МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКА НАЦІОНАЛЬНА АКАДЕМІЯ ХАРЧОВИХ ТЕХНОЛОГІЙ

ПРИЙНЯТО:

на засіданні Вченої ради ОНАХТ

18 грудня 2015 року

Протокол № 06

ВВЕДЕНО В ДІЮ

наказом ОНАХТ від 18.12.2015 року

№ 290-01

ПОРЯДОК

застосування електронного цифрового підпису в Одеській національній академії харчових технологій

Порядок застосування електронного цифрового підпису в Одеській національній академії харчових технологій розроблено, відповідно до Закону України «Про електронний цифровий підпис» від 22.05.2003 року № 852-IV (із змінами) та Постанови Кабінету Міністрів України від 28.10.2004 року № 1452 «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» (із змінами).

Дія цього Порядку не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

1. У цьому Порядку терміни вживаються у такому значені:

електронний підпис - дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа;

засіб електронного цифрового підпису - програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

особистий ключ - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

відкритий ключ - параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

засвідчення чинності відкритого ключа - процедура формування сертифіката відкритого ключа;

сертифікат відкритого ключа (далі - сертифікат ключа) - документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

посилений сертифікат відкритого ключа (далі - посилений сертифікат ключа) - сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

акредитація - процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

компрометація особистого ключа - будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

блокування сертифіката ключа - тимчасове зупинення чинності сертифіката ключа;

підписувач - особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

послуги електронного цифрового підпису - надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

надійний засіб електронного цифрового підпису - засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється у порядку, визначеному законодавством.

2. Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;

особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

3. Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

4. Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

5. Електронний цифровий підпис використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

6. Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

7. Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

8. Цей Порядок визначає вимоги до застосування електронного цифрового підпису в Одеській національній академії харчових технологій (далі - ОНАХТ).

9. ОНАХТ застосовує електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від Адміністрації Держспецзв'язку, та наявності посилених сертифікатів відкритих ключів у своїх працівників - підписувачів.

10. Для вчинення правочинів ОНАХТ застосовує електронний цифровий підпис, що ґрунтується на посиленому сертифікаті відкритого ключа.

11. ОНАХТ не застосовує електронний цифровий підпис:

для складання електронних документів, які не можуть бути оригіналами у випадках, передбачених законодавством;

для вчинення правочинів на суму, що перевищує 1 млн. гривень.

12. ОНАХТ отримує на договірних засадах послуги, пов'язані з електронним цифровим підписом, від акредитованих центрів сертифікації ключів. У разі коли генерація особистого та відкритого ключів здійснена підписувачем безпосередньо в ОНАХТ, засвідчення чинності відкритого

ключа може бути здійснено лише в одному акредитованому центрі сертифікації ключів.

13. Відповідальність за організацію застосування електронного цифрового підпису в ОНАХТ несуть керівники, які організовують в межах своєї компетенції застосування електронного цифрового підпису.

14. Застосування електронного цифрового підпису в ОНАХТ забезпечує Навчально науковий центр інформаційних технологій (Хобін В.А.).

15. Зазначений структурний підрозділ забезпечує:

підготовку та подання акредитованому центру сертифікації ключів інформації, необхідної для отримання послуг, пов'язаних з електронним цифровим підписом;

надання допомоги підписувачам під час генерації їх особистих та відкритих ключів;

подання до акредитованого центру сертифікації ключів звернень про скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів;

доступ підписувачів через телекомунікаційні мережі до акредитованих центрів сертифікації ключів у разі неможливості здійснення ними такого доступу із своїх робочих місць;

ведення обліку надійних засобів електронного цифрового підпису, що використовуються в ОНАХТ; ведення обліку програмно-апаратних та апаратних носіїв особистих ключів підписувачів;

зберігання документів та їх електронних копій, на підставі яких отримано послуги, пов'язані з електронним цифровим підписом;

контроль за використанням підписувачами надійних засобів електронного цифрового підпису та зберіганням ними особистих ключів.

16. Порядок надання працівникам ОНАХТ права застосування електронного цифрового підпису, ведення обліку, зберігання та знищення їх особистих ключів, а також надання акредитованому центру сертифікації ключів інформації, необхідної для формування, скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів ОНАХТ, визначається наказом ректора, якщо інше не встановлено законодавством.

