

**СОГЛАСОВАНО**

Советом АНО СПО «ММК»

(протокол от «11» марта 2026г. № 3)

**УТВЕРЖДАЮ**

Генеральный директор

АНО СПО «ММК»



П.Г. Харитоновна

от «11» марта 2026г.

## **ПОЛОЖЕНИЕ**

**ОБ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ  
ОБРАБОТКИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ДОКУМЕНТОВ,  
РАЗМЕЩАЕМЫХ НА ОФИЦИАЛЬНОМ САЙТЕ  
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОРГАНИЗАЦИИ  
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«МНОГОПРОФИЛЬНЫЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»**

**Содержание**

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 1. Общие положения .....                                                | 3  |
| 2. Термины и определения .....                                          | 7  |
| 3. Положения .....                                                      | 11 |
| 4. Контроль за выполнением требований настоящего положения.....         | 20 |
| 5. Заключительные положения .....                                       | 20 |
| Приложение 1 Форма заявления на использование электронной подписи ..... | 21 |
| Приложение 2 Согласие .....                                             | 22 |
| Приложение 3 Перечень документов.....                                   | 23 |

## 1. Общие положения

- 1.1. Настоящее Положение об использовании электронной подписи в Автономной некоммерческой организации среднего профессионального образования «Многопрофильный медицинский колледж» (далее - Положение), (далее - Организация, Колледж) является локальным нормативным актом и определяет порядок и условия работы сотрудников с электронными документами в Информационной Системе (далее - ИС), непосредственно связанными с их трудовой деятельностью, с применением электронной подписи (далее - ЭП).
- 1.2. Настоящее Положение разработано в соответствии со следующими нормативными документами.

**Электронная подпись.** Действующие нормативные акты, регулирующие вопросы получения и использования электронной подписи:

- Федеральный закон от 29.12.2012 № 273-ФЗ (последняя редакция) «Об образовании в Российской Федерации»;
- Федеральный закон от 27.07.2010 № 210-ФЗ (последняя редакция) «Об организации предоставления государственных и муниципальных услуг»;
- Федеральный закон от 06.04.2011 № 63-ФЗ (последняя редакция) «Об электронной подписи»;
- Постановление Правительства РФ от 28.11.2011 № 976 (последняя редакция) «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи»;
- Постановление Правительства РФ от 25.06.2012 № 634 (последняя редакция) «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг» (вместе с «Правилами определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг»);
- Постановление Правительства РФ от 25.08.2012 № 852 (последняя редакция) «Об утверждении Правил использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг и о внесении изменения в Правила разработки и утверждения административных регламентов предоставления государственных услуг»;
- Постановление Правительства РФ от 09.02.2012 № 111 (последняя редакция) «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи» (вместе с «Правилами использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой», «Требованиями к обеспечению совместимости средств электронной подписи при организации электронного взаимодействия органов исполнительной власти и органов местного самоуправления между собой»);
- Постановление Правительства РФ от 25.01.2013 № 33 (последняя редакция) «Об использовании простой электронной подписи при оказании государственных и

муниципальных услуг»;

- Приказ Минкомсвязи России от 13.04.2012 № 107 (последняя редакция) «Об утверждении Положения о федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»;
- Приказ ФАПСИ от 13.06.2001 № 152 (последняя редакция) «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»;
- Приказ ФСБ России от 27.12.2011 № 795 (последняя редакция) «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- Приказ ФСБ России от 27.12.2011 № 796 (последняя редакция) «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
- Приказ Минцифры России от 08.11.2021 № 1138 (последняя редакция) «Об утверждении Порядка формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации»;
- Приказ Минцифры России от 18.08.2021 № 857 (последняя редакция) «Об утверждении единых требований к формам доверенностей, необходимых для использования квалифицированной электронной подписи».

**Электронные торги.** Действующие нормативные акты, регулирующие государственные и коммерческие закупки, а также реализацию имущества с использованием электронной подписи:

- Федеральный закон от 05.04.2013 № 44-ФЗ (последняя редакция) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;
- Федеральный закон от 21.12.2001 № 178-ФЗ (последняя редакция) «О приватизации государственного и муниципального имущества»;
- Федеральный закон от 18.07.2011 № 223-ФЗ (последняя редакция) «О закупках товаров, работ, услуг отдельными видами юридических лиц»;
- Федеральный закон от 26.10.2002 № 127-ФЗ (последняя редакция) «О несостоятельности (банкротстве)»;
- Постановление Правительства РФ от 08.06.2018 № 656 (последняя редакция) «О требованиях к операторам электронных площадок, операторам специализированных электронных площадок, электронным площадкам, специализированным электронным площадкам и функционированию электронных площадок, специализированных электронных площадок, подтверждении соответствия таким требованиям, об утрате юридическим лицом статуса оператора электронной площадки, оператора специализированной электронной площадки»;
- Постановление Правительства РФ от 25.12.2018 № 1663 (последняя редакция) «Об утверждении Положения об особенностях документооборота при осуществлении

