УДК 347.77/.78

Д. В. Бойко,
кандидат юридичних наук, старший науковий співробітник НДІ правового забезпечення інноваційного розвитку НАПрН України

ВИМОГИ ДО ЦЕНТРІВ СЕРТИФІКАЦІЇ КЛЮЧІВ

Стаття присвячена аналізу основних вимог законодавства України до створення і діяльності такого суб'єкту правовідносин у сфері обігу електронних цифрових підписів як центри сертифікації ключів у порівнянні з аналогічними вимогами Європейського Союзу. У статті проаналізовані основні вимоги до створення та діяльності центрів сертифікації ключів, сформульовані пропозиції щодо удосконалення національного законодавства.

***Ключові слова**: електронна комерція, електронний цифровий підпис, центр сертифікації ключів.*

В контексті проекту Закону України «Про електронну комерцію» №2306 а від 17 червня 2013 р. [1], постає питання щодо можливостей ефективного використання електронних цифрових підписів при вчиненні приватноправових електронних правочинів, в тому числі – в мережі Інтернет.

Основні нормативні акти, які регламентують використання в України електронно-цифрового підпису, зокрема, Закон України «Про електронний цифровий підпис» [2] та Закон України «Про електронні документи та електронний документообіг» [3] були прийняті ще у 2003 році. Безумовно, прийняття вказаних законів мало позитивне значення і сприяло певному поширенню використання електронно-цифрового підпису, зокрема, для подання податкової звітності та у банківській сфері.

Разом з тим, у сфері приватно-правових відносин електронний цифровий підпис не став доступною і зручною альтернативою використання паперових документів та звичайних підписів і печаток.

На нашу думку, такий стан речей обумовлений, не в останню чергу, складністю адміністративних процедур, дотримання яких вимагається для створення та розвитку суб'єктів інфраструктури, яка необхідна для поширення сфери використання електронних цифрових підписів.

Нагадаємо, що відповідно ст. 3 Закону України «Про електронний цифровий підпис», «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».

В цьому контексті постає питання щодо вимог до суб'єктів цих правовідносин, які мали б забезпечити можливість використання електронних цифрових підписів. Власне, і завданням цієї статті автор бачить висвітлити зазначені вимоги та сформулювати пропозиції щодо їх удосконалення.

© Бойко Д. В., 2014

Безумовно, з урахуванням проєвропейського курсу України автор вважає доцільним також порівняти принципи організації ринку надання послуг в сфері електронного цифрового підпису та вимоги до суб'єктів такого ринку із відповідними нормами Європейського Союзу.

В ЄС питання вимог до учасників ринку надання послуг в галузі електронного цифрового підпису регламентується єдиним документом – Директивою ЄС «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС [4].

Одним з основних принципів організації ринку електронних цифрових підписів в ЄС є закріплення в п. 12 Преамбули Директиви 1999/93/ЕС можливості надання послуг електронного цифрового підпису особами як публічного, так і приватного права. При цьому країни ЄС зобов'язалися не забороняти провайдерам послуг в сфері електронного цифрового підпису вільно без обмежень використовувати власні схеми акредитації. Також країни ЄС зобов'язалися не вводити обмеження щодо таких схем акредитації, які могли б обмежити конкуренцію в цій сфері.

Крім того, в п. 16 Преамбули вказаної Директиви ЄС [4] прямо вказано, що ця Директива покликана сприяти використанню та юридичному визнанню електронних підписів; нормативна база не повинна використовуватися для обмеження використання електронних підписів, обіг яких здійснюється в системах, основаних на добровільній згоді учасників такої системи; гарантовано визнання таких підписів в якості доказів в судових процесах.

Крім того, нечисленні чітко визначені технічні вимоги в ЄС стосуються лише посилених сертифікатів ключів, які використовуються в сфері публічно-правових відносин, зокрема, при сплаті податків, в банківській сфері тощо. Регламентування ж використання електронного цифрового підпису в приватноправових відносинах залишено учасникам таких відносин.

Таким чином, в ЄС використання електронних цифрових підписів здійснюється здебільшого за диспозитивним принципом, а регулююче втручання держав обмежено. Такий підхід, на нашу думку, сприяє розвитку цих відносин, принаймні, не гальмує їх.

На відміну від ЄС чинне законодавство України містить диференційовані детальні вимоги до приватноправових учасників відносин у сфері використання електронного цифрового підпису та їх діяльності. Відповідно, можна виділити наступних суб'єктів цих відносин:

1) Підписувач;

2) Користувач;

3) Центр сертифікації ключів (надалі – ЦСК);

4) Акредитований центр сертифікації ключів (надалі – АЦСК).

Аналіз законодавства дозволяє дійти висновку про те, що не існує спеціальних адміністративних вимог до підписувача та користувача електронного цифрового підпису, тобто підписувати електронні документи та приймати електронні документи, що були підписані іншими особами, може будь-яка фізична або юридична особа без необхідності дотримання будь-яких адміністративних процедур.

Проходження адміністративних процедур вимагається тільки від таких суб'єктів відносин, пов'язаних з електронним цифровим підписом, як центр сертифікації ключів та акредитований центр сертифікації ключів.

