Федеральное государственное бюджетное образовательное учреждение
высшего образования «Воронежский государственный
медицинский университет имени Н.Н. Бурденко»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 29DA63E73B264EA326A68D5EC1676813
Владелец: Есауленко Игорь Эдуардович
Действителен: с 18.07.2024 до 11.10.2025

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО ВГМУ
им. Н.Н. Бурденко
Минздрава России
«01» ноября 2024 года № 676

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ В СЛУЖЕБНЫХ ЦЕЛЯХ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Н. БУРДЕНКО» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Воронеж, 2024

1. РАЗРАБОТАНО

Центром информационной безопасности и инженерно-технических средств защиты

полное наименование структурного подразделения, ответственного за разработку документа

2. ПРИНЯТО НА ЗАСЕДАНИЯ УЧЁНОГО СОВЕТА ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России

31.10.2024 г., протокол № 3.

3. ВЕРСИЯ I.

Один экземпляр принят на хранение:

Должность _____ Л.А. Гришина

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее положение об использовании в служебных целях квалифицированной электронной подписи устанавливает порядок работы с электронной подписью (далее – ЭП), выданной на должностное лицо или юридическое лицо, ответственность и обязанности сотрудников при использовании ЭП в ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России (далее – университет).

1.2. Изменения и дополнения настоящего положения вступают в силу с момента их утверждения приказом по университету.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. Настоящее положение разработано на основе Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

2.2. Положение разработано с дополнительными нормативно-правовыми документами:

2.2.1. ЭЛЕКТРОННАЯ ПОДПИСЬ

1) Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

2) Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3) Постановление Правительства Российской Федерации от 28 ноября 2011 г. № 976 «О федеральном органе исполнительной власти, уполномоченном в сфере использования электронной подписи».

4) Постановление Правительства Российской Федерации от 25.06.2012 № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг».

5) Постановление Правительства Российской Федерации от 25.08.2012 № 852 «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».

6) Постановление Правительства Российской Федерации от 09.02.2012 №111 «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».

7) Постановления Правительства Российской Федерации от 25.01.2013 № 33 «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».

8) Приказ ФАПСИ от 13 июня 2001 г. № 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».

9) Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

10) Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

11) Приказ Минкомсвязи России от 22.08.2017 № 436 «Об утверждении Порядка формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров».

12) Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.08.2018 № 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей».

13) Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.08.2021 № 857 «Об утверждении единых требований к формам доверенностей, необходимых для использования квалифицированной электронной подписи.

2.2.2. ЭЛЕКТРОННЫЕ ТОРГИ

1) Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

2) Федеральный закон от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

3) Постановление Правительства Российской Федерации от 30.12.2018 № 1752 «О порядке регистрации участников закупок в единой информационной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд и ведения единого реестра участников закупок и внесении изменений в постановление Правительства Российской Федерации от 8 июня 2018 г. № 656».

4) Постановление Правительства Российской Федерации от 25.12.2018 № 1663 «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».

2.2.3 ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

1) Федеральный закон от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

2) Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3) Постановление Правительства Российской Федерации от 22.09.2009 №754 «Об утверждении Положения о системе межведомственного электронного документооборота».

4) Приказ Минфина России от 10.11.2015 №174н «Об утверждении Порядка выставления и получения счетов-фактур в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи»

5) Приказ Минздрава России от 07.09.2020 N 947н "Об утверждении Порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов" (Зарегистрировано в Минюсте России 12.01.2021 N 62054)

2.2.4. ЭЛЕКТРОННАЯ ОТЧЕТНОСТЬ

1) Постановление правительства Российской Федерации от 26.12.2011 №1137 «О формах и правилах заполнения (ведения) документов, применяемых при расчетах по налогу на добавленную стоимость».

2) Приказ ФНС России от 05.12.2016 N ММВ-7-21/668 «Об утверждении формы и формата представления налоговой декларации по транспортному налогу в электронной форме и порядка ее заполнения».

3) Приказ Федеральной налоговой службы России от 17.02.2008 № ММ-3-6/665 «Об утверждении Порядка ведения единого пространства доверия сертификатам ключей ЭЦП».

4) Приказ ФНС России от 30.01.2012 № ММВ-7-6/36@ «Об утверждении форматов представления документов, используемых при выставлении и получении счетов-фактур в электронном виде по телекоммуникационным каналам связи с применением электронной подписи».

2.2.5. ЗАЩИТА ИНФОРМАЦИИ

1) Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

2) Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне».

3) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

4) Постановление Правительства Российской Федерации от 16.04.2012 №313 «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)».

5) Постановление Правительства Российской Федерации № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6) Указ президента России от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

7) Приказ ФСБ и ФСТЭК России от 31.08.2010 №416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

8) Приказ ФСБ России от 10.07.2014 №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».

9) Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владелец сертификата ключа проверки квалифицированной электронной подписи – лицо, которому в установленном порядке выдан сертификат ключа проверки квалифицированной электронной подписи;

Ключ квалифицированной электронной подписи – уникальная последовательность символов, предназначенная для создания квалифицированной электронной подписи;

Заявление на создание ключа – документ, заверяющийся подписью заявителя, подтверждающий личность для создания ключа электронной подписи;

Информационная система общего пользования – информационная система, участники электронного взаимодействия в которой составляют неограниченное количество лиц и в использовании которой этим лицам не может быть отказано;

Простая электронная подпись – подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом;

Неквалифицированная электронная подпись – подпись, которая 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;

Квалифицированная электронная подпись – подпись, которая имеет все признаки неквалифицированной электронной подписи и дополнительные признаки: 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 настоящим Федеральным законом;

Ключ шифрования – ключ, предназначенный для закрытия электронного документа при электронных взаимодействиях;

Машинный носитель ключевой информации – физический носитель для электронной подписи. Выполнен в виде USB-носителя;

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;

Компрометация ключевой информации – утрата, хищение, несанкционированное копирование или подозрение на копирование носителя ключевой информации или любые другие ситуации;

Корпоративная информационная система (КИС) – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

Программное средство криптографической защиты – компьютерная программа, позволяющая осуществлять операции с электронной подписью: установка, проверка сертификата электронной подписи;

Машиночитаемая доверенность (МЧД) – доверенность в электронном виде, подписанная усиленной квалифицированной электронной подписью ректора университета ФГБОУ ВО ВГМУ им. Н.Н. Бурденко, где описаны полномочия сотрудника организации, например, подписывание документов от имени организации, и позволяет сотрудникам представлять интересы организации в электронном документообороте с контрагентами, сдавать отчетность, выставлять счета, оформлять закрывающие документы. Одна машиночитаемая доверенность может выдаваться на группу сотрудников организации;

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 удостоверение личность человека, который обратился за сертификатом электронной подписи, изготовить и выдать сертификат, в котором включены данные о владельце сертификата и его открытый ключ проверки;

ЦИБИТСЗ – центр информационной безопасности и инженерно-технических средств защиты.

4. ОБЩИЕ ПОЛОЖЕНИЯ

4.1. 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.

4.2. В случае необходимости использования электронной подписи сотрудником университета для выполнения своих должностных (функциональных) обязанностей, данный сотрудник должен обратиться со служебной запиской на имя начальника ЦИБИТСЗ.

4.3. В случае утверждения начальником ЦИБИТСЗ, служебная записка передается сотруднику ЦИБИТСЗ для выполнения им работ по формированию электронной подписи и подготовке места для работы с электронной подписью.

4.4. В случае получения отказа в использовании ЭП по поступившей от работника служебной записки, данное заявление обрабатывается в соответствии с правилами документооборота и делопроизводства Университета.

4.5. Для формирования электронной подписи сотруднику университета необходима следующая информация: ФИО, структурное подразделение, должность, ИНН, СНИЛС, USB-устройство, на которое будет записан компонент электронной подписи, контактный телефон, электронная почта.

4.6. Машиночитаемая доверенность выпускается начальником ЦИБИТСЗ по соответствующей форме на ресурсах федеральной налоговой службы или иных платформах.

4.7. Срок сертификата ключа проверки электронной подписи – 1 год и 3 месяца с даты формирования сертификата ЭП. По истечении этого срока электронную подпись нужно либо перевыпустить с новым пакетом документов, либо продлить не менее чем за две недели до окончания срока.

4.8. Электронная подпись должна использоваться только на рабочем месте пользователя электронной подписи, указанном в заявлении.

4.9. Не допускается использование одной электронной подписи несколькими пользователями электронной подписи на одном рабочем месте.

Каждый пользователь должен иметь соответствующие полномочия, выданные начальником ЦИБИТСЗ.

4.10. Сотрудникам университета, не являющимися владельцами электронной подписи, запрещено использование электронной подписи. Сотрудники ЦИБИТСЗ имеют право использовать открытую часть ЭП для выдачи полномочий на рабочих ресурсах и полной ЭП для ее продления.

4.11. Сотрудники ЦИБИТСЗ имеют право потребовать электронную подпись должностного лица у любого сотрудника университета, у которого она имеется для проверки работоспособности.

4.12. Электронная подпись должностного лица должна находится в пределах рабочего места.

4.13. Сотрудникам запрещается вынос USB-устройства с электронной подписью за пределы университета.

4.14. Электронная подпись должна храниться в сейфе или в запирающемся ящике, или в труднодоступном, неизвестным для других сотрудников, месте у владельца.

5. ПРАВА И ОБЯЗАННОСТИ ВЛАДЕЛЬЦА ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. Владелец электронной подписи имеет право:

1) Обращаться к сотруднику ЦИБИТСЗ для аннулирования, приостановки, перевыпуска и иной технической поддержки электронной подписи.

2) Обращаться к начальнику ЦИБИТСЗ для решения споров, возникающих при применении электронной подписи в информационной системе.

5.2. Владелец электронной подписи обязан:

1) Вести обработку внутренних электронных документов информационной системе университета в соответствии со своими должностными обязанностями.

