Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 1F216E3F8FE8145BF878D224B6CBDB95
Владелец: Колсанов Александр Владимирович
Действителен: с 13.11.2023 до 05.02.2025

УТВЕРЖДАЮ
Ректор ФГБОУ ВО СамГМУ
Минздрава России
профессор РАН

_____ А.В. Колсанов

Приказ № 19 от 05.02.2024 г.

ПОЛОЖЕНИЕ № 29П
по организации процесса получения усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности в ФГБОУ ВО СамГМУ Минздрава России

Самара, 2024

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Усиленная квалифицированная электронная подпись (УКЭП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. цифровой аналог собственноручной подписи.

Владелец УКЭП – лицо (сотрудник), которому в установленном настоящим Положением выдана электронная подпись, в соответствии с Федеральным законом № 63-ФЗ;

Компрометация – хищение, утрата, разглашение, несанкционированное копирование, связанные с ключевыми носителями;

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

СКЗИ – Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

ЦИБ – центр информационной безопасности;

УЦ – (Удостоверяющий центр) Юридическое лицо или индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

ТОФК – территориальные органы Федерального казначейства;

АУЦ УФК – аккредитованный удостоверяющий центр Управления Федерального казначейства;

ФНС России – Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соблюдением законодательства о налогах и сборах;

СМЭВ (система межведомственного электронного взаимодействия) – обеспечивает оказание государственных услуг, предоставляемых в электронном виде.

Машиночитаемая доверенность (МЧД) — это электронная доверенность на подписание электронных документов или совершение действий от лица руководителя Университета;

Структурированный электронный медицинский документ (СЭМД) – это электронный документ, имеющий общепринятый формат. С помощью СЭМД обеспечивается функциональная кооперация информационных систем, задействованных в процессах цифровизации медицины, что в итоге дает возможность сформировать единое пространство достоверных первичных медицинских сведений, которые в дальнейшем могут быть использованы в прикладных системах;

Реестр электронных медицинских документов (РЭМД) – это централизованная подсистема учета обращения медицинской документации и организации электронного документооборота в сфере охраны здоровья;

ЕМИАС СО – Единая медицинская информационно-аналитическая система Самарской области, которая обеспечивает доступ к электронным регистратурам и предоставляет пациентам и медицинским учреждениям инновационные инструменты для улучшения качества медицинского обслуживания.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящее Положение по организации процесса получения усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности в ФГБОУ ВО СамГМУ Минздрава России (далее – Положение) является локальным нормативным актом ФГБОУ ВО СамГМУ Минздрава России (далее - Университет) и определяет

порядок организации процесса получения усиленной квалифицированной электронной подписи (далее - УКЭП) в аккредитованном удостоверяющем центре Управления Федерального казначейства (далее - АУЦ УФК) и машиночитаемой доверенности (далее - МЧД) с использованием автоматизированных информационных систем и сервисов.

2.2. В соответствии с приказом Министерства здравоохранения Российской Федерации от 07.09.2020 г. № 947н «Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов» и распоряжения ФГБУ ВО СамГМУ Минздрава России от 20.12.2022 № 280-К «О формировании СЭМД и их регистрации в подсистеме РЭМД в системе ЕМИАС СО», уполномоченные сотрудники медицинских организаций должны подписывать электронные документы УКЭП.

2.3. В соответствии с Приказом Министерства финансов Российской Федерации от 15 апреля 2021 г. № 61н "Об утверждении унифицированных форм электронных документов бухгалтерского учета, применяемых при ведении бюджетного учета, бухгалтерского учета государственных (муниципальных) учреждений, и Методических указаний по их формированию и применению, по переходу на применение с 2023 г. организациями бюджетной сферы унифицированных форм электронных первичных учетных документов, используемых при ведении бюджетного учета, бухгалтерского учета государственных (муниципальных) учреждений», электронные документы, задействованных в электронном документообороте бухгалтерского учета, уполномоченные сотрудники должны подписывать УКЭП.

2.4. В случаях, при которых необходимо применение УКЭП, предусмотренных федеральными законами и принимаемыми с ними нормативными правовыми актами.

2.5. Настоящее Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
- Федеральным законом от 19.12.2022 № 536-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»
- Федеральным законом от 04.08.2023 № 457-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»

2.6. Документы в электронной форме, подписанные участником электронного взаимодействия с помощью УКЭП, признаются электронными

документами, равнозначными документу на бумажном носителе, подписанному собственноручной подписью и влекут такие же правовые последствия осуществляемых действий.

