Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шуматов Валентин Борисович
Должность: Ректор
Дата подписания: 16.02.2024 13:52:46
Уникальный программный ключ:
1cef78fd73d75dc6ecf72fe1eb94fee387a2985d2657b784eec019bf8a794cb4

УТВЕРЖДАЮ
Руководитель
ФГБОУ ВО ТГМУ Минздрава России

(В.Б. Шуматов)
«29 » декабря 2023 г.

ПОЛОЖЕНИЕ
об использовании электронно-цифровой подписи

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение применяется в соответствии Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановление Правительства РФ от 29.06.2021 № 1044 «Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере электронной подписи», Приказ Минкомсвязи России от 14.09.2020 № 472 «Об утверждении Формата электронной подписи, обязательного для реализации всеми средствами электронной подписи», Приказ Минфина России от 12.01.2023 № 3н «О внесении изменений в Порядок выставления и получения счетов-фактур в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи, утвержденный приказом Министерства финансов Российской Федерации от 5 февраля 2021 г. № 14н», иными нормативно-правовыми актами российского законодательства в сфере применения электронных подписей.

1.2. Цель Положения – установить единые требования к подписанию первичных учетных электронных документов и регистров бухгалтерского учета сотрудниками учреждения и информационному обмену с третьими лицами, в том числе с государственными и муниципальными органами, государственными корпорациями, органами государственных внебюджетных фондов.

1.3. Требования настоящего Положения не распространяются на документы, для которых установлен собственный регламент подписания и обмена.

1.4. Порядок использования электронной подписи в системе ЭДО устанавливается локальными нормативными актами учреждения, приказами о назначении лиц, ответственных за осуществление обмена информацией (администраторов), об организации системы ЭДО. В приказе о назначении лиц, ответственных за осуществление обмена информацией (администраторов), указывается, какими видами электронной подписи (простой, квалифицированной) пользователь вправе заверять электронные документы. Подписание Уведомления об ознакомлении с данным Положением равнозначно к присоединению к действующей системе ЭДО.

1.5. Наделить правом подписи квалифицированной ЭЦП следующих должностных лиц:
- руководитель учреждения (первый проректор);
- председатель комиссии по поступлению и выбытию активов;
- председатель инвентаризационной комиссии;
- председатель приемочной комиссии;
- главный бухгалтер (заместитель главного бухгалтера);

- кассир;
- иные (в случае производственной необходимости)

1.6. Департамент информационных технологий
- обеспечить получение сертификатов ключей электронной цифровой подписи лицами, имеющими право подписи;
- организовать техническую и информационную поддержку рабочих мест, выделенных для совершения действий в системе ЭДО;
- организовать проведение инструктажа лиц, участвующих в системе ЭДО, о правилах эксплуатации средств электронной цифровой подписи.

1.7. К видам электронных подписей относится:
- простая электронная подпись;
- усиленная электронная подпись.
Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

1.7. Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

В качестве публичной части ключа простой ЭП используется уникальное имя учетной записи, применяемое для авторизации пользователя в системе ЭДО. В качестве конфиденциальной части ключа простой ЭП используется пароль к учетной записи.

1.8. Усиленная (неквалифицированная или квалифицированная) электронная подпись используется только в специально определенных целях, в установленном для этого законодательством или локальным правовым актом учреждения порядке, с использованием соответствующей инфраструктуры.

1.9. Возложить персональную ответственность за сохранение в тайне закрытых ключей электронной цифровой подписи и соблюдение правил эксплуатации средств электронной цифровой подписи на лиц, имеющих право подписи электронных документов соответствующей ЭП.

1.10. В случае, если от имени юридического лица действует его представитель, уполномоченный действовать от имени юридического лица на основании доверенности, выданной юридическим лицом в соответствии с гражданским законодательством Российской Федерации, электронный документ подписывается квалифицированной электронной подписью такого представителя юридического лица. Одновременно представляется доверенность от имени юридического лица. Данная доверенность, выданная в электронной форме от имени юридического лица, должна быть подписана квалифицированной электронной подписью, указанной в п. 1 ч. 1 ст. 17.2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или квалифицированной электронной подписью лица, которому выдана доверенность с правом передоверия, или квалифицированной электронной подписью нотариуса в случае, если доверенность, в том числе доверенность, выданная в порядке передоверия, удостоверена нотариусом.