закрытых конкурентных закупок в электронной форме и порядке аккредитации на электронных площадках для осуществления закрытых конкурентных закупок»;

- Постановление Правительства РФ от 27.08.2012 № 860 (последняя редакция) «Об организации и проведении продажи государственного или муниципального имущества в электронной форме» (вместе с «Положением об организации и проведении продажи государственного или муниципального имущества в электронной форме»);
- Постановление Правительства РФ от 28.02.2019 № 223 (последняя редакция) «Об особенностях проведения закрытых электронных процедур и порядке аккредитации на специализированных электронных площадках» (вместе с «Положением об особенностях проведения закрытых электронных процедур и порядке аккредитации на специализированных электронных площадках»);
- Постановление Правительства РФ от 10.05.2018 № 564 (последняя редакция) «О взимании операторами электронных площадок, операторами специализированных электронных площадок платы при проведении электронной процедуры, закрытой электронной процедуры и установлении ее предельных размеров» (вместе с «Правилами взимания операторами электронных площадок, операторами специализированных электронных площадок платы с лица, с которым заключается контракт по результатам проведения электронной процедуры, закрытой электронной процедуры»);
- Постановление Правительства РФ от 30.05.2018 № 626 (последняя редакция) «О требованиях к договору специального счета и порядку использования имеющегося у участника закупки банковского счета в качестве специального счета, требованиях к условиям соглашения о взаимодействии оператора электронной площадки с банком»;
- Распоряжение Правительства РФ от 28.04.2018 № 824-р (последняя редакция) «О создании единого агрегатора торговли»;
- Приказ Минэкономразвития России от 23.07.2015 № 495 (последняя редакция) «Об утверждении Порядка проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, Требований к операторам электронных площадок, к электронным площадкам, в том числе технологическим, программным, лингвистическим, правовым и организационным средствам, необходимым для проведения торгов в электронной форме по продаже имущества или предприятия должников в ходе процедур, применяемых в деле о банкротстве, внесении изменений в приказ Минэкономразвития России от 05.04.2013 № 178 и признании утратившими силу некоторых приказов Минэкономразвития России».

**Электронный документооборот.** Действующие нормативные акты, связанные с правовым регулированием электронного документооборота:

- Федеральный закон от 27.07.2010 № 210-ФЗ (последняя редакция) «Об организации предоставления государственных и муниципальных услуг»;
- Федеральный закон от 27.07.2006 № 149-ФЗ (последняя редакция) «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ от 22.09.2009 № 754 (последняя редакция) «Об утверждении Положения о системе межведомственного электронного документооборота»;
- Приказ Минфина России от 05.02.2021 № 14н (последняя редакция) «Об утверждении Порядка выставления и получения счетов-фактур в электронной форме по

телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи».

**Электронная отчетность.** Действующие нормативные акты, регулирующие использование электронной подписи при сдаче отчетности через информационно-телекоммуникационную сеть «Интернет»:

- Постановление Правительства РФ от 26.12.2011 № 1137 (последняя редакция) «О формах и правилах заполнения (ведения) документов, применяемых при расчетах по налогу на добавленную стоимость»;
- Приказ СФР от 06.07.2023 № 1319 (последняя редакция) «О защищенном обмене документами в электронном виде с применением электронной цифровой подписи для целей обязательного социального страхования»;
- Приказ ФНС РФ от 17.12.2008 № ММ-3-6/665@ (последняя редакция) «Об утверждении Порядка ведения единого пространства доверия сертификатам ключей ЭЦП»;
- Приказ ФНС России от 30.01.2012 № ММВ-7-6/36@ (последняя редакция) «Об утверждении форматов представления документов, используемых при выставлении и получении первичных и иных документов хозяйствующих субъектов, включая счета-фактуры, в электронной форме по телекоммуникационным каналам связи с применением электронной подписи».

**Защита информации.** Действующие нормативные акты, содержащие правовые основы защиты информации:

- Закон РФ от 21.07.1993 № 5485-1 (последняя редакция) «О государственной тайне»;
- Федеральный закон от 29.07.2004 № 98-ФЗ (последняя редакция) «О коммерческой тайне»;
- Федеральный закон от 27.07.2006 № 149-ФЗ (последняя редакция) «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ (последняя редакция) «О персональных данных»;
- Постановление Правительства РФ от 16.04.2012 № 313 (последняя редакция) «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- Постановление Правительства РФ от 01.11.2012 № 1119 (последняя редакция) «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Указ Президента РФ от 06.03.1997 № 188 (последняя редакция) «Об утверждении Перечня

сведений конфиденциального характера»;

- Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 (последняя редакция) «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;
- Приказ ФСТЭК России от 18.02.2013 № 21 (последняя редакция) «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

## **2. Термины и определения**

**Владелец сертификата ключа проверки электронной подписи** - лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи.

**Ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи.

**Вручение сертификата ключа проверки электронной подписи** - передача доверенным лицом удостоверяющего центра, изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

**Заявка на регистрацию ключа** - служебное сообщение, содержащее новый открытый ключ, подписанное электронной цифровой подписью.

**Информационная система общего пользования (ИС)** - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

**Квалифицированная электронная подпись (КЭП)** - аналог собственноручной подписи руководителя. Технически КЭП это файл с данными владельца подписи и информацией о подписанном документе в зашифрованном виде. КЭП используется для участия в электронных торгах, работы в госсистемах и на госпорталах, отчетности, обмена электронными документами с сотрудниками и партнерами. Собственноручная и электронная подписи имеют одинаковую юридическую силу.

КЭП соответствует следующим требованиям:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи;
- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с законом.

Работник организации получает КЭП самостоятельно в удостоверяющем центре на своё имя как физическое лицо. Ключ защищён от передачи другим лицам, что повышает безопасность операций.

**Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат)** - сертификат ключа проверки электронной подписи,

соответствующий требованиям, установленным Федеральным законом № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

**Классификатор полномочий** - портал с перечнем полномочий сотрудника, которые следует указывать в машиночитаемой доверенности. Каждое полномочие содержит наименование, дату включения в классификатор и уникальный идентификационный номер - именно он дает право подписи. Классификатор позволяет быстро определить полномочия сотрудника и корректно отобразить их в МЧД. (Актуальный классификатор полномочий размещен на сайте «Единой системы нормативной справочной информации (ЕСНСИ) Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

**Ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

**Ключ шифрования** - ключ, предназначенный для закрытия электронного документа при электронных взаимодействиях.

**Ключевой носитель (носитель ключевой информации) (НКИ)** - физический носитель для ЭП. Выполнен в виде флэш-карты, вставляемой в USB-порт любого компьютера.

**Компрометация закрытого ключа ЭП** - любая ситуация, свидетельствующая об утере владельцем или пользователем ЭП исключительного права владения и распоряжения ключевым носителем и/или его PIN-кодом. Причины компрометации ключа ЭП могут быть совершенно различными: от невнимательности владельца до хакерской атаки. Поэтому, обладая ключевым носителем, нужно знать его характеристики, чтобы лучше понимать, как и когда ваш ключ может быть скомпрометирован. За компрометацию ключа несет ответственность не только ее владелец, но и удостоверяющий центр.

**Компрометация ключевой информации** - утрата, хищение, несанкционированное копирование или подозрение на копирование носителя ключевой информации НКИ или любые другие ситуации, при которых достоверно не известно, что произошло с НКИ. К компрометации ключевой информации также относится увольнение сотрудников, имевших доступ к ключевой информации.

**Корпоративная информационная система (КИС)** - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

**Крипто-программа** - компьютерная программа, позволяющая осуществлять операции с ЭП: устанавливать сертификаты, проверять подписи других работников под документом и др.

**Машиночитаемая доверенность (МЧД)** - доверенность в электронном виде в формате XML, подписанная усиленной квалифицированной электронной подписью (УКЭП) руководителя организации, где описаны полномочия сотрудника организации подписывать документы от имени организации и позволяет сотрудникам предоставлять интересы организации в электронном документообороте с контрагентами, сдавать отчетность, выставять счета, оформлять закрывающие документы. Одна МЧД может выдаваться сразу на группу сотрудников организации, а в одной МЧД можно указать сразу несколько полномочий: по одной доверенности сотрудник может выполнять разные операции. Подписывать документы без МЧД могут только руководители организаций. С 01.09.2023 юридические лица обязаны передавать все выданные МЧД в единый



реестр машиночитаемых доверенностей ФНС России. Хранение МЧД осуществляется в едином блокчейн хранилище машиночитаемых доверенностей распределенного реестра ФНС России. Помимо блокчейна хранить доверенность можно в информационных системах доверителя, оператора ЭДО, а также федеральных органов исполнительной власти. Главное, чтобы хранение МЧД было публичным и можно было без проблем получить информацию о статусе документа.

**PIN-код** - пароль доступа пользователя ЭП к функционалу ключевого носителя. Предотвращает несанкционированное использование ключевого носителя. Требования к паролю доступа: длина пароля должна быть не меньше 8 символов, пароль должен включать в себя цифры и буквы в разных регистрах, а также специальные символы, не должны использоваться стандартные и легко вычисляемые комбинации символов, при смене пароля новый должен отличаться от старого как минимум по 4 знакам, периодичность смены пароля - не реже 6 месяцев.