17. Генерація особистого та відкритого ключів здійснюється підписувачем в акредитованому центрі сертифікації ключів, що обслуговує ОНАХТ, або безпосередньо в ОНАХТ з використанням надійних засобів електронного цифрового підпису. У разі потреби під час генерації особистого та відкритого ключів підписувачеві надається допомога працівниками Навчально - наукового центру інформаційних технологій (Хобін В.А.) або персоналом акредитованого центру сертифікації ключів із дотриманням вимог щодо недопущення ознайомлення з особистим ключем підписувача осіб, що надають таку допомогу.

18. У посиленому сертифікаті відкритого ключа підписувача додатково зазначається його належність до ОНАХТ та посада, яку він займає.

19. У разі коли згідно із законодавством необхідне засвідчення печаткою справжності підпису на документах та відповідності копій документів оригіналам, ОНАХТ застосовує спеціально призначений для таких цілей електронний цифровий підпис (далі - електронна печатка).

ОНАХТ застосовує електронну печатку лише за наявності у неї відповідної печатки, що застосовується для документів на папері.

У посиленому сертифікаті відкритого ключа, що використовується ОНАХТ для електронної печатки, додатково зазначається спеціальне призначення електронного цифрового підпису та сфера його застосування, а також відтворюється текстова інформація, розміщена на відповідній печатці.

20. Право проставлення електронної печатки на електронних документах надається лише тому працівнику ОНАХТ, який проставляє відповідну печатку на документах на папері.

Отримання в акредитованому центрі сертифікації ключів посиленого сертифіката відкритого ключа для забезпечення застосування електронної печатки, а також генерація відповідних ключів здійснюється в тому ж порядку, що й для електронного цифрового підпису.

21. Підписувач використовує у процесі виконання своїх посадових обов'язків лише особистий ключ, отриманий відповідно до пунктів 16 та 17 цього Порядку. Використання особистого ключа у випадках, не пов'язаних з діяльністю ОНАХТ, забороняється.

Після припинення виконання підписувачем посадових обов'язків, для яких генерувалися особистий та відкритий ключі, підписувач або ОНАХТ звертається до акредитованого центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа, а особистий ключ знищується методом, що не допускає можливості його відновлення.

22. Підставами для блокування та/або скасування посиленого сертифіката відкритого ключа підписувача є:

звільнення з посади;

переведення на іншу посаду;

відсторонення від виконання повноважень за посадою;

смерть працівника;

набрання законної сили рішенням суду про оголошення працівника померлим, визнання безвісно відсутнім, недієздатним, обмеження його цивільної дієздатності;

подання заяви на блокування та/або скасування сертифіката у зв'язку з підтвердженням факту компрометації особистого ключа;

зміни інформації, необхідної для отримання послуг, пов'язаних з електронним цифровим підписом.

23. Підписувач для виконання своїх посадових обов`язків не може використовувати одночасно кілька чинних посилених сертифікатів відкритого ключа. Зазначене обмеження не стосується електронної печатки.

24. Підписувач несе відповідальність за зберігання особистого ключа.

25. Передача особистих ключів іншим особам забороняється.

26. Ідентифікація підписувача та підтвердження цілісності даних в електронній формі здійснюються шляхом перевірки електронного цифрового підпису, накладеного на такі дані. Електронний цифровий підпис вважається таким, що пройшов перевірку, якщо:

перевірку електронного цифрового підпису проведено з використанням надійного засобу електронного цифрового підпису;

у результаті перевірки встановлено, що на момент накладення електронного цифрового підпису був чинним посилений сертифікат відкритого ключа підписувача, посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів, посилений сертифікат відкритого ключа відповідного засвідчувального центру та посилений сертифікат відкритого ключа центрального засвідчувального органу;

під час перевірки підтверджено цілісність даних, на які накладено електронний цифровий підпис.

Проректор з науково-педагогічної
та навчальної роботи Ф.А. Трішин

ПОГОДЖЕНО:

Начальник юридичного відділу В.Л. Михайлова