В случае, если такая доверенность выдана в порядке передоверия, представляется также доверенность, допускающая возможность указанного передоверия, подписанная квалифицированной ЭЦП, указанной в п. 1 ч. 1 ст. 17.2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или квалифицированной ЭЦП нотариуса, если доверенность удостоверена нотариусом. Представление доверенности осуществляется посредством ее включения в пакет электронных документов, если иной порядок представления

такой доверенности не предусмотрен соглашениями при взаимодействии юридических лиц между собой или с индивидуальными предпринимателями, физическими лицами или нормативными правовыми актами федеральных органов исполнительной власти, принятыми в соответствии с требованиями к указанным соглашениям или нормативным правовым актам, которые вправе устанавливать Правительство Российской Федерации.

1.11. Электронная подпись используется в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью.

1.12. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

1.13. Электронные документы, подписанные электронной подписью и размещенные в системе ЭДО, равнозначны документам на бумажных носителях, подписанным собственноручной подписью. Пользователи ИС признают, что визуализация штампа ЭП при демонстрации документа в интерфейсе системы ЭДО, выполненная средствами ЭДО, является неоспоримым подтверждением факта подписания документа соответствующим владельцем ЭП (подлинность и неотрекаемость).

1.14. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

1.14.1. Ключевые носители должны иметь маркировку с учетным номером, присвоенным Администратором безопасности учреждения.

1.14.2. Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи.

1.14.3. Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной ЭЦП.

1.15. Лицами, обеспечивающими функционирование системы обмена информацией с использованием средств ЭП, являются:

администратор безопасности - назначается из числа сотрудников подразделений безопасности, который отвечает за изготовление (генерацию), выдачу и регистрацию в системе ЭДО ключей ЭП, осуществляет установку средств ЭП на автономные рабочие места (АРМ) владельца сертификата ключа ЭП, контролирует соблюдение правил обращения со средствами ЭП и ее ключами, ведет адресную книгу владельцев сертификатов ключей подписи и доводит до них ее содержание;

системный администратор (далее - Администратор) - назначается из числа сотрудников, осуществляющих техническое сопровождение АРМ работников учреждения или лиц,

осуществляющих техническое сопровождение АРМ на договорной основе, обеспечивает техническое сопровождение АРМ сотрудников, участвующих в обмене;

оператор - назначается из числа сотрудников подразделений, отвечающих за организацию документооборота, обеспечивает учет, прием, передачу информации, ее хранение.

1.16. Администратор формирует и ведет базу электронных форм, необходимых для получения, сопровождения, изменения, замены, отзыва сотрудниками учреждения электронных подписей, а также консультирует пользователей по вопросам заполнения указанных форм.

1.16.1. Администратор обязан разработать и применять политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее __ символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в __ позициях;
- личный пароль пользователь не имеет права никому сообщать;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать __ календарных дней.

Пароль пользователя системы ЭДО может быть изменен его владельцем в любой момент после авторизации в ИС. Рекомендуется изменять пароль не реже одного раза в три месяца.

Для снижения риска подбора пароля и несанкционированного использования другим лицом ключа ЭП рекомендуется не задавать пароли, использованные ранее.

1.16.2. Администратором при использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;
- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;
- на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;
- все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;
- необходимо предусмотреть меры, максимально ограничивающие доступ:

к системному реестру;
файлам и каталогам;
временным файлам;
журналам системы;
файлам подкачки;
кэшируемой информации (пароли и т.п.);

отладочной информации.

1.16.3. Администратору на средствах вычислительной техники необходимо:
- организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;
- регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы.

1.16.4. В случае подключения технических средств с установленными средствами квалифицированной электронной подписи к общедоступным сетям передачи данных Администратору необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

1.16.5. Администратору необходимо организовать и использовать:
- систему аудита, организовать регулярный анализ результатов аудита;
- комплекс мероприятий по антивирусной защите.

1.17. Администратору и пользователям запрещается:
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;
- вносить какие-либо изменения в программное обеспечение средств квалифицированной электронной подписи;
- записывать на ключевые носители постороннюю информацию;
- оставлять средства вычислительной техники с установленными средствами квалифицированной электронной подписи без контроля после ввода ключевой информации;
- использовать ключ электронной подписи и соответствующий сертификат ключа проверки электронной подписи, заявление на изменение статуса которого подано в течение времени, исчисляемого с момента подачи заявления на изменение статуса сертификата по момент официального информирования об изменении статуса сертификата либо об отказе в изменении статуса;
- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;
- удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

1.18. Владельцы ключа электронной подписи используют электронную подпись в соответствии с системой ЭДО, установленной графиком документооборота в учреждении и Положением об электронном документообороте.