**Подтверждение владения ключом электронной подписи** - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

**Пользователь ЭП** - работник университета, наделенный полномочиями подписывать документацию с использованием ЭП.

**Рабочее место пользователя ЭП** - кабинет или аудитория, на территории университета оснащённая компьютерным оборудованием для использования ЭП.

**Сертификат ключа проверки электронной подписи** - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

**Сертификация организации (юрлица)** - с 01.09.2023 выдаются два типа сертификата организации (юрлица) - 1) на руководителя (выдается один на организацию) и 2) обезличенный сертификат без реквизитов пользователя, который содержит в себе только реквизиты юрлица (выдается по количеству информационных систем). Оба типа сертификата организации выдаются только на защищенном токене в УЦ ФНС, УЦ Федерального казначейства и УЦ ЦБ, при этом: УЦ ФНС обеспечивает сертификатами все организации, УЦ Федерального казначейства выдает сертификаты всем бюджетным организациям УЦ ЦБ выдает сертификаты всем кредитным и финансовым организациям.

**Сертификация ключа** - процедура заверения (подписания) открытой части регистрируемого ключа электронной цифровой подписью.

**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.

**Средства удостоверяющего центра** - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

**Удостоверяющий центр (УЦ)** - юридическое лицо, 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 законом. В обязанности УЦ входят следующие:

- удостоверить личность человека, который обратился за сертификатом электронной подписи;
- изготовить и выдать сертификат, в который включены данные о владельце сертификата и его открытый ключ проверки;
- управлять жизненным циклом сертификата (выпуск, приостановление, возобновление, окончание срока действия).

**Усиленная квалифицированная электронная подпись (УКЭП)** - цифровой аналог собственноручной подписи. Документы, подписанные от руки или с помощью УКЭП имеют равнозначную ценность, это файл, в котором хранится зашифрованная информация, подтверждающая личность человека и подлинность подписанного документа.

**Участники электронного взаимодействия** - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

**Шифрование** - специализированный метод защиты информации от ознакомления с ней третьих лиц, основанный на кодировании информации по алгоритму ГОСТ 28147-89 с использованием соответствующих ключей.

**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.

**Владелец простой электронной подписи** - сотрудник Организации, подписавший Уведомление об ознакомлении с настоящим Положением и использующий имя пользователя и пароль для авторизации в ИС.

**Внутренний электронный документ (далее - Документ)** - документ одного из типов документов, приведенных в [Приложении 3](#) к настоящему Положению, созданный в ИС в электронной форме и подписанный электронной подписью сотрудника (электронными подписями сотрудников) Организации.

**Реестр выданных ключей электронной подписи** - хранящийся в ИС 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.

**Простая электронная подпись (ПЭП)/(неквалифицированная электронная подпись (НЭП))** - информация в электронной форме в ИС, возникающая в момент выполнения владельцем электронной подписи команды подписания Документа в интерфейсе ИС, подтверждающая подлинность Документа и/или факт ознакомления владельца ПЭП с Документом, которая взаимно однозначно связывается с Документом и владельцем подписи.

**Штамп ПЭП** - визуальная отметка об электронной подписи, включающая реквизиты ПЭП, которая автоматически создается средствами ИС при открытии (визуализации) документа, подписанного ПЭП, в интерфейсе ИС. Время формирования ПЭП отображается в штампе по часовому поясу пользователя ИС.

**Обработка электронного документа** - действия пользователя ИС с электронным документом средствами ИС, включая, но не ограничиваясь: создание, проверка, подписание ПЭП,

информирование другого пользователя ИС о документе, подтверждение получения, ознакомление, создание копии на бумажном носителе, отклонение, удаление.

### 3. Положения

#### 3.1. Общие положения.

- 3.1.1. Единая система идентификации и аутентификации является информационным элементом инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.
- 3.1.2. Реализация условий применения электронной подписи обеспечивает придание юридической силы внутренним электронным документам образовательной организации в информационных системах, требующим личной подписи генерального директора образовательной организации и операциям с ними.
- 3.1.3. Наличие электронной подписи в электронном документе подтверждает авторство данного документа и сохраняет его целостность. Таким образом, документ, содержащий электронную подпись, не может быть изменен после подписания.
- 3.1.4. Для подписания документов в информационных системах используется усиленная квалифицированная электронная подпись в виде присоединяемой к документу информации, генерируемой программой или информационной системой совместно с пользователем или по его команде.
- 3.1.5. В качестве публичной части ключа электронной подписи в образовательной организации используется уникальное имя учетной записи, применяемое для авторизации пользователя в информационной системе.
- 3.1.6. В качестве конфиденциальной части ключа электронной подписи в образовательной организации используется пароль к учетной записи.
- 3.1.7. Изготовление (генерацию), выдачу и регистрацию в информационной системе имен пользователей и паролей осуществляет системный администратор.
- 3.1.8. Создание и выдачу сертификатов ключей проверки электронных подписей осуществляет Удостоверяющий центр на основании соглашения между удостоверяющим центром и образовательной организацией.
- 3.1.9. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.
- 3.1.10. В случае необходимости использования ЭП работником организации для выполнения своих должностных (функциональных) обязанностей, данный работник должен обратиться с заявлением на использование ЭП ([Приложение 1](#)) на имя генерального директора колледжа.
- 3.1.11. В случае утверждения (согласования) генеральным директором колледжа заявления, оно передаётся системному администратору для выполнения им работ по