2.7. Наличие УКЭП обеспечивает электронным документам следующие свойства:

подлинность - подтверждение авторства документа;

целостность - документ не может быть изменен после подписания;

не отрицание авторства (неотрекаемость);

3. ПОРЯДОК ПОЛУЧЕНИЯ УКЭП В АУЦ УФК

3.1. Для получения сотрудником Университета УКЭП АУЦ УФК, при организации направления деятельности, выполнения должностных обязанностей, проректор по соответствующему направлению/руководитель структурного подразделения (сотрудников прямого или косвенного подчинения), подготавливает проект приказа «Об организации выпуска усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности», в соответствии с Приложением №1.

3.2. В Приказе «Об организации выпуска усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности» (далее - Приказ), указывается должность и ФИО сотрудника, на которого оформляется УКЭП (далее - Заявитель). Приказ утверждается Ректором Университета или лицом его замещающим (исполняющим обязанности). После регистрации, в отделе документационного обеспечения, Приказ передается в ЦИБ для формирования запроса на изготовление УКЭП.

3.3. Порядок формирования запроса на изготовление УКЭП, описан в пункте 4 настоящего Положения.

3.4. На основании Приказа «Об организации выпуска усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности» отдел кадров подготавливает и предоставляет в ЦИБ документ, подтверждающий право сотрудника Университета обращаться за получением УКЭП (Выписка из Приказа о назначении на должность), заверенный руководителем отдела кадров.

3.5. При одобрении запроса на изготовление УКЭП от АУЦ УФК, сотрудник ЦИБ уведомляет Заявителя о необходимости посещения ТОФК с оригиналами соответствующих документов, предусмотренных «Порядком реализации федеральным казначейством функций аккредитованного удостоверяющего центра и исполнения его обязанностей» утверждённым приказом Федерального Казначейства от 15 июня 2021 г. N 21н (далее - Регламент УФК).

3.6. Для получения УКЭП в ТОФК, необходимо предоставить

следующий пакет документов, предусмотренный Порядком реализации Федеральным казначейством функций удостоверяющего центра не позднее, чем через 5 рабочих дней после получения одобрения:

- оригинал заявления на изготовление УКЭП;
- оригинал документа, удостоверяющий личность сотрудника (заявителя) Университета;
- оригинал документа, подтверждающий право сотрудника Университета обращаться за получением УКЭП (Выписка из Приказа о назначении на должность).

3.7. Если пакет документов не будет предоставлен в указанный срок, запрос на УКЭП будет отклонен.

3.8. В случае отклонения запроса на изготовление УКЭП от АУЦ УФК, в связи с несоответствием данных, содержащихся в документах, необходимо руководствоваться инструкцией, согласно Приложения №2 данного Положения.

3.9. После внесённых изменений в базу данных ФНС, МВД, заявитель информирует ЦИБ о необходимости повторного направления запроса на изготовление УКЭП в АУЦ УФК.

4. ПОРЯДОК ФОМИРОВАНИЯ УКЭП

4.1. В соответствии с Регламентом УФК, создание УКЭП осуществляется с использованием информационной системы АУЦ УФК.

4.2. Заявитель предоставляет в ЦИБ:

- собственноручно подписанное заявление на изготовление УКЭП.

Регламентированные сроки подписания заявления - 2 рабочих дня.

4.3. После получения всех документов сотрудник ЦИБ направляет запрос посредством информационной системы АУЦ УФК.

4.4. После проверки документов в ТОФК и прохождения идентификации Заявителя, сертификат УКЭП направляется на корпоративную электронную почту ЦИБ.

4.5. ЦИБ уведомляет сотрудника о готовности УКЭП.

4.6. Владелец УКЭП обязан расписаться в:

- журнале ознакомления сотрудников с инструкцией пользователя, допущенного к обработке конфиденциальной информации с использованием СКЗИ;
- журнале выдачи парольной документации;
- журнале поэкземплярного учета СКЗИ;
- акте установки средства электронной подписи.

4.7. При работе с СКЗИ владельцем УКЭП необходимо руководствоваться инструкцией пользователя средств криптографической

защиты информации, в соответствии с Приложением №3.

