

НАУКОВО-ПРАКТИЧНИЙ КОМЕНТАР

ДО

ЗАКОНУ УКРАЇНИ

«Про електронний цифровий підпис»

Київ - 2009

Зміст

Вступ	1
«Стаття 1. Визначення термінів.....	2
«Стаття 2. Суб'єкти правових відносин у сфері послуг електронного цифрового підпису	3
«Стаття 3. Правовий статус електронного цифрового підпису	4
«Стаття 4. Призначення електронного цифрового підпису	5
«Стаття 5. Особливості застосування електронного цифрового підпису	6
«Стаття 6. Вимоги до сертифіката ключа	14
«Стаття 7. Права та обов'язки підписувача	15
«Стаття 8. Центр сертифікації ключів.....	15
«Стаття 9. Акредитований центр сертифікації ключів.....	16
«Стаття 10. Засвідчувальний центр	17
«Стаття 11. Центральний засвідчувальний орган.....	18
«Стаття 12. Контролюючий орган	19
«Стаття 13. Скасування, блокування та поновлення посиленого сертифіката ключа.....	19
«Стаття 14. Припинення діяльності центру сертифікації ключів.....	20
«Стаття 15. Відповідальність за порушення законодавства про електронний цифровий підпис.....	21
«Стаття 16. Розв'язання спорів	21
«Стаття 17. Визнання іноземних сертифікатів ключів.....	21
«Стаття 18. Прикінцеві положення	21
Джерела:.....	23
Додаток 1	25
Додаток 2.....	33

НАУКОВО-ПРАКТИЧНИЙ КОМЕНТАР ДО ЗАКОНУ УКРАЇНИ «ПРО ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС»

Редакція від 10.02.2009 року

Цей науково-практичний коментар складено на виконання статті 8 Закону України «Про електронний цифровий підпис» в частині надання своїм дійсним та потенційним клієнтам консультацій в частині застосування електронного цифрового підпису в Україні.

Вступ

В повсякденне життя все більше входять новітні інформаційні технології. Сьогодні вже нікого не лякає думка про те, що дуже скоро більшість документів буде виконана в електронному вигляді і вони за юридичною силою будуть такі ж, як і паперові документи.

22 травня 2003 році Верховною Радою України прийнятий Закон України **«Про електронні документи та електронний документообіг»** [2], нормою статті 6 якого визначено, що:

«Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.»

Тому наразі актуальною є потреба поєднати знання юриспруденції та технологій цифрового підпису, щоб надати допомогу юристам, суддям, адвокатам, правознавцям та будь-яким іншим особам, що цікавляться питаннями застосування норм чинного законодавства при використанні електронних документів для вчинення правочинів.

Відповідно до статті 5 Закону України «Про електронні документи та електронний документообіг» термін **електронний документ** - це **«документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.**

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.»

Цей коментар стосується лише окремої форми електронного підпису – електронного цифрового підпису, застосування якого регулюється Законом «Про електронний цифровий підпис» (надалі по тексту коментаря використовується термін - Закон, або Закон про ЕЦП).

22 травня 2003 року Президентом України Л.Д.Кучмою підписано Закон України **«Про електронний цифровий підпис»** [1].

«Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

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

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.»

На сьогодні Верховною Радою України не ратифіковано жодної угоди з іншими країнами щодо електронного цифрового підпису. В першу чергу, на думку авторів коментаря, це пов'язано з тим, що в законодавстві багатьох країн застосовується поняття **«цифровий підпис»** (Digital Signature), який в цілому відповідає терміну електронний цифровий підпис, однак має ряд суттєвих відмінностей від прийнятого законодавчим органом Закону України «Про електронний цифровий підпис», як за сутністю, так і за обмеженнями у використанні. Законодавчі розбіжності на фоні загальної неузгодженості основних норм можуть призвести до самоізоляції України в світовому інформаційному просторі. Але детальний аналіз законодавчих розбіжностей та можливих наслідків є темою окремого дослідження, а деякі висновки автори коментаря раніше опублікували на сайті [24].