формированию реестра пользователей ЭП и подготовке рабочего места для работы с ЭП.

3.1.12. В случае получения отказа в использовании ЭП по поступившему от работника заявлению, данное заявление обрабатывается в соответствии с правилами документооборота и делопроизводства колледжа.

3.1.13. Системный 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.

3.1.14. Работник колледжа, получивший положительное решение на использование ЭП, самостоятельно производит сбор пакета документов на выпуск ЭП (паспорт, СНИЛС и ИНН - в случае создания новой ЭП). Доверенность на получение документов и ЭП в удостоверяющем центре, делается по соответствующей форме на работника, подавшего заявление на использование ЭП.

3.1.15. Пользователи ЭП имеют право допускать до работы с ЭП системного администратора только в случаях проведения им работ по установке, настройке или восстановлению работы компонентов ЭП и доступа к информационным системам.

3.1.16. Системному администратору запрещается самостоятельно подписывать какие-либо документы ЭП.

3.1.17. Срок сертификата ключа проверки ЭП - 1 год с даты его выдачи. По истечении этого срока сертификат необходимо продлить. Порядок продления срока действия ключа проверки ЭП описан в подпункте 4.5. настоящего положения.

3.1.18. ЭП должна использоваться только на рабочем месте пользователя ЭП, указанном в заявлении ([Приложение 1](#)).

3.1.19. Сотрудникам колледжа, не являющимся владельцами ЭП, запрещено использование ЭП.

## 3.2. Права и обязанности владельца (пользователя) ЭП.

3.2.1. Владелец ЭП имеет право:

- вести электронные документы, подписанные электронной подписью при размещении их на сайте образовательной организации, согласно приказу №831 Федеральной службы по надзору в сфере образования и науки «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации», которые должны соответствовать условиям ст.6 №63-ФЗ «Об электронной подписи» для их признания равнозначными документам на бумажном носителе, подписанным собственноручной подписью;
- обращаться к ответственному за техническую поддержку информационной

системы для аннулирования (отзыва), приостановки (возобновления) действия принадлежащего ему ключа электронной подписи;

- в случае необходимости замены, восстановления ключа электронной подписи обратиться к ответственному за техническую поддержку информационной системы с соответствующей просьбой и получить новый ключ электронной подписи;
- обращаться к руководству колледжа для разбора конфликтных ситуаций (споров), возникающих при применении ЭП в информационной системе.

### 3.2.2. Владелец ЭП обязан:

- вести обработку внутренних электронных документов в информационной системе в соответствии со своими должностными обязанностями;
- принимать все возможные меры для предотвращения несанкционированного использования своего ключа электронной подписи;
- ни при каких условиях не передавать ключевой носитель с PIN-кодом сторонним лицам (включая работников университета);
- обеспечить сохранность и конфиденциальность ключей электронной подписи, не допускать использование ключей электронных подписей другими работниками университета;
- при утере или пропаже ключевого носителя, компрометации ключа электронной подписи незамедлительно обратиться к своему непосредственному руководителю, системному администратору для приостановки действия принадлежащего ему ключа электронной подписи;
- уведомлять своего непосредственного начальника, системного администратора о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ;
- хранить в тайне закрытый ключ ЭП;
- самостоятельно контролировать срок действия сертификата проверки ключа ЭП.

### 3.2.3. Владелец электронной подписи несет личную ответственность за сохранность своего ключа электронной подписи и его защиту от несанкционированного использования.

## 3.3. Аннулирование (отзыв) сертификата ключа проверки ЭП.

### 3.3.1. Аннулирование сертификата электронной подписи производится только удостоверяющим центром в случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ:

- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

- установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

3.3.2. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи удостоверяющий центр обязан уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

3.3.3. При получении соответствующего уведомления об аннулировании сертификата ключа, данное уведомление должно быть доведено в течение одного рабочего дня до непосредственного руководителя, системного администратора.