5. ПОРЯДОК АННУЛИРОВАНИЯ УКЭП ПРИ СМЕНЕ ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ ИЛИ ПРЕКРАЩЕНИЯ ТРУДОВОЙ ДЕЯТЕЛЬНОСТИ

5.1. В соответствии со ст. 14 ч. 6 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», при увольнении, переводе, изменения должностных обязанностей сотрудника или ином случае, отделу кадров необходимо предоставить соответствующую информацию сотрудникам ЦИБ для инициирования процедуры аннулирования УКЭП. Срок информирования не позднее чем за 2 дня до осуществления соответствующих кадровых изменений.

5.2. Усиленная квалифицированная электронная подпись, выданная сотруднику от имени организации АУЦ УФК, аннулируется и считается недействительной с момента его увольнения, перевода, изменения должностных обязанностей или ином случае.

5.3. Владелец УКЭП обязан расписаться в:

- журнале выдачи парольной документации;
- журнале поэкземплярного учета СКЗИ;
- акте уничтожения средств электронной подписи.

6. МАШИНОЧИТАЕМАЯ ДОВЕРЕННОСТЬ

6.1. Машиночитаемая доверенность (МЧД) — электронный аналог бумажной доверенности на подписание электронных документов. Это файл в формате xml, в котором указана информация о доверителе, представителе (уполномоченный сотрудник) и полномочиях, которые он получает.

6.2. Основная задача МЧД — подтверждение того, что сотрудник, имеет право подписывать электронные документы от имени организации.

6.3. В МЧД используется специальный формат и требования к содержанию. Сведения из МЧД информационная система или сервис могут распознать автоматически.

6.4. МЧД формируется сотрудниками ЦИБ на определенных сервисах и ресурсах информационных систем, по запросу сотрудника, которому МЧД необходима для исполнения его должностных обязанностей.

6.5. При оформлении МЧД, сотрудник обязан зафиксировать факт получения МЧД путем собственноручной подписи, соответствующей записью в журнале «Оформления МЧД», с указанием информационной системы для которой она будет использоваться.

6.6. Хранение МЧД осуществляется в распределенном реестре ФНС России.

7. ОБЯЗАННОСТИ ВЛАДЕЛЬЦА УКЭП И МЧД

7.1. В соответствии со ст. 10 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», ответственность за получение, хранение и использование УКЭП лежит на владельце УКЭП;

7.2. В случае компрометации УКЭП, ответственность за последствия использования УКЭП и МЧД в информационных системах злоумышленниками, лежит на владельце УКЭП;

7.3. Пользователь обязан:

− соблюдать конфиденциальность УКЭП, не допускать разглашения, передачи, размножения;

− принимать все возможные и допустимые меры, предотвращающие нарушение конфиденциальности ключа проверки УКЭП и способствующие его защите;

− использовать УКЭП и МЧД в порядке, установленном законодательством Российской Федерации и настоящим Положением;

7.4. За нарушение установленных требований настоящего Положения владелец УКЭП несет персональную ответственность, в соответствии с действующим законодательством Российской Федерации.

Приложение №1

Об организации выпуска усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности

В целях исполнения требований Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Федерального закона от 19.12.2022 № 536-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», Федерального закона от 04.08.2023 № 457-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»; Приказ «Об утверждении Положения по организации процесса получения усиленной квалифицированной электронной подписи и оформления машиночитаемой доверенности» № ___ от _____

ПРИКАЗЫВАЮ:

1. Центру информационной безопасности организовать выпуск усиленной квалифицированной электронной подписи следующим сотрудникам:
    1. должность сотрудника Фамилия Имя Отчество.
    2. должность сотрудника Фамилия Имя Отчество.

При запросе информационной системы, оформить машиночитаемую доверенность.

2. Ответственность за получение, хранение и использование электронной подписи возложить на владельца электронной подписи.

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

Приложение №2

Инструкция по устранению выявленных ошибок, расхождений, несоответствий в данных, содержащихся в документах, предоставляемых для создания УКЭП и МЧД.

При выявлении ошибок, расхождений, несоответствий в данных, содержащихся в документах, предоставляемых для создания УКЭП и МЧД с данными, содержащимися в информационных базах ФНС России и проверяемых по сервисам СМЭВ, получателям УКЭП необходимо:

- самостоятельно обратиться в налоговый орган для их актуализации (или через представителя по доверенности);
- через Интернет-сервис ФНС России (https://nalog.ru) «Обратиться в ФНС России» - «Обратная связь»;
- через Интернет-сервис ФНС России «Личный кабинет» (при наличии) в разделе «Каталог обращения» - «Уточнить (изменить) сведения в личном кабинете».