2) Не допускать инциденты с несанкционированным использованием должностной электронной подписи.

3) Не передавать кому-либо из сотрудников должностную электронную подпись, кроме случаев, предусмотренных настоящим положением.

4) Обеспечить сохранность и конфиденциальность ключей электронной подписи.

5) При утере, пропаже USB-носителя, компрометации ключа электронной подписи необходимо обратиться к начальнику центра информационной безопасности или иному сотруднику из центра.

6) Не использовать электронную подпись при наличии оснований полагать, что конфиденциальность подписи была нарушена.

7) Самостоятельно контролировать срок действия сертификата проверки ключа электронной подписи.

6. ОТЗЫВ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

6.1. Отзыв сертификата ключа проверки электронной подписи производится только удостоверяющим центром в случаях, предусмотренных в ФЗ № 63-ФЗ:

1) У владельца сертификата ключ проверки электронной подписи не соответствует ключу проверки электронной подписи, указанному в сертификате.

2) Установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи.

3) Удостоверяющий центр во время проверок вынес решение, что ключ проверки электронной подписи содержит недостоверную информацию.

6.2. 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.

7. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

7.1. 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 иных случаях, установленными федеральными законами.

7.2. При необходимости прекратить действие сертификата ключа проверки электронной подписи досрочно, владелец формирует заявление и информирует начальника ЦИБИТСЗ о своем решении с обоснованием (служебная записка).

7.3. Заявление о прекращении действия сертификата проверки ключа электронной подписи подписывается владельцем и направляется в удостоверяющий центр.

8. ПРОДЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

8.1. Владелец электронной подписи должен оповестить начальника или иного сотрудника центра информационной безопасности о необходимости продления сертификата ключа проверки электронной подписи не позднее, чем за 14 дней до даты прекращения действия данного сертификата, подкрепленный служебной запиской.

8.2. После получения служебной записки от владельца электронной подписи, начальник или иной сотрудник оказывает содействие владельцу электронной подписи в формировании нового ключа проверки сертификата и необходимых документов к этому.

8.3. Установка нового сертификата на рабочее место владельца электронной подписи производится сотрудником центра информационной безопасности в течение двух рабочих дней со дня получения сертификата владельца электронной подписи.

9. ПЕРЕНОС КОМПОНЕНТОВ ЭЛЕКТРОННОЙ ПОДПИСИ НА НОВОЕ РАБОЧЕЕ МЕСТО

9.1. Выполнять перенос компонентов электронной подписи с одного рабочего компьютера на другое рабочее место владельцу электронной подписи своими силами категорически запрещено без участия сотрудников центра информационной безопасности.

9.2. В случае необходимости переноса владельцу необходимо составить служебную записку на имя начальника центра информационной безопасности с обоснованием и заблаговременно.

9.3. Перенос компонентов электронной подписи выполняет только сотрудник центра информационной безопасности университета.

10. ПОРЯДОК ХРАНЕНИЯ И ВЫДАЧИ ЭЛЕКТРОННОЙ ПОДПИСИ

10.1. Учет USB-носителей с компонентами электронной подписи осуществляется в специальном журнале, который хранится в центре информационной безопасности.

10.2. Выдача USB-носителей с компонентами электронной подписи осуществляется доверенным лицом, определенным настоящим положением. Владелец USB-носителя обязан расписаться при получении и сдаче в специальном журнале поэкземплярного учета.

10.3. Хранение USB-носителя электронной подписи осуществляется только в защищенном от взлома сейфе, находящимся у доверенного лица, определенным настоящим положением, чтобы исключить возможность утраты или компрометации посторонними лицами.

10.4. Установить PIN-код - на компьютер, токен и контейнер ключей. Установка пароля носит рекомендательный характер. Также рекомендовано заменить заводские пароли токена и контейнера ключей ЭЦП.

10.5. Пароль не должен храниться на бумаге и на видном месте.

10.6. Необходимо осуществлять регулярные проверки компьютера на наличие компьютерных вирусов, на котором используется носитель ЭП, сроки которых устанавливает начальник ЦИБИТСЗ.

11. ОТВЕТСТВЕННОСТЬ ВЛАДЕЛЬЦА ЭЛЕКТРОННОЙ ПОДПИСИ

11.1. Владелец несет персональную ответственность за:

1) Сохранность своего ключа ЭП и его защиту от несанкционированного использования.

2) Полноту и достоверность сведений, находящихся на подписываемом электронной подписью документе.

3) Возникновение причин, которые по его вине привели к аннулированию сертификата электронной подписи.

4) Выполнение правил эксплуатации ключа ЭП при выполнении непосредственных работ.

5) Сотрудник, нарушивший требования настоящего положения, несет ответственность в соответствии с действующим законодательством Российской Федерации.

12.ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1 Положение вступает в силу с 01.11.2024 после утверждения приказом ректора.

12.2 Проект Положения с листом согласования храниться в ученом совете, утвержденный экземпляр Положения - в административно-правовом управлении, на официальном сайте в сети Интернет - в виде электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».