3.3.4. При аннулировании сертификата ЭП, в течение 3-х рабочих дней в университете создаётся комиссия по установлению причин, приведших к аннулированию данного сертификата. Комиссию возглавляет ректор университета или по его решению - проректор по цифровой трансформации. Руководитель структурного подразделения, сертификат ЭП работника, которого аннулируется, а также системного администратора являются обязательными членами данной комиссии. По итогам работы комиссии готовится Протокол с описанием причин, приведших к аннулированию сертификата ЭП и установлением работников университета, действия которых привели к аннулированию сертификата ЭП.

3.4. Прекращение действия сертификата ключа проверки ЭП.

3.4.1. Сертификат ключа проверки ЭП прекращает своё действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

3.4.2. При необходимости прекратить действие сертификата ключа проверки ЭП досрочно, пользователь ЭП информирует своего непосредственного руководителя, системного администратора о данном решении путем направления служебной записки в свободной форме с обязательным указанием причины возникновения необходимости в прекращении действия данного сертификата.

3.4.3. Заявление о прекращении действия сертификата проверки ключа ЭП в виде формируется пользователем ЭП, подписывается владельцем данного сертификата и направляется в удостоверяющий центр. Копия заявления передаётся пользователем ЭП системному администратору.

3.5. Продление действия сертификата ключа проверки ЭП.

- 3.5.1. Пользователь ЭП должен оповестить системного администратора о необходимости продления сертификата ключа проверки ЭП не позднее 30-ти рабочих дней до даты прекращения действия данного сертификата служебной запиской.
- 3.5.2. После получения информации о необходимости продления сертификата, системный администратор оказывает содействие пользователю ЭП в формировании перечня документов на продление сертификата.
- 3.5.3. Сбором документов на продление сертификата занимается пользователь ЭП.
- 3.5.4. Системный администратор отслеживает факты продления сертификатов через ведение соответствующего реестра пользователей ЭП.
- 3.5.5. Установка нового сертификата на рабочее место пользователя ЭП производится системным администратором в течение двух рабочих дней со дня получения сертификата пользователем ЭП.
- 3.6. Перенос компонентов ЭП на новое рабочее место пользователя ЭП.
  - 3.6.1. В случае необходимости переноса компонентов ЭП на новое рабочее место, пользователь ЭП заблаговременно (служебной запиской) информирует об этом системного администратора.
  - 3.6.2. Перенос компонентов ЭП и соответствующая фиксация в реестре пользователей ЭП производится системным администратором.
- 3.7. Порядок хранения и выдачи ЭП.
  - 3.7.1. Порядок хранения ЭП должен строго соблюдаться и отвечать следующим правилам:
    - выдача ключевых носителей ЭП осуществляется на основании положительной резолюции генерального директора колледжа на заявлении работника под роспись работника;
    - хранение ключевого носителя ЭП работник (владелец ЭП) осуществляет только в сейфе или в запираемом рабочем столе таким образом, чтобы исключить любую возможность утраты или попадания ключевого носителя ЭП посторонним лицам.
    - установить PIN-код - на компьютер, токен и контейнер ключей. Также следует заменить заводские пароли токена и контейнера ключей ЭЦП;
    - категорически запрещено передавать носитель ЭП другому работнику. Каждый носитель ЭП определен под конкретного работника.
    - менять ЭП необходимо сразу же, как только работник уволился или поменялось название организации (учреждения).
    - пароль не должен храниться на бумаге и на видном месте.
    - необходимо осуществлять периодические проверки компьютера, на котором используется носитель ЭП на наличие компьютерных вирусов.
- 3.8. Ответственность пользователя ЭП.
  - 3.8.1. Пользователь ЭП несет персональную ответственность:
    - за сохранность своего ключа ЭП и его защиту от несанкционированного использования;
    - за полноту и достоверность сведений, находящихся на подписываемом электронной подписью документе;
    - за возникновение причин, которые по его вине привели к аннулированию сертификата электронной подписи.
    - за выполнение правил эксплуатации ключа ЭП при выполнении непосредственных

работ.

3.8.2. Работник, нарушивший требования настоящего положения, несет ответственность в соответствии с действующим законодательством Российской Федерации.

3.9. Правила и средства использования электронных подписей.

3.9.1. Электронный документ считается подписанным усиленной квалифицированной электронной подписью при выполнении следующих условий:

- усиленная квалифицированная электронная подпись содержится в самом электронном документе;
- ключ усиленной квалифицированной электронной подписи применяется в соответствии с правилами, установленными оператором информационных систем, с использованием которой осуществляются создание и/или отправка электронного документа, и в созданном и/или отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и/или отправлен электронный документ.

3.9.2. Нормативные правовые акты и/или соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных усиленной квалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

- правила определения лица, подписывающего электронный документ, по его усиленной квалифицированной электронной подписи;
- обязанность лица, создающего и/или использующего ключ усиленной квалифицированной электронной подписи, соблюдать его конфиденциальность.