Діюча Конституція визначає що ратифіковані угоди є частиною українського законодавства та мають пріоритет над внутрішніми (наприклад, абзац 3 преамбули Закону про ЕЦП). До таких угод відносяться: «Декларація прав людини» ООН (1945 рік), Закон України «Про ратифікацію Угоди про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами» (№ 237-94-ВР від 10.11.1994), Угода про формування Єдиного економічного простору (Дата набуття чинності 20.05.2004 р.), Протокол про вступ України до Світової організації торгівлі 5 лютого 2008 року та Генеральні угоди ГАТТ, ГАТС. Цими законодавчими документами визначені зобов'язання України щодо зняття бар'єрів у міждержавних комунікаціях та торгівлі, гармонізації та коригування національної політики та нормативних актів, технічних правил і стандартів, комерційних стандартів, визнання пріоритетними стандартів міжнародних організацій, у тому числі Міжнародного союзу електрозв'язку та Міжнародної організації зі стандартизації, сприяння застосуванню технічних правил та стандартів ЄС і процедур оцінки відповідності тощо. Зважаючи на визначений Україною напрямок повноцінного вступу до Європейської Спільноти потрібно поступове скасування тих адміністративних процедур та звичаїв, які впливають із національного законодавства або раніше укладених угод, які перешкоджають свободі підприємницької діяльності і є бар'єрами в ефективній співпраці з ЄС та міжнародною спільнотою. Детальніше див. у коментарі до ст.5 Закону «Про ЕЦП».

Переважно українські закони починаються з тлумачення термінів, у тому числі і Закон «Про електронний цифровий підпис»:

«Стаття 1. Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

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 заблокованих 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.»

На перший погляд Стаття 1 досить насичена термінами, які надалі використовуються в Законі. Однак автори коментаря вважають, що цей перелік термінів не є вичерпним і залишає «білі плями» (прогалини), або дає суперечливі визначення. Так наприклад, стаття 2 Закону визначає одного з суб'єктів правових відносин у сфері електронного цифрового підпису (далі - ЕЦП) як «користувача», проте в Законі не визначений сам термін та не надано жодного пояснення про його права та обов'язки у правових відносинах.

Зважаючи на сучасне міжнародне законодавство в галузі цифрового підпису та електронного документообігу [7,8] та визначення Закону щодо обов'язків центрів сертифікації ключів, можна навести таке визначення терміну: «Користувач – особа, яка перевіряє електронний цифровий підпис, що накладений підписувачем на електронний документ, та яка під час перевірки покладається на належність і чинність сертифіката підписувача та дійсність інформації, зазначеної у цьому сертифікаті.».

Проаналізуємо певні статті Закону більш детально.

«Стаття 2. Суб'єкти правових відносин у сфері послуг електронного цифрового підпису

Суб'єктами правових відносин у сфері послуг електронного цифрового підпису є:

підписувач;

користувач;

центр сертифікації ключів;

акредитований центр сертифікації ключів;

центральний засвідчувальний орган;

*засвідчувальний центр органу виконавчої влади або іншого державного органу (далі - засвідчувальний центр);
контролюючий орган.»*

Цією статтею визначений перелік суб'єктів правових відносин у сфері послуг ЕЦП, до якого входить «користувач», але визначення терміну та правового статусу цього суб'єкта Закон не дає.

Права та обов'язки інших суб'єктів, вказаних у цій статті, описані статтями 7, 8, 9, 10, 11 та 12 цього Закону.

«Стаття 3. Правовий статус електронного цифрового підпису

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.

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

Стаття 3 Закону є наріжним каменем застосування електронного цифрового підпису в електронному документообігу, через те, що визначає правовий статус не лише електронного цифрового підпису, але й електронних документів в цілому, обов'язковим реквізитом яких є ЕЦП (стаття 6 Закону України «Про електронні документи та електронний документообіг»).

ЕЦП прирівнюється до власноручного підпису (печатки) тільки у випадку виконання всіх трьох умов. Дві з трьох умов вимагають використання посиленого сертифікату, який є українським ноу-хау і не визначений міжнародним та Європейським законодавством (Директивою ЄС 1999/93/ЄС [7] або Модельним законом ООН про електронні підписи), якими визначається удосконалений електронний підпис та кваліфікований сертифікат, і які є міжнародними умовами визнання цифрового підпису еквівалентним власноручному та вимоги до яких дещо інші [24]. Параметри для посиленого сертифіката не відображені у стандартах X.509¹ і однозначний зв'язок між посиленим та кваліфікованим сертифікатом ключа законодавцем не встановлений.

Законодавство ЄС на відміну від українського під електронним підписом розуміє не тільки *ідентифікацію* автора, а і *достовірність/цілісність* самих підписаних даних. Поняття «електронного цифрового підпису» у Законі України є більш слабким ніж визначення «удосконалений електронний підпис» Директиви ЄС, який визнається еквівалентним власноручному, оскільки для ЕЦП відсутня ключова вимога щодо забезпечення можливості автору підпису утримувати **під своїм повним контролем** засіб створення підпису (особистий ключ підпису). Крім того, обов'язкові вимоги до «*безпечного механізму створення підпису*» Директиви ЄС відрізняються від вимоги до «*надійного засобу електронного цифрового підпису*», регламентованою Законом України, як об'єкту, який має сертифікат відповідності виключно українського походження.

