СЕВЕРО-КАВКАЗСКИЙ
МЕДИЦИНСКИЙ
КОЛЛЕДЖ

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ**
**СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**
**«СЕВЕРО-КАВКАЗСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»**

**УТВЕРЖДАЮ**
**Директор АНО СПО «СКМК»**

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат:
0128CABE0060B0A5AD4494AF47B1C7615F
Владелец: Станислав Сергеевич Наумов
Действителен с 16.08.2023 до 16.11.2024

Приказ от 19.05.2023 № 39-ОД
29 мая 2024 г.

# ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ, ИДЕНТИФИКАЦИИ
И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ
В АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "СЕВЕРО-КАВКАЗСКИЙ
МЕДИЦИНСКИЙ КОЛЛЕДЖ",
ЕГО СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ И ФИЛИАЛАХ

(с изменениями, внесенными приказом АНО СПО "СКМК" от 09.01.2024 № 01-ОД)

(выписка)

## I. Общие положения

1.1. Инструкция по организации парольной защиты, идентификации и аутентификации пользователей информационных систем (далее – Инструкция) в автономной некоммерческой организации среднего профессионального образования "Северо-Кавказский медицинский колледж", его структурных подразделениях и филиалах (далее – АНО СПО "СКМК"), разработана в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, № 31, 31.07.2006, ст. 3448);

– Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701);

– Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (Собрание законодательства Российской Федерации, № 45, 05.11.2012, ст. 6257);

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден приказом ФСТЭК России от 18.02.2013 № 21 (Зарегистрировано в Министерстве юстиции Российской Федерации 14.05.2013, регистрационный № 28375);

– Для служебного пользования;

– Методический документ "Меры защиты информации в государственных информационных системах", утвержден ФСТЭК России 11.02.2014.

1.2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, использования, смены и прекращения действия аутентификаторов (на основе паролей) в АНО СПО "СКМК", а также алгоритмы контроля действий пользователей при работе с аутентификационной информацией.

1.2[1]. Для служебного пользования.

1.2[2]. Для служебного пользования.

1.2[3]. Для служебного пользования.

1.2[4]. В информационных системах АНО СПО "СКМК" обеспечивается однозначное сопоставление идентификатора пользователя с запускаемыми от его имени процессами.

1.3. Общее и методическое руководство, организационное обеспечение процессов генерации, смены и прекращения действия аутентификационной информации в АНО СПО "СКМК" возлагается на отдел цифрового развития и информационной безопасности.

1.3[1]. Приказом (распоряжением) директора АНО СПО "СКМК" назначаются должностные лица (администраторы) из числа работников отдела цифрового развития и информационной безопасности, ответственные за создание, присвоение, выдачу, инициализацию, уничтожение идентификаторов пользователей и устройств, принятие мер в случае утраты и (или) компрометации средств аутентификации.

1.4. Исполнение контрольно-надзорных функций в рамках требований настоящей Инструкции, а также иных нормативных актов, регламентирующих работу с аутентификационной информацией, возлагается на ответственного за организацию обработки персональных данных.

## II. Термины и определения

2.1. Идентификация – присвоение субъектам и объектам доступа уникального и однозначно определяющего их идентификатора, и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2.2. Компрометация – факт доступа (подозрения доступа) постороннего лица к аутентификационной информации.

2.3. Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

2.4. Пароль – признак субъекта доступа, предъявляемый совместно с идентификатором субъекта в процессе идентификации.

2.5. Правила доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

2.6. Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2.7. Несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа в автоматизированной системе.

2.8. Аутентификация – процедура проверки подлинности. В рамках настоящей Инструкции под аутентификацией понимается проверка подлинности субъекта доступа путем сравнения введtнного им аутентификатора (пароля) с перечнем присвоенных аутентификаторов (паролей).

2.9. Авторизация – предоставление субъекту доступа прав на выполнение определённых действий (предусмотренных правилами доступа) в автоматизированной системе (подтверждение данных прав при попытке выполнения этих действий).

## III. Порядок управления средствами аутентификации, правила и условия формирования аутентификационной информации

3.1. Личные аутентификаторы субъектов АНО СПО "СКМК" генерируются и распределяются централизованно либо персонально на автоматизированном рабочем месте при отсутствии технической возможности централизованного формирования.