3.9.3. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:

- позволяют установить факт изменения подписанного электронного документа после момента его подписания;
- обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;
- позволяют создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

3.9.4. При создании электронной подписи средства электронной подписи должны:

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;
- создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи;



- однозначно показывать, что электронная подпись создана.

### 3.9.5. При проверке электронной подписи средства электронной подписи должны:

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, содержание электронного документа, подписанного электронной подписью, включая визуализацию данной электронной подписи, содержащую информацию о том, что такой документ подписан электронной подписью, а также о номере, владельце и периоде действия сертификата ключа проверки электронной подписи;
- показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;
- указывать на лицо, с использованием ключа электронной подписи, которого подписаны электронные документы.

## 3.10. Сертификат ключа проверки электронной подписи

### 3.10.1. Удостоверяющий центр:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;
- осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведет реестр выданных и аннулированных сертификатов ключей проверки электронных подписей;
- осуществляет проверку электронных подписей по обращениям участников электронного взаимодействия.

### 3.10.2. Сертификат ключа проверки электронной подписи содержит следующую информацию:

- уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;
- фамилия, имя и отчество заявителя или информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;
- уникальный ключ проверки электронной подписи;

- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;
- наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи.

3.10.3. Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи;
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам.

3.11. Технология применения средств электронной подписи.

3.11.1. Изготовление (генерацию), регистрацию, выдачу, отзыв и уничтожение ключа усиленной квалифицированной электронной подписи осуществляет ответственный сотрудник, назначаемый приказом генерального директора.

3.11.2. Изготовление усиленной квалифицированной электронной подписи производится посредством создания цифрового удостоверения с использованием специализированного программного обеспечения.

3.11.3. Правом получения и использования усиленной квалифицированной электронной подписи наделяется генеральный директор организации, а также лица, которым вменены должностные и/или функциональные обязанности по обработке внутренних электронных документов с использованием усиленной квалифицированной электронной подписи.

3.11.4. Информация обо всех выданных пользователю ключах электронной подписи, датах получения и прекращения их действия (изъятия) хранится постоянно.

3.11.5. При прекращении у сотрудника организации должностных и/или функциональных обязанностей по обработке внутренних электронных документов с использованием усиленной квалифицированной электронной подписи или при увольнении сотрудника его ключ отзывается и передается ответственному лицу для уничтожения.

3.12. Используемые программные средства.

3.12.1. В качестве электронного документооборота и взаимодействия с органами власти используются цифровые сервисы.

3.12.2. В качестве платформы для ЭИОС в колледже используются «Продукты 1С».

3.12.3. В качестве средства электронной подписи используется криптопровайдер включенный в реестр Российского ПО.

3.13. Порядок использования неквалифицированной электронной подписи.

3.13.1. Жизненный цикл электронного документа в СЭД и ЭИОС включает: создание и прочие действия по его обработке, отражение в учете, а также хранение. ЭИОС обеспечивает регистрацию действий пользователей с электронным документом (логирование) в течение жизненного цикла.

3.13.2. Все владельцы КЭП и НЭП признают равнозначность своей электронной подписи собственноручной подписи на бумажном носителе, что подтверждается согласием ([Приложение 2](#)).

3.13.3. Полномочия владельца ЭП, подписавшего электронный документ, автоматически

подтверждаются в момент подписания электронного документа в СЭД и ЭИОС по положительному результату следующих проверок:

- соответствующий пользователь авторизован в СЭД или ЭИОС;
- соответствующий ключ электронной подписи включен в реестр выданных ключей электронной подписи;
- соответствующий ключ электронной подписи отсутствует в реестре отозванных ключей электронной подписи.

3.13.4. Время формирования электронной подписи фиксируется средствами СЭД или ЭИОС по местному времени.

3.13.5. Внутренние электронные документы, перечисленные в Перечне документов ([Приложение 3](#)), подписанные КЭП или НЭП, признаются в колледже равными по юридической силе документам на бумажных носителях, заверенным собственноручной подписью.

3.13.6. Пользователи признают, что визуализация штампа КЭП или НЭП при демонстрации электронного документа в интерфейсе СЭД или ЭИОС, является неоспоримым подтверждением факта подписания документа соответствующим владельцем ЭП (подлинность и неотрекаемость).

3.13.7. Хранение электронных документов осуществляется путем записи сведений об электронных документах в архив электронных документов, который является частью СЭД или ЭИОС.

3.13.8. Колледж обеспечивает техническими и организационными мерами защиту от несанкционированного доступа и преднамеренного уничтожения и/или искажения сведений об электронных документах в архиве электронных документов, а также гарантирует подтверждение авторства документа, подписанного КЭП или НЭП автора, в том числе путем утверждения поименного ограниченного списка лиц, имеющих расширенные (административные) права доступа к архиву электронных документов ЭИОС.