В той же час Закон вказує норму, згідно з якою **електронний цифровий підпис, як вид електронного підпису, не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.**

Важливою гарантією реалізації цивільних прав учасниками правовідносин є презумпція правомірності правочину, яка полягає у припущенні, що особа, вчиняючи правочин, діє правомірно. **Як зазначено у ст.204 Цивільного кодексу України (далі - ЦК), правочин є**

¹ комплекс стандартів міжнародного технічного комітету ІТУ-Т у цій галузі позначається як X.509, який є обов'язковим та якого дотримуються практично всі держави, які впроваджують національні та міжнародні системи електронного документообігу з використанням цифрового підпису.

правомірним, якщо його недійсність прямо не встановлена законом або якщо він не визнаний судом недійсним.

Своїм підґрунтям встановлення презумпції правомірності правочину має визначальний принцип приватного права: "Дозволено усе, що прямо не заборонено законом", а також такі засади цивільного права, як свобода договору (правочину); свобода підприємницької діяльності, не забороненої законом; справедливість, добросовісність та розумність цивільного законодавства. Згідно з цими засадами припускається, що **суб'єкт цивільного права, реалізуючи право свободи правочину, може вчиняти з метою створення, зміни, припинення цивільних прав і обов'язків тощо будь-які правомірні дії.** При цьому не вимагається прямої вказівки на правомірність дій у акті цивільного законодавства: достатньо, що закон не визначає ці дії, як заборонені.

Спростування презумпції правомірності правочину можливе у разі:

1) визнання неправомірності правочину прямим приписом закону. В цьому разі правочин неправомірний і не створює правових наслідків. Він є недійсним вже з моменту вчинення, оскільки припис закону забороняє такі дії на сьогоднішній день і на майбутнє. Такий правочин є нікчемним і спеціального визнання його недійсним у судовому порядку не вимагається. Нікчемним є, наприклад, правочин, укладений з порушенням вимоги про обов'язкову нотаріальну форму (ст.219 ЦК);

2) визнання неправомірності правочину судом. У цьому разі презумпція правомірності правочину існує в момент укладення правочину, оскільки він не порушує конкретної норми закону (або у момент укладення правочину порушення закону залишається прихованим, невідомим іншим особам). Проте його правомірність може бути оскаржена однією із сторін або іншою заінтересованою особою, а відтак правочин може бути визнаний судом недійсним.

Виходячи з того, що Цивільний кодекс України має переважне значення в трактуванні норм законодавства України перед Законом України «Про електронний цифровий підпис», **вимога Закону щодо використання лише посиленого сертифікату в якості аналога власноручного підпису йде в супереч справедливості, добросовісності та розумності цивільного законодавства - основним засадам цивільних прав громадян України.** (див. коментар до ст.5 Закону про ЕЦП нижче)

«Стаття 4. Призначення електронного цифрового підпису

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

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

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

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

Так законодавець України визначив цільове призначення ЕЦП - для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Проте ряд протиріч та невідповідностей в Законі, про які йдеться в цьому коментарі, веде до великих труднощів та іноді неможливості застосування електронного цифрового підпису та використання електронних документів в роботі державних і місцевих органів, органів юстиції, фізичних осіб та в господарській діяльності. В якості прикладу можна навести «Інструкцію про порядок вчинення нотаріальних дій нотаріусами України» [22], за якою вони зобов'язані завіряти електронні цифрові підписи у своїй діяльності (підпункт 26) п.2 глава 1, п.264 розділ 28), але практичної можливості виконувати такі дії вони не мають. Цією ж Інструкцією нотаріуси можуть застосовувати електронний цифровий підпис для здійснення правочинів (п.18 глава 2), а вимоги до застосування практично повторюють норми

Закону «Про електронний цифровий підпис» по статтях 5 та 6, які розглянуті нижче. На цей час нотаріус практично не може вчинити посвідчувальний напис (п.264 розділ 28) з причин, які наведені нижче у коментарі до статей 5 та 7 Закону, не кажучи вже про проставлення «апостилю» (п.257 розділ 27), як печатки відповідного зразка, і яке потребує застосування засобів накладання та перевірки цифрового підпису, повністю сумісного з міжнародними нормами та технічними стандартами.

