



Инструкция по организации парольной защиты в ГБУЗ «Ленинская ЦРБ»

1. Правила формирования пароля

1.1. Персональные пароли должны генерироваться специальными программными средствами административной службы либо выбираться пользователями информационных систем персональных данных ГБУЗ «Ленинская ЦРБ» самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в составе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (“~!@#\$%^&*()-+_=\\|/?,”);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 (2,3...,7,8) позициях;
- личный пароль пользователь не имеет права сообщать никому;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе.

2. Ввод пароля

2.1. При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамеры и т.п.).

3. Порядок смены личных паролей

- 3.1. Смена паролей должна проводиться регулярно, не реже одного раза в 2 месяца.
- 3.2. В случае прекращения полномочий пользователя производится немедленное удаление учетной записи пользователя Администратором безопасности.
- 3.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий администраторов информационной системы и других сотрудников, которым по роду деятельности были предоставлены полномочия по управлению системой парольной защиты.
- 3.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п.3.1 настоящей Инструкции.
- 3.5. Временный пароль, заданный Администратором безопасности при регистрации нового пользователя, следует изменить при первом входе в систему.

4. Хранение пароля

- 4.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
- 4.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5. Действия в случае утери и компрометации пароля

- 5.1. В случае утери или компрометации пароля пользователя должны быть немедленно приняты меры в соответствии с п.3.3 или п.3.4 настоящей инструкции в зависимости от полномочий владельца скомпрометированного пароля.

6. Ответственность при организации парольной защиты

- 6.1. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
- 6.2. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора информационной безопасности.

Лист ознакомления с документом «Инструкция по организации парольной защиты»

[illegible]