1.19. Срок сертификата ключа проверки ЭП - 1 год с даты его выдачи удостоверяющим центром. По истечении этого срока сертификат необходимо продлить. Порядок продления срока действия ключа проверки ЭП описан в разделе 7 настоящего Положения

1.20. Допускается использование одной ЭП несколькими пользователями ЭП на одном рабочем месте. При этом каждый пользователь должен иметь соответствующие полномочия (положительное решение по заявлению на использование ЭП).

2. ОСНОВНЫЕ ПОНЯТИЯ

Владелец ключа электронной подписи - лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и локальным нормативным актом учреждения выдан ключ ЭП (далее - Владелец ключа ЭП).
Ключ электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - Ключ проверки ЭП).
Компрометация электронной подписи - любая ситуация, свидетельствующая об утрате (утеря, похищение, изъятие, передача третьему лицу) владельцем электронной подписи исключительного права владения и распоряжения ключом, и/или носителем, и/или PIN-кодом.
Отправитель электронного сообщения - инициатор информационного взаимодействия, который формирует и посылает электронное сообщение получателю или в другую систему управления документами.
Пользователь электронной подписи - сотрудник, наделенный правом согласно приказам о назначении лиц, ответственных за осуществление обмена информацией, об организации системы электронного документооборота подписывать документы в электронном виде, являющийся владельцем сертификата ключа проверки электронной подписи, в соответствии с положениями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее - Пользователь).
Реестр выданных ключей электронной подписи - хранящийся в системе ЭДО список уникальных последовательностей символов, содержащихся в выданных пользователям именах учетных записей и паролях.
Реестр отозванных ключей электронной подписи - хранящийся в ИС список пользователей ИС, ключи электронной подписи которых к моменту обращения к данному реестру были отмечены как недействительные
Сертификат ключа электронной подписи - электронный документ или документ на бумажном носителе, выданный уполномоченным удостоверяющим центром либо доверенным лицом уполномоченного удостоверяющего центра и подтверждающий принадлежность Ключа проверки электронной подписи Владельцу Ключа проверки электронной подписи (далее - сертификат).
Система электронного документооборота (система ЭДО) - аппаратно-программный комплекс, обеспечивающий обмен электронными сообщениями, в том числе с использованием электронных подписей.
Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание Ключа электронной подписи и Ключа проверки электронной подписи (далее - СЭП).
Транзакция - единичный шаг передачи сообщения (или: контейнера с документами) и электронной подписи требуемого вида в рамках документооборота определенного типа, который определяет набор передаваемых документов, ЭП, их отправителя и получателя.

Уполномоченный удостоверяющий центр - юридическое лицо, осуществляющее функции по созданию и выдаче ключей и/или сертификатов электронной подписи (далее - удостоверяющий центр).
Электронный документ (ЭД) - электронное сообщение определенного формата, соответствующее требованиям, установленным законодательством или соглашением сторон электронного документооборота для данного типа документов.
Электронный документооборот (ЭДО) - последовательность транзакций по обмену документами между участниками документооборота, обеспечивающая регламентированный процесс по обмену, отслеживанию, хранению документов.
Электронная подпись - уникальный набор электронно-цифровых символов, идентифицирующий лицо без его личного присутствия (далее - ЭП или Ключ ЭП).
ETOKEN, RUTOKEN, иной носитель - физический носитель для электронной подписи, выполненный в виде накопителя на флеш-памяти, вставляемой в USB-порт любого компьютера (далее - Носитель).
PIN-код (Пин-код) - пароль Пользователя для применения ЭП или для доступа к функционалу Носителя, предотвращающий их несанкционированное использование.
Обработка электронного документа - действия пользователя системы ЭДО с электронным
документом средствами ЭДО, включая, но не ограничиваясь: создание, проверка, подписание ЭП, информирование другого пользователя системы ЭДО о документе, подтверждение получения, ознакомление, создание копии на бумажном носителе, отклонение, удаление.

3. ОФОРМЛЕНИЕ ИЛИ ПОЛУЧЕНИЕ ЭП

3.1. Пользователи оформляют простую ЭП самостоятельно или с помощью Администратора и сообщают ее реквизиты Администратору безопасности.

3.2. Пользователи получают усиленную ЭЦП у Администратора в порядке и в сроки, которые установлены приказом о назначении лиц, ответственных за осуществление обмена информацией.

3.3.Учреждение самостоятельно финансирует оформление, приобретение, использование, обслуживание, продление, изменение, отзыв, уничтожение СЭП, ЭП, ключей проверки ЭП, их носителей, а также СЭДО.

