О внесении изменений в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ "Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре"

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 17 марта 2023 года № 95/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 28 марта 2023 года № 32129

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ "Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 21549) следующие изменения:

в Правилах создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре, утвержденных указанным приказом:

пункты 1 и 2 изложить в следующей редакции:

"1. Настоящие Правила создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре (далее- Правила) разработаны в соответствии с Законом Республики Казахстан "Об электронном документе и электронной цифровой подписи" (далее - Закон) и определяют порядок создания, использования, и хранения закрытых ключей электронной цифровой подписи в облачных сервисах.

2. В настоящих Правилах применяются следующие понятия:

1) биометрическая аутентификация – комплекс мер, идентифицирующих личность на основании физиологических и неизменных биологических признаков;

2) блокчейн - информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования;

3) многофакторная аутентификация – способ проверки подлинности пользователя при помощи комбинации различных параметров, в том числе генерации и ввода

паролей или аутентификационных признаков (цифровых сертификатов, токенов, смарт-карт, генераторов одноразовых паролей и средств биометрической идентификации);

4) удостоверяющий центр (далее - УЦ) - юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства;

5) владелец регистрационного свидетельства (далее - владелец) – физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

6) электронная цифровая подпись (далее - ЭЦП) – набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

7) открытый ключ ЭЦП - последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе;

8) закрытый ключ ЭЦП - последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

9) средства электронной цифровой подписи - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

10) облачная ЭЦП – сервис удостоверяющего центра, позволяющий создавать, использовать, хранить и удалять закрытые ключи электронной цифровой подписи в HSM удостоверяющего центра, где доступ к закрытому ключу осуществляется владельцем удалҰнно посредством не менее двух факторов аутентификации, одним из которых является биометрическая;

11) хэш – преобразование массива входных данных произвольной длины в битовую сторону фиксированной длины;

12) аппаратный криптографический модуль (Hardware Security Module) (далее - HSM) - аппаратный криптографический модуль предназначенный для шифрования информации и управления открытыми и закрытыми ключами ЭЦП.";

пункт 20 изложить в следующей редакции:

"УЦ обеспечивает отсутствие возможности подписания электронных документов с использованием закрытых ключей ЭЦП облачной ЭЦП без многофакторной аутентификации".

2. Департаменту цифровых решений Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательством порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр цифрового развития, инноваций
и аэрокосмической промышленности *Б. Мусин*
Республики Казахстан

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан