УТВЕРЖДАЮ
Директор ГУ «Республиканский научно-практический центр медицинских технологий, информатизации, управления и экономики здравоохранения»

_____ М.М.Сачек
«19» 09 2018

Регламент использования электронной цифровой подписи врача в медицинских информационных системах для подписания электронных рецептов

СОГЛАСОВАНО
Заместитель директора РНПЦ МТ
по информационным технологиям

_____ С.В.Новиков
«19» 09 2018

Заведующий отделом
организационно-методической
работы информатизации
здравоохранения РНПЦ МТ

_____ Ю.Ч.Чичин
«19» 09 2018

Минск 2018

Содержание

Оглавление

1. Общие сведения

1.1. В рамках данного документа описывается применение электронной цифровой подписи врача для подписания рецептов, формируемых в электронном формате, для придания им статуса электронного документа.

1.2. В соответствии с Решениями по обеспечению поддержки инфраструктуры автоматизированной информационной системы обращения электронных рецептов (далее - АИС ЭР) для выработки и проверки электронной цифровой подписи (далее – ЭЦП) действия медицинских работников в процессе выработки ЭЦП от электронных рецептов в рамках функционирования АИС ЭР будет осуществляться с применением сертифицированных программных средств ЭЦП с использованием сертификатов открытых ключей (далее - СОК), изданных республиканским удостоверяющим центром Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (далее – РУЦ ГосСУОК).

1.3. Порядок получения сертификатов регламентируется документами, издаваемыми РУП «НЦЭУ».

1.4. Выработка и проверка ЭЦП электронных рецептов будет осуществляться на основе **сертификатов юридического лица.**

1.5. Функции врача по выработке электронной цифровой подписи и подписанию электронных рецептов реализуются на автоматизированном рабочем месте врача в рамках используемой медицинской информационной системы (далее – МИС).

1.6. Для МИС должно быть реализовано регулярное обновление списков отозванных сертификатов (далее – СОС), издаваемых РУЦ ГосСУОК. Регулярное обновление СОС для МИС будет организовано в рамках корпоративной сети АИС ЭР с точки центральной серверной платформы, доступной всем МИС. Процедура обновления СОС на автоматизированном рабочем месте врача в рамках МИС формируется организацией, отвечающей за эксплуатацию (сопровождение) МИС.

1.7. Действия врача по подписанию электронных рецептов ЭЦП приводятся в эксплуатационной документации МИС.

1.8. Для обеспечения выполнения функций по выработке ЭЦП на каждом рабочем месте врача должно быть установлено сертифицированное средство выработки ЭЦП «Программный комплекс «Комплект Абонента АВЕСТ» AvUCK, который передается абоненту РУЦ ГосСУОК при выпуске сертификата.

Примечание. В случае если на одном АРМ работает несколько врачей (например, при посменной работе), то на этом компьютере необходимо с помощью Персонального менеджера сертификатов из

состава «Программного комплекса «Комплект Абонента АВЕСТ» AvUCK импортировать сертификаты каждого врача.

2. Получение (продление, обновление данных) ЭЦП

2.1. Сертификат открытого ключа проверки ЭЦП (далее – СОК) издается (приобретается) персонально для каждого врача, выписывающего рецепты в электронном формате.

2.2. Порядок формирования заявки на выпуск СОК приведен на сайте оператора ГосСУОК РУП «НЦЭУ» по адресу https://nces.by/pki/ruc/order/initial-registration/ в разделе **«для уполномоченного представителя юридического лица»**.

2.3. До истечения срока действия СОК (срок действия – 2 года) при необходимости формируется заявка на продление срока действия сертификата. Порядок формирования заявки на продление срока действия СОК приведен на сайте РУП «НЦЭУ» по адресу https://nces.by/pki/ruc/order/prodlenie-registracii/ в разделе **«для уполномоченного представителя юридического лица»**

2.4. В период действия СОК может понадобиться перерегистрация (обновление данных) СОК. Причины, по которым может понадобиться обновление данных сертификата следующие:

выход из строя носителя ключевой информации Подписчика (здесь и ниже под подписчиком подразумевается врач, владеющий ЭЦП);

при изменении данных, влияющих на содержание СОК Подписчика — данные указаны в Перечне сведений о Подписчике;

утрата Подписчиком пароля доступа к контейнеру личного ключа на носителе ключевой информации;

утрата (порча) Подписчиком личного ключа;

компрометация личного ключа Подписчика;

компрометация личного ключа Удостоверяющего центра;

личное желание Подписчика.

Порядок формирования заявки на перерегистрацию (обновление данных) СОК приведен на сайте РУП «НЦЭУ» по адресу https://nces.by/pki/ruc/order/pereregistracia/ в разделе **«для уполномоченного представителя юридического лица»**

3. Отзыв (приостановка действия)-СОК

3.1. Отзыв или приостановка действия ЭЦП (сертификата открытого ключа) СОК становятся необходимы в следующих случаях:

компрометация ключа Подписчика (под компрометацией подразумевается, что информация личного ключа Подписчика стала известна, или есть подозрение, что стала известна, третьей стороне);

прекращение деятельности Подписчика;

прекращение действия открытого ключа;

невозможность использования ключа;

иное.

3.2. Образец заявления на отзыв (приостановку действия) СОК приведен на сайте РУП «НЦЭУ» по адресу https://nces.by/pki/kak-poluchit-ecp/.

4. Обязанности владельца СОК

4.1. Владелец СОК обязан:

принять и соблюдать требования использования и хранения личных и открытых ключей ЭЦП (п. 2.3 Регламента деятельности республиканского удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь);

использовать личный и открытый ключи только по прямому назначению, т.е. для выработки и проверки ЭЦП в процессе выписки электронных рецептов;

в случае компрометации (угрозы компрометации) личного ключа ЭЦП обратиться в РУЦ с целью приостановки действия СОК;

в случае изменения сведений, влияющих на содержание СОК, обратиться в РУЦ для отзыва СОК с неактуальными данными и издания нового СОК, представив пакет необходимый пакет документов (см. разд. 2;

самостоятельно установить пароль на доступ к личному ключу ЭЦП. Личный ключ ЭЦП Подписчика после генерации хранится в зашифрованном виде на НКИ. Доступ к контейнеру личного ключа ЭЦП на НКИ защищен паролем, который должен быть не менее 8 (восьми) символов и состоять из цифр и/или букв;

хранить в тайне личный ключ ЭЦП, принимать все возможные меры для предотвращения его компрометации (в том числе потери, раскрытия содержания, искажения содержания, несанкционированного использования);

не применять личный ключ ЭЦП, если ключ скомпрометирован или отозван;

принимать необходимые меры для обеспечения безопасности средств ЭЦП.