3.4. Администратор в течение _____ (_____) рабочих дней с даты ознакомления с приказом о назначении лиц, ответственных за осуществление обмена информацией заказывает, приобретает ЭП, ключи проверки ЭП и передает носители с ними Пользователям.

Администратор ведёт реестр пользователей ЭП с указанием следующей информации:
- ФИО;
- структурное подразделение, должность;
- наименование информационной системы, в которой используется ЭП;
- инвентарный номер компьютера, на котором установлена ЭП и компоненты для работы с ЭП;
- номер рабочего кабинета, где установлен компьютер с компонентами ЭП;
- идентификатор ЭП;
- идентификатор ключевого носителя;
- срок действия сертификата ключа проверки ЭП.

3.5. Инструментарий, позволяющий работать с электронной подписью, может содержаться в облаке, на сервере учреждения, ETOKEN, RUTOKEN, ином Носителе, на котором записаны Ключ ЭП, Ключ проверки ЭП.

3.5.1. ETOKEN, RUTOKEN, иной Носитель, на котором записаны Ключ ЭП, Ключ проверки ЭП, защищен секретным PIN-кодом и предназначен только для Пользователя.

3.5.2. Передача ETOKEN, RUTOKEN, иного Носителя, на котором записаны Ключ ЭП, Ключ проверки ЭП и/или PIN-код, другим лицам запрещается, а при возникновении таких случаев ключи, PIN-коды, содержащиеся на ETOKEN, RUTOKEN, ином Носителе, считаются скомпрометированными и подлежат замене.

3.5.3. Пользователь ЭП и/или Ключа проверки ЭП, PIN-кода несет персональную ответственность за их сохранность и обеспечивает контроль срока их действия.

3.6. В течение _____ (_____) часов с даты получения заявки Пользователя Администратор настраивает для Пользователя систему ЭП.

3.7. Срок действия ЭП и/или Ключа проверки ЭП продлевается на основании приказа учреждения, инициированного владельцем ЭП через Администратора.

4. ОФОРМЛЕНИЕ ДОВЕРЕННОСТЕЙ ЭП

4.1. Учреждение вправе оформлять доверенности с использованием ЭП.

4.2. Электронные доверенности от имени учреждения, аналогичные доверенностям письменной формы, оформляются с использованием усиленной ЭП.

4.2.1. В случае оформления доверенности простой письменной формы лицо, обратившееся за удостоверением доверенности, обязано подписать документ в присутствии Администратора усиленной квалифицированной ЭЦП. Усиленная квалифицированная ЭЦП и ее принадлежность доверителю должны быть проверены Администратором в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

4.2.2. В случае оформления нотариальной доверенности лицо, обратившееся за удостоверением доверенности, обязано подписать документ в присутствии нотариуса усиленной квалифицированной ЭЦП. Усиленная квалифицированная ЭЦП и ее принадлежность доверителю должны быть проверены нотариусом в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ст. 44.2 Основ законодательства Российской Федерации о нотариате, утвержденных Верховным Советом Российской Федерации 11.02.1993 № 4462-1).

4.3. В случае оформления доверенностей для совершения от имени учреждения сделок определенной формы дополнительные требования, которым должна соответствовать форма электронной доверенности, устанавливаются по аналогии в порядке, предусмотренном ст. 160 Гражданского кодекса Российской Федерации.

4.4. При удостоверении электронной доверенности, предназначенной для совершения действий за границей, Организации или нотариусу необходимо учитывать требования п. 1 ст. 1209, ст. 1217.1 Гражданского кодекса Российской Федерации.

5. УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. Установка системы ЭП и проверки ее работоспособности должны производиться Администратором только в присутствии Пользователя.

5.2. Администратор в согласованное с Пользователем время обязан произвести установку и настройку СЭП на рабочем месте Пользователя, произвести инструктаж Пользователя по вопросам использования и работы СЭП, а также обязан выдать Носитель и первичный PIN-код Пользователю.

5.3. После установления Администратором СЭП Пользователь обязан проверить ее работоспособность, а также согласно полученным инструкциям ввести первичный PIN-код с последующим подписанием акта о выполненной Администратором работе.