При выявлении ошибок, расхождений, несоответствий в данных, содержащихся в информационных базах МВД России и проверяемых по сервисам СМЭВ, получателям УКЭП необходимо:

- Обратиться в орган МВД России по месту регистрации (нахождения) для проведения корректировки о паспортных данных в федеральной базе.

Воспользоваться онлайн сервисом:

- перейти по ссылке http://сервисы.гувм.мвд.рф/info-service.htm?sid=2000;
- заполнить серию и номер паспорта, а также код с картинки и нажать кнопку «Отправить запрос»;
- нажать кнопку «Сообщить об ошибке»;
- в поле «Описание ошибки» сообщить о существующей проблеме; Заполнить адрес электронной почты, ФИО и нажать кнопку «Отправить»;
- получить ответ «Ваше сообщение направлено».

Приложение №3

Инструкция
пользователей средств криптографической защиты информации

1. Общие положения

1.1. Инструкция пользователей средств криптографической защиты информации определяет основные обязанности и ответственность сотрудников ФГБОУ ВО СамГМУ Минздрава России, допущенных к обработке конфиденциальной информации (в том числе персональных данных) с использованием средств криптографической защиты информации (далее – СКЗИ);

1.2. Доступ пользователей к работе с СКЗИ осуществляется в соответствии с внутренними локально-нормативными актами в ФГБОУ ВО СамГМУ Минздрава России» и действующим законодательством РФ;

1.3. При необходимости использования ключа электронной подписи, для выполнения должностных обязанностей сотрудника, не являющегося владельцем ключа ЭП, оформляется Разрешение на использование ключа электронной подписи, согласно приложению №5 Приказа «Об утверждении состава и содержания организационных мер, необходимых для выполнения требований по обеспечению безопасности персональных данных при их обработке в информационных системах с использованием средств криптографической защиты информации в ФГБОУ ВО СамГМУ Минздрава России»;

1.4. Пользователи при выполнении своих функциональных (должностных) обязанностей, выполняют требования, предъявляемые к работе с использованием средств криптографической защиты информации (далее - СКЗИ), обеспечивают безопасность конфиденциальной информации и несут персональную ответственность за соблюдение требований руководящих документов по защите информации;

1.5. Под работами с использованием СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия, согласно технической документации к СКЗИ;

1.6. В ФГБОУ ВО СамГМУ Минздрава России для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации используется СКЗИ, позволяющее реализовать принцип абонентского шифрования и предусматривающие запись криптоключей на электронные ключевые носители многократного (долговременного) использования со строгой двухфакторной аутентификацией и защищенного хранения ключей электронной подписи, имеющих сертификат соответствия ФСБ;

1.7. В Инструкции пользователей средств криптографической защиты информации (далее – Инструкция) использованы следующие термины и определения:

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи;

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Несанкционированный доступ (НСД) — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для

публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Электронно-вычислительная машина (ЭВМ) – комплекс технических, аппаратных и программных средств, предназначенных для автоматической обработки информации, вычислений, автоматического управления;

Пользователи СКЗИ – сотрудники ФГБОУ ВО СамГМУ Минздрава России, непосредственно допущенные к работе с СКЗИ.

Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.8. Настоящая Инструкция разработана в целях исполнения:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;
- Федерального закона от 06.04.2011г. №63-ФЗ «Об электронной подписи»;
- Приказа ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
- Приказа ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

1.9. Требования Инструкции обязательны для выполнения всеми Пользователями СКЗИ ФГБОУ ВО СамГМУ Минздрава России.

2. Порядок работы со средствами криптографической защиты информации

2.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних

лиц к указанным средствам. В ФГБОУ ВО СамГМУ Минздрава России обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации;

2.2. Для получения доступа пользователям к работе с СКЗИ, сотруднику необходимо пройти инструктаж по информационной безопасности, ознакомиться с инструкцией пользователя СКЗИ и действующим законодательством Российской Федерации в сфере защиты персональных данных и конфиденциальной информации с использованием СКЗИ, с отметкой в «Журнале ознакомления сотрудников с инструкцией пользователя, допущенного к обработке конфиденциальной информации с использованием СКЗИ»;

2.3. Пользователь получает у ответственного сотрудника ЦИБ, на основании служебной записки от руководителя структурного подразделения на имя Директора института цифрового развития учетную запись для работы со специализированным программным обеспечением, с помощью которого будет подключен USB порт с защищенным носителем, на котором записан сертификат ключа проверки электронной подписи, с отметкой в Журнале выдачи парольной документации»;