3.1[1]. Сформированный и присвоенный идентификатор, содержащийся в аутентификационной информации, должен однозначно идентифицировать пользователя и (или) устройство.

3.2. Для служебного пользования.

3.3. Для служебного пользования.

3.4. Аутентификатор не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии), общепринятые сокращения (LAN, USER), последовательности символов и знаков (111, qwerty, abcd), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно подобрать, основываясь на информации о субъекте.

Для генерации "стойких" значений паролей могут применяться специальные программные средства. Система генерации паролей должна исключать возможность ознакомления других работников с паролями исполнителей.

3.5. Для служебного пользования.

3.5[1]. Для служебного пользования.

3.6. Не допускается использование единого пароля для доступа субъекта к разным информационным системам (ресурсам).

3.6[1]. Не допускается использование гостевых (анонимных) и временных учетных записей пользователей в информационных системах АНО СПО "СКМК".

3.7. Личный аутентифкатор субъект не имеет права передавать или разглашать третьим лицам, в том числе своим коллегам и руководителям.

3.8. Для служебного пользования.

3.9. Для служебного пользования.

3.10. После генерации аутентификатора субъекту выдается Карточка регистрации аутентификатора (форма прилагается) с указанием автоматизированной (информационной) системы к которой предоставляется доступ, Ф.И.О., должности, структурного подразделения, уровня системных полномочий субъекта, даты генерации атуентификатора и срока его действия.

Карточка регистрации аутентификатора удостоверяется личной подписью начальника отдела цифрового развития и информационной безопасности, скрепляется печатью АНО СПО "СКМК".

3.11. Карточка регистрации аутентификатора является основным документом, подтверждающим системные полномочия субъекта. Субъект несет персональную ответственность за сохранность документа.

## IV. Порядок ввода аутентификаторов

В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля в информационных (автоматизированных) системах АНО СПО "СКМК" определены следующие правила ввода пароля:

4.1. Для служебного пользования.

4.2. Для служебного пользования.

4.3. Ввод аутентификатора должен осуществляться непосредственно субъектом доступа (владельцем), запрещается передавать аутентификатор для ввода другим лицам.

4.4. Непосредственно перед вводом аутентификатора для предотвращения возможности неверного ввода субъект должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша Caps Lock, а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, чтобы исключить возможность увидеть набираемый текст посторонними).

4.5. При вводе аутентификатора субъекту запрещается проговаривать вслух вводимые символы.

## V. Порядок смены аутентификаторов

5.1. Смена аутентификационной информации осуществляется отделом цифрового развития и информационной безопасности.

5.1[1]. Для служебного пользования.

5.2. Для служебного пользования.

5.3. Внеплановая смена аутентификатора осуществляется в случае его компрометации (или подозрении на компрометацию), при обращении субъекта или его непосредственного руководителя, а также на основании решения начальника отдела цифрового развития и информационной безопасности.

5.4. В случае прекращения полномочий пользователя (отзыв допуска, увольнение) осуществляется немедленное удаление соответствующей аутентификационной информации.

5.5. Срочная (внеплановая) полная смена аутентификаторов осуществляется в случае прекращения полномочий (отзыв допуска, увольнение) ответственных за обеспечение информационной безопасности и защиту конфиденциальной информации должностных лиц, администраторов информационных систем и других сотрудников, которым по роду деятельности были предоставлены полномочия по управлению системой парольной защиты.

5.6. Для служебного пользования.

5.7. Отдел кадров обязан известить отдел цифрового развития и информационной безопасности о состоявшемся приказе (распоряжении) (в том числе путем предоставления заверенной копии приказа (распоряжения)) в течение 24 часов после приема, увольнения, перевода работника в другое структурное подразделение или филиал, а также в случае изменения должностных (функциональных) обязанностей.

5.8. Выдача аутентификатора осуществляется лично субъекту при предъявлении основного документа удостоверяющего личность.

5.8[1]. Перед выдачей аутентификатора уполномоченное должностное лицо отдела цифрового развития и информационной безопасности обязано установить личность субъекта, проверить его должностные (функциональные) обязанности.

