федеральное государственное бюджетное
образовательное учреждение высшего образования
«Самарский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО СамГМУ Минздрава России)

ПРИКАЗ

31.03.2021 № 82

Самара

Об утверждении Инструкции
по организации парольной защиты

В целях исполнения требований Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ; Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по организации парольной защиты в ФГБОУ ВО СамГМУ Минздрава России согласно Приложению 1 к настоящему приказу.
2. Контроль за исполнением настоящего Приказа возложить на директора Института цифрового развития Одобеску С.В.
3. Отделу документационного обеспечения довести данный Приказ до проректоров и руководителей структурных подразделений.

Ректор,
профессор РАН **А.В. Колсанов**

Приложение 1 к приказу
от «31» 03 2021 г. № 82

Инструкция
по организации парольной защиты

1. Общие положения

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, хранения, смены и прекращения действия паролей в ФГБОУ ВО СамГМУ Минздрава России, а также контроль за действиями сотрудников ФГБОУ ВО СамГМУ Минздрава России (далее – Пользователи) при работе с личными паролями.

2. Правила формирования и ввода пароля

В целях обеспечения информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России, для доступа в домен Active Directory и прочие автоматизированные информационные системы, сотрудникам предоставляются учетные записи, защищенные паролем. Не допускается использование учетных записей, не защищенных паролем.

Пароль для своей учетной записи Windows Пользователь получает после регистрации его учетной записи в домене Active Directory сотрудниками Управления информационных технологий. Пароль учетной записи Пользователя состоит не менее чем из 8 символов, а в числе символов пароля обязательно используются буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

Порядок формирования пароля Пользователями в иных автоматизированных информационных системах должен соответствовать следующим условиям:

- пароль не может содержать имя учетной записи пользователя или его часть;
- пароль должен состоять не менее чем из 8 символов;
- пароль должен включать в себя:
  - буквы нижнего регистра;
  - буквы верхнего регистра;

- десятичные цифры (от 0 до 9);
- специальные символы (!, $, #, % и т.п.);

– запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, общепринятые сокращения (ЭВМ, USER, PASSWORD и т.п.), а также имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
– запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «ааааааааа»);
– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567» и т.п.);
– запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке ЭВМ) для входа в иные автоматизированные информационные системы;
– запрещается выбирать пароли, которые уже использовались ранее.
– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
– Пользователь обязан хранить в тайне свои личные пароли;
– Пользователю запрещается передавать любые пароли и доступы третьим лицам, ставшие ему известными в рамках исполнения должностных обязанностей.

При вводе пароля Пользователю необходимо исключить возможность получения информации о нем 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 видеокамерами и т.п.).

3. Порядок хранения и смены паролей

Хранение Пользователями значений своих паролей на бумажном носителе и личных идентификаторов допускается лишь в пенале, пакете или конверте, опечатываемых и хранящихся в личном сейфе, либо в ящике стола, запирающимся на замок.

Полная плановая смена паролей Пользователей автоматизированных информационных систем должна проводиться регулярно, не реже чем через 120

дней, каждым Пользователем самостоятельно.

Внеплановая смена пароля или удаление учетной записи Пользователя в случае прекращения его полномочий (увольнение, перемещение по должности и т.п.) производится сотрудниками Управления информационных технологий немедленно после окончания последнего сеанса работы данного Пользователя.

В случае компрометации (утраты доверия к тому, что используемый пароль обеспечивает безопасность информации) личного пароля Пользователя производится внеплановая смена пароля в следующем порядке:

- Пользователь немедленно прекращает работу на своем автоматизированном рабочем месте и сообщает о факте компрометации (или предполагаемом факте компрометации) в Центр информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745), эл. почта: cib@samsmu.ru);
- Центр информационной безопасности производит смену скомпрометированного пароля;
- по факту компрометации проводится служебное расследование.

4. Ответственность за организацию парольной защиты

Ответственность за организационное и техническое обеспечение парольной защиты информации в ФГБОУ ВО СамГМУ Минздрава России возлагается на Управление информационных технологий.

Все Пользователи несут ответственность, согласно действующему законодательству, за несоблюдение требований настоящей Инструкции в ФГБОУ ВО СамГМУ Минздрава России.