

УТВЕРЖДЕНО:
И.о. главного врача ГБУЗ «ЦРБ»
Майского муниципального района
Т.В. Аникушина
ПРИКАЗ УЧРЕЖДЕНИЯ
ОТ «14» АВГУСТА 2017Г. № 275
ПРИЛОЖЕНИЕ № 14

ИНСТРУКЦИЯ

по применению парольной защиты в информационной системе персональных данных

1. Настоящая Инструкция определяет порядок использования, генерации, смены и прекращения действия паролей пользователей в информационной системе персональных данных (ИСПДн) ГБУЗ «ЦРБ» Майского муниципального района, а также контроль действий пользователей при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, а также контроль действий пользователей при работе с паролями возлагается на ответственного в учреждении за обеспечение безопасности персональных данных в ИСПДн - программиста.

3. Пароли для всех учетных записей пользователей ИСПДн должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 6 буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
- максимальное действие пароля - не более чем 90 дней;
- пароль не должен повторяться;
- пользователь не может неправильно ввести пароль учетной записи более 5 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки.

3.1 При первичной регистрации пользователя в системе пароль ему назначает ответственный в учреждении за обеспечение безопасности персональных данных в ИСПДн.

3.2 Пользователи ИСПДн обязаны хранить свой личный пароль в тайне от других и не передавать любым способом пароль третьим лицам.

3.3. Пользователь ИСПДн лично должен проводить смену пароля учетной записи регулярно не реже одного раза в три месяца.

4. В случае прекращения полномочий учетной записи пользователя ИСПДн (увольнение, переход на другую работу, в другой отдел или помещение, а также другие обстоятельства) учетная запись должна быть удалена.

5. В случае компрометации личного пароля пользователя ответственным в учреждении за обеспечение безопасности персональных данных в ИСПДн должны быть немедленно предприняты меры в соответствии с п. 6 настоящей Инструкции.

6. Ответственный в учреждении за обеспечение безопасности персональных данных в ИСПДн должен провести служебное расследование для выяснения причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины ущерба, который может быть нанесен собственнику информационных ресурсов.