационная система (ИС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Информационная безопасность (ИБ) - обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности процесса и минимизации рисков.

Принцип минимальных привилегий - принцип, согласно которому каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

Компрометация - утрата доверия к тому, что информация недоступна посторонним лицам.

Ключевой носитель - электронный носитель (дискета, флэш-накопитель,

компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

3. Общие требования к паролям

3.1. Пароли доступа ко всем информационным ресурсам первоначально формируются администратором ЛВС, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.

3.2. Личные пароли пользователей автоматизированной системы Учреждения должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, $,&,*,% и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, p@sswOrd и т.п.);
- при смене пароля новый пароль должен отличаться от старого не менее чем двумя символами.

4. Контроль

4.1. Контроль над соблюдением требований данного Положения осуществляется администратором ЛВС Организации.

4.2. Администратор ЛВС Организации проводит выборочный контроль выполнения работниками Организации требований Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности сообщается руководителю Организации в форме служебной записки.

5. Ответственность

5.1. Пользователи ИС Организации несут персональную ответственность за несоблюдение требований по парольной защите.

5.2. Администратор ЛВС несет ответственность за компрометацию и нецелевое использование учетных записей.

5.3. Форма и размер ответственности определяются исходя из вида и размера ущерба, нанесенного ресурсам ИС Организации действиями либо бездействием соответствующего пользователя.