Аналіз Закону України «Про електронний цифровий підпис» дозволяє сформулювати наступні основні відмінності центру сертифікації ключів (надалі – ЦСК) від акредитованого центру сертифікації ключів (надалі –АЦСК):

1) ЦСК може надавати послуги електронного цифрового підпису та обслуговувати звичайні сертифікати ключів (ст. 8 Закону України «Про електронний цифровий підпис»);

2) АЦСК може надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів (ст. 9 Закону України «Про електронний цифровий підпис»).

Практично ця різниця полягає у можливості або неможливості надання послуг електронного цифрового підпису органам державної влади та місцевого самоврядування України (Постанова Кабінету Міністрів України «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» від 28 жовтня 2004 р. №1452) [5].

Разом з цим, посилені сертифікати ключів можуть видавати центральний засвідчувальний орган, функції якого покладені на Міністерство юстиції України згідно з Постановою Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган» №1451 від 28 жовтня 2004 р. [6], а також відповідний та засвідчувальний центр органу виконавчої влади або іншого державного органу.

Розглянемо вимоги щодо створення та діяльності простого (неакредитованого) центру сертифікації ключів (ЦСК) детальніше.

Відповідно до ст. 8 Закону України «Про електронний цифровий підпис» до створення та діяльності ЦСК пред'являються наступні вимоги:

1) **Кваліфікаційні вимоги.**

Кваліфікаційних вимог до керівництва та/або персоналу ЦСК не встановлено.

2) **Організаційні вимоги.**

– Юридична особа будь-якої організаційно-правової форми або приватний підприємець-фізична особа (ч. 1 ст. 8 Закону України «Про електронний цифровий підпис»).

– Засвідчення власного відкритого ключа в центральному засвідчувальному органі (Міністерство юстиції України) або засвідчувальному центрі (АЦСК).

– Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

– Про рішення щодо припинення діяльності центр сертифікації ключів повинен повідомити підписувачів за три місяці, якщо інші строки не визначено законодавством. Після повідомлення про припинення діяльності центр сертифікації ключів не має права видавати нові сертифікати ключів. Усі сертифікати ключів, що були видані центром сертифікації ключів, після припинення його діяльності скасовуються.

– ЦСК, що повідомив про припинення своєї діяльності, зобов'язаний забезпечити захист прав споживачів шляхом повернення грошей за послуги, що не можуть надаватися в подальшому, якщо вони були попередньо оплачені.

Певні вказані вимоги відповідають приписам Директиви ЄС 1999/93/ЕС.

2) **Технологічні та інші вимоги.**

– ЦСК зобов'язаний забезпечувати захист інформації в автоматизованих системах відповідно до законодавства. Фактично мова йде про дотримання численних вимог до захисту інформації в автоматизованих системах, які є занадто змістовними і детальними для цієї статті.

– ЦСК зобов'язаний забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством. Фактично, мова йде про дотримання організаційних вимог Закону України «Про захист персональних даних» [7], а також технічних та організаційних вимог до захисту інформації в автоматизованих системах, про які згадувалося вище.

– ЦСК зобов'язаний встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу.

– ЦСК зобов'язаний своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених цим Законом.

– ЦСК зобов'язаний своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;

– ЦСК зобов'язаний перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;

– ЦСК зобов'язаний цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

– ЦСК зобов'язаний вести електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

– ЦСК зобов'язаний забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

– ЦСК зобов'язаний забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

– ЦСК зобов'язаний надавати консультації з питань, пов'язаних з електронним цифровим підписом.

Здебільшого аналогічні вимоги містяться і в Директиві ЄС, але за суттєвим виключенням: найбільш суттєві і суворі вимоги щодо захисту інформації в інформаційних системах стосуються тільки діяльності осіб, які забезпечують обіг посилених сертифікатів ключів – в Україні це акредитовані центри сертифікації ключів.

Для початку діяльності ЦСК в Україні необхідно мати наступні документи:

1) Засвідчення власного відкритого ключа в центральному засвідчувальному органі (Міністерство юстиції України) або засвідчувальному центрі (АЦСК).

В процесі діяльності центру сертифікації ключів необхідно мати наступні документи:

2) Копія сертифікату відповідності на засоби криптографічного захисту інформації, що використовуються.

3) Копія сертифікату відповідності на засоби технічного захисту інформації, що використовуються.

Фактично, вимога що вказаних документів може бути дотримана за умови, що ЦСК використовує засоби криптографічного та технічного захисту інформації, розроблені та впроваджені третьою особою, яка має відповідні ліцензії на провадження діяльності у сфері криптографічного та/або технічного захисту інформації, а також

відповідні сертифікати відповідності на ці системи. Якщо ЦСК планує розробляти та впроваджувати системи криптографічного та/або технічного захисту інформації самостійно, йому доведеться ще й отримувати відповідні ліцензії та забезпечувати дотримання ліцензійних умов.

Все це робить процедуру створення простого центру сертифікації ключів в Україні занадто складною та дорогою. Для порівняння – Директива ЄС 1999/93/ЕС встановлює вимоги щодо технічного та криптографічного захисту інформації тільки щодо осіб, які забезпечують обіг посилених сертифікатів ключів.