Власне, вимоги, які зазначені в Інструкції, не відповідають встановленій останнім абзацом ст.4 нормі Закону «Про електронний цифровий підпис», якою визначено, що порядок нотаріальних дій встановлюється законом, а не підзаконним актом, яким є Інструкція.

«Стаття 5. Особливості застосування електронного цифрового підпису»

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим центром сертифікації ключів, а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються електронними цифровими підписами без сертифіката ключа, визначається суб'єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Захист прав споживачів послуг електронного цифрового підпису, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України "Про захист прав споживачів".

У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для таких цілей.

Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України.

Порядок застосування цифрового підпису в банківській діяльності визначається Національним банком України.»

Норма статті 5 має принципове значення в даний час і в майбутньому для використання електронного документообігу із застосуванням електронного цифрового підпису при взаємодії між собою громадян України з органами державної влади, громадян з юридичними особами будь-якої форми власності, державних органів України між собою та з іншими організаціями і підприємствами, а також у сфері взаємодії з іноземними державами, громадянами та бізнесом.

Так, український законодавець визначив, що органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

З огляду на те, що стаття 1 Закону чітко визначає поняття «засвідчення чинності відкритого ключа», як процедури формування сертифіката відкритого ключа (і лише формування), частина перша статті 5 зрозумілою для пересічного громадянина України мовою звучить так: **«Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для формування сертифікату відкритого ключа використовують лише такий сертифікат, який має позначку - посилений».**

У випадках, коли відповідно до законодавства України необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на

електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для таких цілей.

Законодавець встановив норму, що порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України.

Кабінет Міністрів України Постановою від 28 жовтня 2004 р. № 1453 [9] затвердив типовий порядок здійснення електронного документообігу в органах виконавчої влади.

Цитуємо: **«3. Орган виконавчої влади здійснює електронний документообіг лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, одержаним на ці засоби від спеціально уповноваженого центрального органу виконавчої влади у сфері криптографічного захисту інформації, та наявності посиленних сертифікатів відкритих ключів у своїх працівників - підписувачів.»**

Пункт 3 Порядку про здійснення електронного документообігу в органах виконавчої влади встановив обов'язковість лише для посадових осіб та працівників органів виконавчої влади використання лише посиленних сертифікатів відкритих ключів і жодним чином не обмежив використання інших видів сертифікатів відкритих ключів для інших громадян України. Тобто, направлення електронного документу, підписаного з використанням сертифікату відкритого ключа, який не є посиленим, не суперечить пункту 3 Порядку про здійснення електронного документообігу в органах виконавчої влади.

Пункт 8 Порядку про здійснення електронного документообігу в органах виконавчої влади встановлює спеціальні вимоги для електронного документу, невиконання яких, дає органу виконавчої влади право відхилити надісланий електронний документ, а саме:

«8. Електронний документ, що надійшов на адресу органу виконавчої влади, підлягає відхиленню у разі:

- відсутності у адресата надійних засобів електронного цифрового підпису;

- надходження не за адресою;

- зараження вірусом;

- негативного результату перевірки на цілісність і справжність усіх накладених на нього електронних цифрових підписів».

Найбільш цікавою вимогою для авторів цього коментаря є «відсутність у адресата надійних засобів електронного цифрового підпису».

Деякі представники виконавчої влади трактують вимоги цього пункту наступним чином: «Якщо хтось хоче відправити до органу виконавчої влади електронний документ з електронним цифровим підписом, то він повинен мати надійні засоби електронного цифрового підпису, тобто такі, що мають 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 відповідно до статті 1 Закону України «Про електронний цифровий підпис».

По-перше, це безглуздо. Тому, що немає жодних механізмів у держави перевіряти наявність у відправника надійного засобу електронного цифрового підпису.

По-друге, Порядок однозначно говорить, що цей пункт стосується адресата, тобто того, на чю адресу відправляється кореспонденція (електронний документ). Тим більше, що Закон України «Про поштовий зв'язок» статтею 1 чітко визначає термін «адресат». Цитуємо: **«адресат (одержувач) - юридична або фізична особа, якій адресується поштове відправлення, телеграфне чи інше повідомлення».**

«10. Кожен одержаний адресатом електронний документ перевіряється на цілісність і справжність усіх накладених на нього електронних цифрових підписів, включаючи ті, що накладені (проставлені) згідно із законодавством як аналоги печатки (далі - електронні печатки). При цьому необхідно, щоб:

- **кожен електронний цифровий підпис був підтверджений 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 відповідав відкритому ключу, зазначеному у сертифікаті;**
- **на час перевірки був чинним посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів та/або посилений сертифікат відкритого ключа відповідного засвідчувального центру.»**

Пункт 10 Порядку про здійснення електронного документообігу в органах виконавчої влади встановлює вимоги до перевірки електронного документу.

