Утверждаю
Ректор
_____ Л.Н.Горбатова
«26» 05. 2021 г.

ИНСТРУКЦИЯ
По организации парольной защиты в информационных системах
Федерального государственного бюджетного образовательного
Учреждения высшего образования
«Северный государственный медицинский университет»
Министерства здравоохранения Российской Федерации

Версия 2.0

Дата введения: 26.05.2021.

Архангельск
2021

	Должность	Фамилия/подпись	Дата
Разработал	Директор информационно-интеллектуального центра	Трифонов И.А.	02.04.2021г.
Проверил	Начальник управления правового и кадрового обеспечения	Котлов И.А.	02.04.2021г.
Согласовал	Первый проректор, проректор по учебно-воспитательной работе	Оправин А.С.	02.04.2021г.
	Проректор по цифровой трансформации и инфраструктурному развитию	Халезин А.С.	02.04.2021г.

1. Рассмотрено на заседании Ученого совета, протокол № 12 от «14» 04 2021 г.
2. Утверждено и введено в действие приказом Ректора, № 146 от «26» 05 2021 г.
3. Соответствует требованиям СГМУ.
4. Введено в действие взамен Инструкции по организации парольной защиты в информационных системах – версия 1.0.

СОДЕРЖАНИЕ

1.ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационной системе персональных данных ФГБОУ ВО СГМУ (г. Архангельск) Минздрава России (далее - Университет), а также контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями.

2.1. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах (далее - ИС) и контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями возлагается на системного администратора, ответственного за защиту информации.

2. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЯ

2.1. Персональные пароли должны создаваться пользователями информационной системы персональных данных Университет самостоятельно либо генерироваться специальными программными средствами 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 или 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, 118ЕК и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

2.2. 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.

2.3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администраторов 2.3. Учет работы пользователей ИСПДн производится средствами защиты информации (далее - СЗИ) от несанкционированного доступа (далее - НСД), установленных на ПЭВМ, в системном журнале.

информационных систем. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

3. ВВОД ПАРОЛЯ

3.1. 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 видеокамерам).

4. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ ИС

4.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 3 месяца.

4.2. При возникновении нештатных ситуаций, форс-мажорных обстоятельств, производственной и технологической необходимости использования имен и паролей некоторых Пользователей в их отсутствие, сменившие пароль сотрудники, обязаны сразу же после смены паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение Администратору информационной безопасности или руководителю структурного подразделения. Опечатанные конверты с паролями Пользователей должны храниться в сейфе.

4.3. Внеплановая смена ***личного пароля*** или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри Университета и т.п.) должна производиться Администратором немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.4. Срочная (внеплановая) ***полная смена паролей*** всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Университета и другие обстоятельства) Администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой информационной системы персональных данных ФГБОУ ВО СГМУ.

4.5. Временный пароль, заданный Администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

5. ХРАНЕНИЕ ПАРОЛЯ И КОНТРОЛЬ ЗА ИСПОЛЬЗОВАНИЕМ ПАРОЛЯ

5.1. Пользователям ИС запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

5.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5.3. Хранение Пользователями значений своих паролей на бумажном носителе, в запечатанном конверте, допускается только в личном, запирающимся владельцем пароля металлическом шкафу, либо в сейфе у ответственного за информационную безопасность или руководителя структурного подразделения.

5.5. Повседневный контроль за действиями Пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность ИС.

6. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ ИЛИ КОМПРОМЕТАЦИИ ПАРОЛЯ

6.1. В случае утери или компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.4.3. или п.4.4. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ

7.1. Владельцы паролей - Пользователи ИС 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.

7.2. Ответственность за организацию парольной защиты в информационной системе персональных данных возлагается на администраторов ИС, при использовании аппаратно - программных средств контроля доступа (СКД).

7.3. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора ИБ Университета.

8. УТВЕРЖДЕНИЕ И ИЗМЕНЕНИЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение вводится в действие с момента подписания приказа Ректором.

8.2. Ответственность за соблюдение требований, изложенных в данном Положении, несет Директор ИИЦ.

8.3 Изменения и дополнения в Положение вносятся по инициативе:

- ректора СГМУ;
- первого проректора, проректора по учебно-воспитательной работе;
- проректор по инфраструктурному развитию
- директор ИИЦ;
- начальника управления правового и кадрового обеспечения;