2.4. В ФГБОУ ВО СамГМУ Минздрава России для организации и обеспечения безопасности хранения и эксплуатации электронной подписи, используются ключевые носители с двухфакторной аутентификацией. Защищенный носитель обеспечивает безопасное хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта. Пользователь при получении доступа к работе с электронной подписью, расписывается в «Журнале поэкземплярного учета СКЗИ» за эксплуатацию ключевого носителя и использование электронной подписи, оформляется акт установки СКЗИ;

2.5. Для начала работы с применением электронной подписи, пользователю необходимо запустить специализированное программное обеспечение, активировать определенный USB порт, зарегистрированный Ответственным сотрудником ЦИБ на его имя и ввести данные учетной записи, выданные Центром информационной безопасности. Персональные идентификаторы (парольные карточки) держать в тайне, не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

2.6. По окончанию работы с применением электронной подписи, необходимо деактивировать USB порт и выйти из специализированного программного обеспечения.

3. Обязанности пользователей СКЗИ

3.1. Пользователи СКЗИ обязаны:

- осуществлять эксплуатацию СКЗИ в соответствии с документацией на СКЗИ, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области;

- не разглашать конфиденциальную информацию, к которой они, допущены, в том числе сведения о криптоключах;

- выполнять общие требования, предъявляемые к работе с использованием средств криптографической защиты информации и обеспечивать безопасность конфиденциальной информации, в соответствии с установленным законодательством РФ, внутренними организационно-распорядительными документами ФГБОУ ВО СамГМУ Минздрава России и настоящей Инструкцией;

- соблюдать правила работы с СКЗИ и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информации при ее обработке;

- обеспечивать сохранность вверенной ключевой документации на них;

- получать ключевые носители под подпись в журнале поэкземплярного учёта СКЗИ;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- хранить ключевую информацию в специальном месте, гарантирующем их сохранность (в запирающемся ящике стола или сейфе).

3.2. **Пользователю СКЗИ запрещается**:

- разглашать содержимое ключевых носителей лицам, к ним не допущенным. Пользователь несет персональную ответственность за эксплуатацию ключевых носителей;

- передавать свой ключевой носитель другим лицам (исключение: передача ключевого носителя сотрудникам Центра информационной безопасности для осуществления настройки средств ЭП на рабочем месте Пользователя);

- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск ЭВМ), вносить изменения в файлы, находящиеся на ключевом носителе;

- сообщать третьим лицам информацию о владении ключом ЭП для какого-либо технологического процесса;

- осуществлять обработку персональных данных, с использованием СКЗИ в присутствии посторонних (не допущенных к данной информации) лиц;

- оставлять включенной без присмотра свою ЭВМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана;

3.3. Действия при компрометации сертификат ключей проверки электронной подписи.

3.3.1. Если у Пользователя СКЗИ появилось подозрение, что его ключевая информация попала или могла попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу, незамедлительно сообщить об этом сотрудникам Центра информационной безопасности (телефон: 8 (846) 374-10-04 (вн.: 4729, 4732, 4745, 4119), эл. почта: cib@samsmu.ru), написать служебную записку о факте компрометации персонального ключевого носителя на имя Директора Института цифрового развития.

3.3.2. В случае утери парольной карточки Пользователь СКЗИ обязан сообщить об этом в Центр информационной безопасности, написать объяснительную записку на имя Директора Института цифрового развития об утере.

4. Порядок прекращения работы пользователей с СКЗИ

4.1. В случае прекращения работы Пользователей с СКЗИ, необходимо оформить служебную записку на имя директора Института Цифрового развития для уничтожения средств криптографической защиты и оформления акта уничтожения СКЗИ;

4.2. В случае прекращения работы Пользователей с электронной подписью необходимо оформить служебную записку на имя директора Института Цифрового развития для аннулирования сертификата ключей проверки электронной подписи, прекращения доступа к информационным системам и удаления учетной записи. После уничтожения ключевой информации оформляется акт уничтожения и делается соответствующая

запись в «Журнале поэкземплярного учета СКЗИ». Пользователю необходимо сдать парольную карточку в Центр информационной безопасности под подпись в «Журнале выдачи парольной документации»;

5. Ответственность Пользователей

5.1. За нарушение установленных требований по эксплуатации криптосредств пользователь СКЗИ несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.