3.13.9. Документы хранятся в ЭИОС в том формате, в котором они были созданы. Срок хранения электронных документов и сведений об электронных документах не может быть менее 3 (трех) лет и определяется локальными нормативными актами Университета.

3.13.10. Копия электронного документа может быть изготовлена (распечатана) на бумажном носителе средствами СЭД или ЭИОС и заверена собственноручной подписью владельца КЭП или НЭП или лица, имеющего расширенные (административные) права доступа к архиву электронных документов. Копия электронного документа на бумажном носителе содержит визуализацию штампа (штампов) КЭП или НЭП, подтверждающую, что оригинал электронного документа подписан КЭП или НЭП. Аутентичность электронного документа и его копии на бумажном носителе обеспечивается средствами СЭД или ЭИОС.

3.14. Технология применения средств ЭП в ЭИОС.

3.14.1. Для применения ЭП в СЭД или ЭИОС владельцу ЭП необходимо авторизоваться использованием имени пользователя и пароля. Подписание электронного документа выполняется путем нажатия на кнопку «Подписать» в интерфейсе в СЭД или ЭИОС.

3.14.2. Информация обо всех выданных пользователю ключах электронной подписи, датах

получения и прекращения их действия (изъятия) хранится в СЭД или ЭИОС постоянно.

- 3.14.3. При прекращении у сотрудника должностных обязанностей по обработке внутренних электронных документов с использованием КЭП или НЭП или при увольнении сотрудника его ключ вносится в реестр отозванных ключей электронной подписи. С момента внесения ключа в реестр отозванных ключей, все последующие электронные документы, подписанные этой НЭП, не считаются подписанными надлежащим образом, т.е. подписью, равнозначной собственноручной.

#### **4. Контроль за выполнением требований настоящего положения**

- 4.1. Контроль за выполнением требований настоящего Положения возлагается на генерального директора Колледжа и лицо, использующее КЭП и НЭП/ПЭП.

#### **5. Заключительные положения**

- 5.1. Настоящее Положение является локальным нормативным актом и утверждается приказом генерального директора АНО СПО «ММК».
- 5.2. Внутренние электронные документы, подписанные простой электронной подписью в соответствии с настоящим Положением, признаются юридически значимыми с даты утверждения Положения.
- 5.3. Документы, созданные в СЭД или ЭИОС и подписанные КЭП или НЭП/ПЭП в соответствии с настоящим Положением, признаются юридически значимыми с даты утверждения Положения.
- 5.4. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии с действующим законодательством Российской Федерации.
- 5.5. Настоящее Положение вступает в силу с даты его утверждения.
- 5.6. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

(Должность)

(Расшифровка)

**СОГЛАСИЕ**

Я, \_\_\_\_\_  
настоящим подтверждаю, что ознакомлен(а) с Положением об использовании электронной подписи в Автономной некоммерческой организации среднего профессионального образования «Многопрофильный медицинский колледж», признаю равнозначность своей квалифицированной/неквалифицированной электронной подписи собственноручной подписи на бумажном носителе и даю согласие на использование НЭП в системе электронного документооборота и электронной информационно-образовательной среде Автономной некоммерческой организации среднего профессионального образования «Многопрофильный медицинский колледж» в соответствии с Положением об использовании электронной подписи в АНО СПО «ММК» с «\_\_\_» \_\_\_\_\_ 20\_\_ г.

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_/\_\_\_\_\_  
(Подпись) (Расшифровка)

**Приложение 3**  
**Перечень документов**

**ПЕРЕЧЕНЬ ДОКУМЕНТОВ**

Участники внутреннего электронного документооборота в АНО СПО «ММК» используют ЭП при обработке следующих электронных документов:

- приказы о движении контингента;
- приказы о смене ФИО;
- справка об обучении;
- справка-вызов;
- акт приемки товаров, работ, услуг;
- заявка-обоснование закупки товаров малого объема через подотчетное лицо;
- отчет о расходах подотчетного лица;
- акт списания материалов;
- акт списания мягкого и хозяйственного инвентаря;
- требование-накладная:
- накладная на отпуск материалов 3-м лицам;
- акт списания БСО;
- решение о признании объекта нефинансовых активов;
- решение о прекращении признания активов;
- списание объектов ОС, ИМА, НПА;
- решение о проведение инвентаризации;
- заявка на кассовый расход;
- заявка на возврат;
- исковые заявления в различные судебные органы Российской Федерации;
- апелляционные, кассационные жалобы в различные судебные органы Российской Федерации;
- отзывы на исковые заявления в различные судебные органы Российской Федерации;
- отзывы на апелляционные, кассационные жалобы в различные судебные органы Российской Федерации;
- заявления, жалобы, ответы, направляемые в различные государственные органы РФ;
- копии документов, представляемые в различные государственные органы РФ;
- документация в системе ЕИС.