Більше того, ч. 1 ст. 3 вказаної Директиви прямо визначає, що країни-учасниці окрім чітко визначених випадків взагалі не повинні вимагати проходження адміністративних процедур для початку провадження діяльності в сфері сертифікації ключів. Такими випадками, коли дотримання адміністративних процедур може вимагатися, є тільки діяльність у сфері надання посилених сертифікатів. І при цьому, впровадження таких адміністративних процедур може здійснюватися виключно на принципах об'єктивності, прозорості, пропорційності та недискримінаційності.

Також не можна обійти увагою питання визнання сертифікатів ключів електронного цифрового підпису, виданих в інших країнах.

Згідно з ст. 6 Закону України «Про електронний цифровий підпис» [2] фактично передбачено, що в Україні визнаються електронно-цифрові підписи, виконані за допомогою лише сертифікатів ключів, одержаних тільки в Україні. Таким чином, учасники правовідносин у сфері електронно-цифрового підпису фактично позбавлені можливості користуватися послугами іноземних компанії, які, доречи, є світовими лідерами у цій галузі і мають розвинену інфраструктуру.

На відміну від України, відповідно до ст. 7 Директиви ЄС 1999/93/ЕС прямо передбачено обов'язкове визнання сертифікатів ключів, виданих в третіх країнах, за умови, що такі сертифікати відповідають хоча б одній із трьох вимог:

(a) виконавець сертифікаційних послуг відповідає вимогам, викладеним в цій Директиві, і акредитований в системі добровільної акредитації, заснованої в державі-члені ЄС; або

(b) виконавець сертифікаційних послуг заснований в країні-члені ЄС і гарантує відповідність своїх сертифікатів вимогам цієї Директиви; або

(c) сертифікат або виконавець сертифікаційних послуг визнається за двосторонньою або багатосторонньою угодою між Європейським Співтовариством і третіми країнами або міжнародними організаціями.

Підводячи підсумок, слід зазначити, що вимоги українського законодавства до створення та діяльності центів сертифікації ключів є занадто надмірними порівняно з Європейським Союзом. Крім того, на відміну від ЄС, вимоги українського законодавства щодо створення та діяльності центрів сертифікації ключів викладені здебільшого у бланкетних та відсилочних нормах цілого ряду нормативно-правових актів. Все це дає підстави вважати, що існуюча в Україні нормативно-правова база суттєво стримує розвиток відповідних суспільних відносин у цій галузі.

На нашу думку, вказані недоліки не можуть бути виправлені внесенням окремих косметичних змін до чинного законодавства України. Найбільш оптимальним виходом із цієї ситуації було б узгодження національного законодавства України із Директивою ЄС «Про порядок використання електронних підписів в Європейському Співтовари-

стві» 1999/93/ЕС з метою суттєвого спрощення відповідних адміністративних процедур. При цьому, з нашої точки зору, було б оптимально, якщо відповідні вимоги були викладені в окремому нормативно-правовому акті.

ЛІТЕРАТУРА

1. Про електронну комерцію [Електронний ресурс] : проект Закону України від 17.06.2013 р. № 2306а. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47409.
2. Про електронний цифровий підпис [Текст] : Закон України від 22.05.2003 р. № 852-IV // Голос України. – 2003. – № 119.
3. Про електронні документи та електронний документообіг [Текст] : Закон України від 22.05.2003 р. № 851-IV // Голос України. – 2003. – № 119.
4. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093.
5. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності [Текст] : Постанова Каб. Міністрів України від 28.10.2004 р. № 1452 // Уряд. кур'єр. – 2004. – № 214.
6. Про затвердження Положення про центральний засвідчувальний орган [Текст] : Постанова Каб. Міністрів України від 28.10.2004 р. № 1451 // Уряд. кур'єр. – 2004. – № 214.
7. Про захист персональних даних [Текст] : Закон України від 01.10.2010 р. № 2297-VI // Голос України. – 2010. – № 172.

Бойко Д. В.

ТРЕБОВАНИЯ К ЦЕНТРАМ СЕРТИФИКАЦИИ КЛЮЧЕЙ

Статья посвящена анализу общих требований законодательства Украины к созданию и деятельности такого субъекта правоотношений в сфере оборота электронных цифровых подписей как центры сертификации ключей, а также анализу аналогичных требований в Европейском Союзе. В статье проанализированы основные требования к созданию и деятельности центров сертификации ключей, сформулированы предложения по усовершенствованию национального законодательства.

***Ключевые слова**: электронная коммерция, электронная цифровая подпись, центр сертификации ключей.*

D. Boyko

REQUIREMENTS TO KEY CERTIFICATION CENTERS

The article is devoted to the analyses of the Ukrainian legislation on the scope of electronic signatures. We analyzed the requirements to the key certification centers in Ukraine the relevant requirements of European legislation, namely – Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. The author proposes to bring Ukrainian legislation into conformity with the provisions of Directive 1999/93/EC.

***Key words:** e-commerce, digital signature, key certification center.*