Парадокс полягає в тому, що електронний документ, який не має вірусів та підписаний з використанням сертифікату ключа, що не є посиленим, за наявності у органа державної влади надійного засобу електронного цифрового підпису, не може бути відхилений (п.8 Порядку та стаття 3 Закону «Про ЕЦП»), але й не проходить перевірку на цілісність і справжність через те, що не був підписаний ЕЦП з використанням посиленого сертифікату відкритого ключа (п.10 Порядку).

Складається думка, що Уряд України, готуючи цей Порядок здійснення електронного документообігу в органах виконавчої влади, мав на увазі лише перевірку підпису електронного документа з використанням посиленого сертифікату відкритого ключа, який надійшов від іншого органу виконавчої влади.

В іншому випадку, вочевидь, Кабінет Міністрів України порушив норму статті 3 Закону України «Про електронний цифровий підпис», згідно якої **електронний цифровий підпис, як вид електронного підпису, не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.**

Тим більше, що статтями Конституції України визнано:

«Стаття 21. Усі люди є вільні і рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними.»

«Стаття 22. Права і свободи людини і громадянина, закріплені цією Конституцією, не є вичерпними.

Конституційні права і свободи гарантуються і не можуть бути скасовані.

При прийнятті нових законів або внесенні змін до чинних законів не допускається звуження змісту та обсягу існуючих прав і свобод.»

«Стаття 24. Громадяни мають рівні конституційні права і свободи та є рівними перед законом.

Не може бути привілеїв чи обмежень за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками.»

«Стаття 40. Усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк».

Кабінет Міністрів України в будь-якому випадку не міг допустити звуження змісту або обсягу існуючих прав і свобод. А це означає, що **орган виконавчої влади зобов'язаний приймати електронний документ, підписаний ЕЦП без використання посиленого сертифікату від громадян України так само, як і електронний документ, що підписаний ЕЦП з використанням посиленого сертифікату.**

Додатково автори цього коментарю звертають увагу на статті 8 і 68 Конституції України:

«Стаття 8. В Україні визнається і діє принцип верховенства права.

Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй.

Норми Конституції України є нормами прямої дії. Звернення до суду для захисту конституційних прав і свобод людини і громадянина безпосередньо на підставі Конституції України гарантується.»

«Стаття 68. Кожен зобов'язаний неухильно додержуватися Конституції України та законів України, не посягати на права і свободи, честь і гідність інших людей.

Незнання законів не звільняє від юридичної відповідальності»

В той же день, 28 жовтня 2004 року, КМ України приймає іншу Постанову за №1452 [10], яка регламентує порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності.

Цитуємо деякі пункти:

«2. Установа застосовує електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису, що повинне бути підтверджено сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від спеціально уповноваженого центрального органу виконавчої влади у сфері криптографічного захисту інформації, та наявності посиленних сертифікатів відкритих ключів у своїх працівників – підписувачів.

3. Установа застосовує електронний цифровий підпис для вчинення правочинів за участю інших юридичних та фізичних осіб лише за наявності у них посиленних сертифікатів відкритих ключів.

...

5. Установа отримує на договірних засадах послуги, пов'язані з електронним цифровим підписом, від акредитованого центру сертифікації ключів. При цьому установа може отримувати такі послуги лише від одного акредитованого центру сертифікації ключів. Використання підписувачами особистих ключів, відповідні відкриті ключі яких засвідчені іншими акредитованими центрами сертифікації ключів, забороняється.

...

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

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

Пункт 2 вказаної Постанови жодним чином не обмежує права громадян України і встановлює вимоги для застосування ЕЦП лише для працівників органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності.

Пункт 3 Порядку вимагає обов'язковість мати юридичним та фізичним особам посилені сертифікати відкритих ключів для укладання правочинів з органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності (дво – або багатосторонні правочини).

Вочевидь, що **Постанова №1452 від 28 жовтня 2004 року жодним чином не стосується односторонніх правочинів.** Тобто цей нормативно-правовий документ жодним чином не регламентує умови складання електронного документу з ЕЦП щодо ознаки посиленого сертифікату для подальшого його направлення в органи державної влади.