## VI. Порядок хранения и контроль использования аутентификаторов

6.1. Хранение личных аутентификаторов субъектов на материальных носителях допускается только в недоступных для третьих лиц местах, гарантирующих защиту аутентификационной информации от неправомерного доступа к ней и модифицирования.

6.2. Для служебного пользования.

6.2[1]. Для служебного пользования.

6.2[2]. Для служебного пользования.

6.3. При возникновении производственной необходимости в срочном доступе к личной учетной записи временно отсутствующего субъекта допускается произвести смену его аутентификатора под личную ответственность непосредственного руководителя.

После возвращения субъекта на рабочее место осуществляется повторная смена аутентификационной информации с ее последующей передачей лично субъекту.

## VII. Компрометация аутентификатора

Для служебного пользования.

## VIII. Ответственность

8.1. Субъекты, имеющие доступ к автоматизированным системам, должны быть ознакомлены с настоящей Инструкцией и предупреждены о правовых последствиях в случае нарушения ее требований.

8.2. Ежедневный контроль исполнения настоящей Инструкции при работе с личными аутентификаторами возлагается на руководителей структурных подразделений. При обнаружении признаков компрометации непосредственный руководитель субъекта обязан в кратчайший срок письменно уведомить начальника отдела цифрового развития и информационной безопасности о нарушении.

8.3. Общий контроль соблюдения режима информационной безопасности и требований, предусмотренных Инструкцией, возлагается на начальника отдела цифрового развития и информационной безопасности в соответствии с ежегодным Планом, утверждаемым директором АНО СПО "СКМК".

8.4. Соблюдение порядка формирования, генерации, смены, хранения и выдачи аутентификационной информации возлагается на отдел цифрового развития и информационной безопасности.

8.5. Субъекты несут персональную ответственность за сохранность личных аутентификаторов, в том числе Карточек регистрации аутентификационной информации.

8.6. Ответственность за несвоевременное уведомление начальника отдела цифрового развития и информационной безопасности о случаях утери, кражи, взлома или компрометации аутентификаторов возлагается на субъекта (владельца) взломанной учетной записи.

8.7. В случае нарушения режима информационной безопасности, компрометации аутентификационной информации, повлекшей разглашение конфиденциальной информации, содержащей персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

**Начальник отдела цифрового развития и информационной безопасности**

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 01DAB0D0459093C000193FF410EF0001
Владелец: Сергей Викторович Семенов
Действителен с 28.05.2024 до 28.05.2025

**С. В. Семенов**

29 мая 2024 г.

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ "СЕВЕРО-КАВКАЗСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ"
Ленина ул., дом 267, офис 1, Ставрополь г., 355003

Форма

КОНФИДЕНЦИАЛЬНО

**КАРТОЧКА РЕГИСТРАЦИИ АУТЕНТИФИКАТОРА**

операционной системы, домена NCMC.LOCAL локальной вычислительной сети АНО СПО "СКМК"

(наименование автоматизированной (информационной) системы)

| | |
|---|---|
| Фамилия:<br>Имя:<br>Отчество:<br>Должность:<br>Основание:<br>Наименование ИСПДн: | Логин:<br>Пароль:<br>Дата регистрации аутентификатора:<br>Срок действия аутентификационной информации: |

Ответственный за организацию парольной защиты:

| Начальник отдела цифрового развития и информационной безопасности | | |
|---|---|---|
| (должность) | (подпись) | (расшифровка подписи) |

С правилами работы ознакомлен(а):

| | | |
|---|---|---|
| (должность) | (подпись) | (расшифровка подписи) |

Линия отреза

**КАРТОЧКА РЕГИСТРАЦИИ АУТЕНТИФИКАТОРА**

операционной системы, домена NCMC.LOCAL локальной вычислительной сети АНО СПО "СКМК"

(наименование автоматизированной (информационной) системы)

Дата регистрации аутентификатора:

Логин:

Начальник ОЦРиИБ

| | | |
|---|---|---|
| (должность) | (подпись) | (расшифровка подписи) |

С правилами работы ознакомлен(а):

| | | |
|---|---|---|
| (должность) | (подпись) | (расшифровка подписи) |