5.4. После выполнения действий, указанных в п. п. 5.1 - 5.3 настоящего Положения, Пользователь подтверждает:
- установку СЭП, ее работоспособность;
- проведение инструктажа по использованию СЭП;
- осуществление произведенного (лично Пользователем) успешного тестирования работоспособности СЭП путем подписи Пользователя в *журнале установки СЭП.*

6. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ВЛАДЕЛЬЦА ЭЛЕКТРОННОЙ ПОДПИСИ

6.1. Учреждение вправе по своему усмотрению использовать любую информационную технологию и (или) технические средства, позволяющие выполнить требования Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» применительно к использованию конкретных видов электронных подписей.

6.2. Владелец электронной подписи обязан:
а) хранить в тайне Ключ ЭП и Ключ проверки ЭП, PIN-коды, принимать все возможные меры, предотвращающие нарушение их конфиденциальности;
б) использовать ЭП только в интересах учреждения;
в) в случае нарушения конфиденциальности ЭП (Ключа проверки ЭП, PIN-кода) или ее утери незамедлительно уведомить об этом Администратора безопасности;
г) при наличии оснований полагать, что конфиденциальность ЭП или Ключа проверки ЭП нарушена или такой Ключ и/или PIN-код скомпрометирован иным образом (утерян, похищен, отобран, передан третьему лицу), немедленно прекратить использование такого ключа самостоятельно или через Администратора безопасности обратиться в выдавший его удостоверяющий центр для прекращения его действия;
д) не использовать ключи ЭП, если они используются или использовались ранее другими владельцами сертификатов ключей подписи;
е) строго соблюдать установленный порядок обращения с ключевой документацией;
ж) немедленно докладывать непосредственному начальнику и в подразделение безопасности об утрате средств ЭП, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о ставших ему известными попытках третьих лиц получить сведения о закрытых ключах, других фактах, которые могут привести к компрометации ключа ЭП, а также о причинах и условиях возможной утечки таких сведений.

6.3 Владелец электронной подписи имеет право:

- обращаться к Администратору безопасности для аннулирования (отзыва), приостановки (возобновления) действия принадлежащего ему ключа электронной подписи;
- в случае необходимости замены, восстановления ключа электронной подписи обратиться к Администратору безопасности с соответствующей просьбой и получить новый ключ электронной подписи;
- обращаться к руководству учреждения для разбора конфликтных ситуаций (споров), возникающих при применении электронной подписи в системе ЭДО.
- допускать до работы с ЭП администратора только в случаях проведения им работ по установке, настройке или восстановлению работы компонентов ЭП и доступа к информационным системам.

7. СОПРОВОЖДЕНИЕ, ПРОДЛЕНИЕ СРОКА ДЕЙСТВИЯ, ЗАМЕНА ЭП

7.1. В случаях сбоев, отказов в работе ЭП Пользователь обращается к Администратору, который обязан немедленно принять меры по выявлению их причин и восстановлению функционирования ЭП.

7.2. Для продления срока действия ЭП или ее замены Администратор на основании служебной записки Пользователя, подписанной руководителем соответствующего структурного подразделения, подает запрос в удостоверяющий центр в течение _____ (_____) дней с момента получения записки.

7.3. Администратор после получения из удостоверяющего центра сведений о продлении срока действия ЭП или замененной ЭП осуществляет регистрацию данной информации в *журнале регистрации ЭП* и при необходимости осуществляет действия, предусмотренные разд. 3 - 5 настоящего Положения.

7.4. Замена Носителя производится в случае его физического повреждения или утраты. В случае необходимости замены Носителя Пользователь сдает поврежденный Носитель ЭП Администратору со служебной запиской за подписью руководителя соответствующего структурного подразделения. Администратор безопасности в 7-дневный срок с даты поступления служебной записки от Пользователя заменяет Носитель ЭП.

7.5. Пользователь проверяет работоспособность Носителя и подтверждает его получение в работоспособном состоянии путем проставления подписи в *журнале регистрации ЭП*.

7.6. В случае компрометации Ключей ЭП, и/или Ключей проверки ЭП, и/или PIN-кода (утери, похищения, изъятия, передачи третьему лицу) их замена осуществляется Администратором в соответствии со служебной запиской Пользователя за подписью руководителя соответствующего структурного подразделения в течение ____ (_____) рабочих дней с даты получения служебной записки.

7.7. Администратор, получивший сообщение от Пользователя о компрометации Ключей ЭП, и/или Ключей проверки ЭП, и/или PIN-кода (утере, похищении, изъятии, передаче третьему лицу), регистрирует в *журнале регистрации ЭП* фактическое время и причину прекращения действия ЭП, а также информирует Пользователя о таком зарегистрированном фактическом времени.

