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

УТВЕРЖДЕНО
Приказом Ректора
член-корреспондента РАН
з.д.н. РФ
А.В. Колсанова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7A6B8A5E9CB221443586B1F30109C6F1
Владелец: Колсанов Александр Владимирович
Действителен: с 02.04.2026 до 26.06.2027

# РЕГЛАМЕНТ № 4П/08-31-2026

создания, учёта, изменения и блокирования, контроля удаления учётных записей ФГБОУ ВО СамГМУ Минздрава России

Приложение № 4
к приказу ректора ФГБОУ ВО
СамГМУ Минздрава России
№ 169 от 31.08.2026 г

Самара 2026

## 1. Общие положения

1.1 Предметом настоящего Регламента является утверждение порядка создания, учёта, изменения и блокирования, контроля удаления учётных записей в ФГБОУ ВО СамГМУ МЗ РФ.

1.2 Целями регламента является:

- Повышение уровня информационной безопасности в сети ФГБОУ ВО СамГМУ МЗ РФ и информационных ресурсах в ФГБОУ ВО СамГМУ МЗ РФ.
- Стандартизация и обеспечение единообразия в сфере информационной безопасности.

1.3 Настоящий Регламент разработан в соответствии со следующими руководящими документами:

- приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- письмо ФСТЭК России от 07.10.2025 № 240/92/3228 «О мерах по повышению защищенности информационной инфраструктуры Российской Федерации».
– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

## 2. Порядок создания учетной записи в домене и получения доступа к информационным ресурсам при трудоустройстве

2.1 При трудоустройстве в ФГБОУ ВО СамГМУ Минздрава России (далее - Университет) сотрудник проходит инструктаж по информационной безопасности, инструктаж по использованию персонального компьютера и ресурсов сети. Руководителю структурного подразделения необходимо оформить служебную записку на имя директора Дирекции по цифровой трансформации с указанием ФИО, должности сотрудника, для создания учетной записи в домене Active Directory.

2.2 Пароль для учетной записи Windows Пользователь получает после регистрации его учетной записи в домене Active Directory сотрудниками Управления информационной безопасности. Требования к паролю пользователя в домене:

- длина, не менее 8 символов
- Не менее одной заглавной и строчной буквы латинского алфавита
- Не менее одной цифры

Парольная карточка, на которой указан пароль от учётной записи Windows, выдаётся пользователю сотрудниками Управления информационной безопасности под запись в Журнале выдачи парольных карточек

2.3 При вводе пароля Пользователю необходимо исключить возможность получения информации о нем посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.). Пользователю запрещается передавать и разглашать пароль третьим лицам, в противном случае, его учетная запись будет считаться скомпрометированной.

В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля, после пяти неудачных попыток ввода пароля, учётная запись блокируется. Для разблокировки учетной записи необходимо оформить служебную записку на имя начальника центра системного администрирования и развития локально-вычислительных сетей.

2.4 Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности. Каждый стационарный компьютер, ноутбук или неттоп, принадлежащий организации, должен находиться в домене Университета. Каждый пользователь должен обладать собственной и уникальной учетной записью в домене.

## 3. Порядок получения доступа к информационным системам Университета пользователям

3.1 При необходимости получения дополнительного доступа к информационным системам Университета, руководитель структурного подразделения оформляет служебную записку на имя директора Дирекции по цифровой трансформации, в которой указывает необходимый доступ к информационным системам Пользователю в соответствии с его должностными обязанностями. В целях обеспечения санкционированного

доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

3.2 Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам, в соответствии с его должностными обязанностями.

В случае изменения должностных обязанностей сотрудника (или переходу на новую должность), руководитель структурного подразделения оформляет служебную записку на имя директора Дирекции по цифровой трансформации, с указанием ФИО и должности сотрудника на аннулирование прав доступа, которые сотруднику более не нужны, и указывает права, которые понадобятся сотруднику для дальнейшего выполнения новых должностных обязанностей.

3.3 В случае служебной необходимости, для работы сотрудника в информационных системах, с использованием усиленной квалифицированной электронной подписи, руководитель структурного подразделения оформляет служебную записку на имя Ректора, с указанием информационных систем, ФИО и должности сотрудника.

3.4 При увольнении сотрудника, у которого на момент прекращения должностных обязанностей имеется действующая электронная подпись, руководитель структурного подразделения оформляет служебную записку на имя директора Дирекции по цифровой трансформации, с просьбой аннулировать (отозвать) электронную подпись данного сотрудника.

## 4. Порядок учёта учётных записей и хранение пароля

4.1 Список всех учётных записей хранится в консоли Active Directory.

4.2 Управление учетными записями осуществляется сотрудниками Управления информационной безопасности.

4.3 При использовании паролей пользователь обязан соблюдать положения должностных инструкций, методических документов по информационной безопасности, а также требования Регламента.

4.4 Пользователь не имеет права сообщать личный пароль другим сотрудникам и допускать их к работе под своей учетной записью.

4.5 Пользователь обязан помнить свой пароль от учётной записи. Парольную карточку от учетной записи Windows необходимо уничтожить после запоминания пароля или хранить его в месте, недоступным другим сотрудникам.

4.6 При утере, компрометации, несанкционированном изменении пароля пользователь обязан немедленно сообщить о данном факте в Управление информационной безопасности, после чего дальнейшее использование соответствующей учетной записи не допускается до смены пароля.

## 5. Порядок отключения учетной записи в домене и отключение доступа к информационным ресурсам при увольнении

5.1 Сотруднику при увольнении необходимо подписать обходной лист у всех должностных лиц, указанных в нем и поставить отметки об отсутствии задолженностей.

5.2 Сотрудники Управления информационной безопасности ежедневно выполняют мониторинг списка уволенных сотрудников, через личный кабинет сотрудника СамГМУ (https://sso.samsmu.ru) и производят удаление учётных записей в случае увольнения сотрудника.

5.3 При увольнении сотрудника учетные записи во всех информационных ресурсах блокируются и удаляются.

## 6. Порядок работы с корпоративной электронной почтой

6.1 Корпоративный почтовый ящик сотрудника создается в автоматическом режиме на основании факта трудоустройства на следующий рабочий день после проведения приказа о приеме на работу, в учетной кадровой системе на период заключения с ним трудового договора или договора ГПХ.

6.2 Официальные почтовые ящики, почтовые ящики подразделений, технические почтовые ящики и тематические почтовые ящики создаются на основе заявки руководителя структурного подразделения, подаваемой в СТП. Обращение в СТП Университета осуществляется через сайт по адресу helpdesk.samsmu.ru. или на почту helpdesk@samsmsu.ru.

6.3 Каждый сотрудник может иметь только один адрес электронной почты вне зависимости от количества должностей, которые он занимает. Каждое подразделение может иметь только один адрес электронной почты в качестве почтового ящика подразделения.

6.4 Корпоративный почтовый ящик сотрудника блокируется в автоматическом режиме на основании факта прекращения трудовых отношений на следующий рабочий день после проведения приказа об увольнении в учетной кадровой системе.

6.5 Корпоративный почтовый ящик сотрудника уничтожается в автоматическом режиме на основании факта прекращения трудовых отношений по прошествии трех месяцев после проведения приказа об увольнении в учетной кадровой системе.