Закон розрізняє два випадки визначення місця вчинення правочину: 1) стосовно вчинення одностороннього правочину; 2) стосовно вчинення дво- або багатостороннього правочину (договору).

Стосовно одностороннього правочину правило про встановлення місця його вчинення безпосередньо сформульоване у ст.211 ЦК [5], місцем вчинення є місце волевиявлення сторони. Волевиявлення можливе у різних формах: усній, письмовій, з нотаріальним посвідченням, з наступною державною реєстрацією (ст.ст.207-210 ЦК). Відповідно форма

волевиявлення може полегшувати або ускладнювати встановлення місця вчинення правочину. Зокрема, практично неможливо встановити місце вчинення одностороннього правочину, вчиненого в усній формі. Досить складно встановити місце вчинення правочину, вчиненого у простій письмовій формі (в тому числі електронній), хіба що у ньому самому може міститися вказівка на таке місце або воно може впливати зі змісту правочину. Наприклад, довіреність у простій письмовій формі може бути посвідчена посадовою особою за місцем перебування або проживання особи, яка її видає (ст.245 ЦК). Отже, і місцем видачі довіреності буде вважатися місце, де засвідчено підпис того, хто її видав. Простіше встановити місце вчинення правочину, якщо він посвідчується нотаріально. Наприклад, місцем вчинення заповіту є місце, де він був складений і нотаріально посвідчений (ст.ст. 1247, 1248 ЦК).

Місце вчинення дво- або багатостороннього правочину (договору) визначається відповідно до правил ст.647 ЦК. Ця норма передбачає, що договір є укладеним у місці проживання фізичної особи (ст.29 ЦК) або за місцезнаходженням юридичної особи (ст.93 ЦК), яка зробила пропозицію (лат. offertus - оферта запропонований) укласти договір, якщо інше не встановлено договором.

Певні труднощі викликає встановлення місця вчинення правочину, який підлягає державній реєстрації, у випадку коли укладення договору відбулося в одному місці, а реєстрація — в іншому. Оскільки такий правочин набуває чинності з моменту його державної реєстрації (ст.210 ЦК), то вирішальне значення мусить мати не місце волевиявлення чи місце проживання фізичної особи або місцезнаходження юридичної особи, а місце державної реєстрації правочину. Адаже до реєстрації правочин вважається таким, що не укладений взагалі.

Законодавець, коли випишував норми для місця здійснення правочинів, жодним чином не враховував особливості укладання правочинів в електронному вигляді.

Умовами чинності правочинів є дотримання вимог:

1) щодо змісту правочину. Зміст правочину не може суперечити актам цивільного законодавства та моральним засадам суспільства (ч. 1 ст.203 ЦК), тобто фізичні та юридичні особи мають враховувати вимоги щодо здійснення цивільних прав, встановлені в ст.ст. 12, 13 ЦК та інших актах цивільного законодавства;

2) щодо наявності правочиноздатності суб'єктів правочину. Правочини можуть укладати лише особи, які мають необхідний обсяг цивільної дієздатності (ч.2 ст.203, ст.ст.30-32, 34-39, 41, 42, 92 ЦК);

3) щодо відповідності волевиявлення внутрішній волі суб'єкта (суб'єктів) правочину (ч.3 ст.203). Наявність правочину свідчить про єдність внутрішньої волі й волевиявлення суб'єкта (суб'єктів) правочину. Тому у випадку, коли воля суб'єкта правочину формувалася не вільно і не відповідала волевиявленню (наприклад, мало місце насильство), такий правочин визнається недійсним (ст.231 ЦК);

4) щодо форми правочину. При укладенні правочину обов'язкове дотримання передбаченої законом форми (ч.4 ст.203). Порушення вимог щодо форми правочину призводить до визнання його недійсним або настання інших наслідків (ст.ст.218-220 ЦК);

5) щодо реальності правочину. Правочин має бути реальним, тобто спрямованим на реальне настання правових наслідків, що обумовлені ним (ч.3 ст.203). Тому правочин, вчинений без наміру створити правові наслідки, є недійсним як фіктивний, тобто вчинений лише про людське око (ст.234 ЦК).

Виходячи з наведеного вище, стає очевидним, що **вимога щодо обов'язковості фізичній особі або юридичній особі мати посилений сертифікат ключа не витримує жодної правової критики**. Такий висновок впливає з аналізу національного законодавства та міжнародних угод, які ратифікувала Україна.