7.8. Для оформления (получения) новой ЭП Пользователю необходимо выполнить действия, предусмотренные п. 3.1 (3.2) Положения.

8. ОТЗЫВ ЭЛЕКТРОННОЙ ПОДПИСИ

8.1. Отзыв ЭП Пользователя производится Администратором в случае прекращения действия полномочий Пользователя по подписанию электронных документов.

8.2. Основанием для действий Администратора по аннулированию ЭП Пользователя является локальный нормативный акт учреждения, изменяющий перечень лиц и/или полномочия этих лиц, ответственных за электронный обмен данными.

8.3. В случае необходимости отзыва ЭП Администратор готовит заявление в удостоверяющий центр (по форме удостоверяющего центра) с указанием даты отзыва, причины отзыва, подписанное руководителем учреждения (лицом, его замещающим).

8.4. В течение _____ (_____) часов с момента подписания заявления об отзыве ЭП Администратор информирует удостоверяющий центр об отзыве ЭП с указанием причины отзыва.

8.5. После отзыва ЭП Администратор, получивший письменное подтверждение об отзыве, должен зарегистрировать в журнале регистрации ЭП время и причину отзыва.

8.6. После отзыва ЭП Пользователь обязан немедленно сдать выданный ему Носитель Администратору.

8.7. Администратор удаляет с Носителя всю информацию.

9. ПОРЯДОК РАБОТЫ С ДОКУМЕНТАМИ В СЭДО С ИСПОЛЬЗОВАНИЕМ ЭП

9.1. Работа пользователя в системе ЭДО с использованием ЭП осуществляется в соответствии с Инструкцией пользователя по работе с ЭП в системе электронного документооборота Организации.

9.2. Подписание (визирование) электронных документов с использованием ЭП может дублироваться подлинными подписями согласующих лиц на бумажных носителях.

9.3. Подписанный ЭП электронный документ направляется в папку «Для регистрации» для дальнейшей регистрации в установленном порядке.

9.4. При поступлении на подпись проектов исходящих документов проверка наличия и корректности ЭП ответственного исполнителя (подразделения), а также наличия и корректности согласующих ЭП соисполнителей (подразделений) в системе ЭДО осуществляется референтами отдела обеспечения деятельности руководства учреждения.

9.5. При наличии замечаний проекты исходящих документов возвращаются на доработку исполнителям.

9.6. Работники, осуществляющие регистрацию и отправку исходящего документа, завизированного с применением ЭП, проверяют наличие виз согласования на электронном документе.

10. ТРЕБОВАНИЯ ПРИ ОРГАНИЗАЦИИ ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ НОСИТЕЛЕЙ, КЛЮЧЕЙ ЭП

10.1. Порядок хранения и использования Носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

10.2. Носитель/Ключ ЭП/Ключ проверки ЭП являются персональными, выдаются Пользователям под подпись и не подлежат передаче другим лицам. Пользователь должен обеспечить все необходимые меры, исключающие несанкционированный доступ к выданному ему Носителю ЭП.

10.3. При работе с ЭП запрещается:
- производить несанкционированное копирование Носителей ключевой информации;
- передавать Носители ключевой информации другим лицам;
- выводить Ключи ЭП на экран монитора или принтер;
- использовать Носитель ключевой информации на других автоматизированных рабочих местах;
- записывать на Носитель ключевой информации посторонние файлы.

10.4. Владельцы Носителей/Ключей несут персональную ответственность за безопасность (сохранение в тайне) ключей ЭП и обязаны обеспечить их сохранность, неразглашение и нераспространение.

10.5. Виновный Пользователь несет ответственность за негативные последствия, наступившие в результате несоблюдения своих обязанностей или нарушения установленных требований.

Приложение 1

Уведомление
об ознакомлении с Положением об использовании электронной подписи в учреждении

Я, _____
(ФИО, должность)
_____,
именуемый в дальнейшем «Работник», настоящим подтверждаю, что ознакомился с Положением об использовании простой электронной подписи в ФГБОУ ВО ТГМУ Минздрава России, а именно: Работник признает равнозначность своей простой электронной подписи собственноручной подписи на бумажном носителе и заявляет о присоединении к соглашению об участии во внутреннем электронном документообороте с использованием электронной подписи на условиях Положения об использовании электронной подписи в ФГБОУ ВО ТГМУ Минздрава России в соответствии со ст. 428 Гражданского кодекса РФ («Договор присоединения») с «__» _____ 202_ года.

«_____»_____202__ г. _____ (_____).
Подпись расшифровка