Питання використання ЕЦП стосується не тільки спілкування з органами державної влади юридичних та фізичних осіб, але й забезпечення прав людини у відповідності з законодавством, у тому числі міжнародним, яке ратифіковане Україною та міжнародними угодами України. В цій частині держава Україна відіграє найсуттєвішу роль у забезпеченні

прав та свобод громадян у цивільних відносинах. Вказані права ґрунтуються на Конституції України, Законах та інших законодавчих актах.

Зокрема, діюча Конституція визначає що ратифіковані угоди є частиною українського законодавства та мають пріоритет над внутрішніми (наприклад, абзац 3 преамбули Закону про ЕЦП). До таких угод відносяться: «Декларація прав людини» ООН (1945 рік), Закон України «Про ратифікацію Угоди про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами» (№ 237-94-ВР від 10.11.1994), Угода про формування Єдиного економічного простору (Дата набуття чинності 20.05.2004 р.), Протокол про вступ України до Світової організації торгівлі 5 лютого 2008 року та Генеральні угоди ГАТТ, ГАТС. Цими законодавчими документами зобов'язанні України щодо зняття бар'єрів у міждержавних комунікаціях та торгівлі, **гармонізація та коригування національної політики та нормативних актів, через технічні правила і стандарти та комерційні стандарти, визнання пріоритетними стандартів міжнародних організацій, у тому числі Міжнародного союзу електрозв'язку та Міжнародної організації із стандартизації, сприяння застосуванню технічних правил ЄС та європейських стандартів і процедур оцінки відповідності тощо.** Зважаючи на визначений Україною напрямок повноцінного вступу до Європейської Спільноти потрібно поступове скасування тих адміністративних процедур та звичаїв, що впливають із національного законодавства чи угод, укладених раніше, та які перешкоджають свободі підприємницької діяльності, які є бар'єром у ефективній співпраці з ЄС та міжнародною спільнотою.

Відповідно Україна та її державні органи та організації зобов'язані максимально сприяти впровадженню міжнародних норм та стандартів у практиці взаємовідносин між державою, особами різних форм власності та громадянами, а також імплементації міжнародних та європейських умов визнання правочинів у практичну діяльність в Україні в галузях електронного документообігу та електронної комерції. Широке застосування електронних підписів можливе лише в умовах мінімізації обмежень та дотримання єдиних технічних стандартів у цій сфері, а також лібералізації законодавства щодо застосування електронного документообігу у цивільних та громадських відносинах.

Звертаючись до діючого законодавства України та обмеження **Постанови №1452** в частині обов'язковості мати посилений сертифікат для усіх підписувачів в Україні, можна зазначити, що це обмеження **фактично відміняє норму**, визначену останнім абзацом ст.3 Закону, **про неможливість невизнання електронного підпису** виключно через його електронну форму чи тому, що він не ґрунтується на посиленому сертифікаті ключа підписувача (та користувача), по крайній мірі для державних органів та їх службовців. Накладання ж технічних обмежень може призвести до не виконання зобов'язань України, узятих на себе за вищенаведеними міжнародними угодами та неможливості ефективного застосування ЕЦП у різних сферах економіки та діяльності держави.

Вказане обмеження є **технічним обмеженням**, яке включає такі обов'язкові елементи:

- використання виключно криптографічних стандартів, які діють в Україні;
- використання засобів ЕЦП, які мають сертифікат відповідності або позитивний експертний висновок регулюючого органу (ДССЗЗІ України);
- використання виключно сертифікатів, які видані акредитованими центрами сертифікації ключів.

Стосовно трактування можливостей визнання еквівалентів власноручного підпису, слід зазначити таке:

Ст. 207 ЦК України визначає застосування власноручного підпису (частково у ст.1248 - засвідчення заповіту нотаріусом). Іншими статтями визначається необхідність письмової форми правочину та підписання документів (без визначення форми підпису) і фактично є посиланням саме на ст.207 ЦК.

Стаття 207 ЦК України вводить ряд норм щодо письмової форми вчинення правочину, зокрема **визначення форми підпису та аналогів власноручного підпису** вказане у п.3:

«3. Використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або **іншого аналога власноручного підпису** допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів.»

Використання будь-яких аналогів власноручного підпису є правомірним при здійсненні правочинів згідно до п.1 Ст.204 ЦК. (Презумпція правомірності правочину): «1. **Правочин є правомірним, якщо його недійсність прямо не встановлена законом** або якщо він не визнаний судом недійсним». Використання ЕЦП, що не ґрунтується на надійних засобах ЕПЦ або на посиленому сертифікаті, не тільки **не заперечується** Законом про ЕЦП або будь-яким іншим, а і **напряму дозволено** ст.5 цього Закону, у тому числі на договірних засадах. При цьому якісь додаткові обмеження для осіб, що взаємодіють з державною влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності Законом **не передбачені**.

Договірна форма відносин між підписувачами та центрами сертифікації ключів, передбачена Законом про ЕЦП і яка на практиці фактично регулює взаємовідносини між ними, **повністю задовольняє вимогу п.3 Ст.207 ЦК** щодо дозволу вчиненні правочинів «за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів» і **не передбачає будь-яких додаткових обмежень**. Центри сертифікації ключів, які зареєстровані в Україні або в інших державах згідно законодавства, виконують функції **документального засвідчення** чинності і належності відкритого ключа підписувача (ст.1 Закону «Про ЕЦП») і **діють завжди на договірних засадах**, і виступають гарантами для усіх користувачів ЕЦП, у тому числі – державних органів, ідентифікації підписувача та цілісності підписаного ним документу, якщо перевірка ЕЦП завершилася успішно (перевірка ЕЦП виконана без помилок).

Більш детально висновки з цього приводу викладені у Додатку 1 до цього Коментаря.

В той же час умова підписання документу в електронному вигляді за адресою (у приміщенні) державного органу є правомірною і обґрунтованою, тому що дає останньому можливість перевірити повноваження представника іншої юридичної особи або фізичної особи.

Пункт 5 Порядку вимагає, щоб установа користувалася послугами лише одного акредитованого центру сертифікації ключів. На жаль, Уряд не побачив тих технічних проблем, які виникають у багатофіліальної структури, філії якої можуть бути в різних точках країни, а присутність там одного і того ж акредитованого центру обмежена.

Більш того, Порядок забороняє використання підписувачами особистих ключів, відповідні відкриті ключі яких засвідчені іншими акредитованими центрами сертифікації ключів. Стає зовсім незрозуміло, **що робити, коли дві державні установи, які отримують послуги ЕЦП від різних акредитованих центрів сертифікації ключів, мають необхідність укласти двосторонній правочин в електронному виді**. Ця норма потребує особливої уваги з боку Антимонопольного комітету України. Але це не є предметом цього коментарю.

Порядок застосування цифрового підпису в банківській діяльності визначається Національним банком України. Ця норма Закону стосується лише застосування ЕЦП всередині банківської системи України і жодним чином не може зачіпати відносини у електронному вигляді між будь-яким банком та громадянином України, якщо інше не встановлено договором між ними з причин, які визначені вище.

Необхідно звернути увагу також на те, що Постановою КМУ №1453 введений порядок Правил електронного документообігу **обов'язковий** тільки для органів виконавчої влади, а для органів місцевого самоврядування він *рекомендаційний* (а для організацій та установ державної форми власності і інших органів державної влади він не регламентується) та, одночасно, Постановою КМУ №1452 регламентацією використання електронного цифрового підпису фактично такий порядок виключається, оскільки порядок застосування ЕПЦ

визначається вже для органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності.

Слід також звернути увагу на те, що згідно з Постановою № 1453, **порядок роботи з електронними документами, що містять інформацію з обмеженим доступом, яка є власністю держави, та порядок роботи з електронними документами за зверненнями громадян, повинні бути визначені спеціальними нормативно-правовими актами, яких нажаль, досі немає.**

Робота із зверненнями громадян є однією з суттєвих функцій державних та місцевих органів, показником рівня демократії та відкритості України та наочним свідомством результатів роботи у напрямку реалізації прагнення отримати статус країни-учасника Європейської спільноти. З точки зору можливих відмов державних службовців органів влади і місцевого самоврядування у прийнятті до розгляду звернень громадян в електронному вигляді та неправомірності розглянутих вище обмежень щодо ЕЦП в Україні слід звернутись до Закону України «Про звернення громадян» № 393/96-ВР від 2 жовтня 1996 року та Указу Президента України «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування» № 109/2008 від 7 лютого 2008 року. Законом України «Про звернення громадян» передбачена **цивільна, адміністративна або кримінальна відповідальність** за дії або бездіяльність, які порушують норми Закону. Законом «Про звернення громадян» чітко визначені підстави та порядок, коли звернення повертається громадянину, який його направив до установи (статті 5, 7 та 8), і серед таких підстав немає якихось обмежень щодо кваліфікації належності підпису. Законодавством України встановлений ряд норм, які обмежують свавілля чиновників та прямо передбачають відповідальність за протиправні дії, як то: за статтею 212-3 **Кодексу України про адміністративні правопорушення** – штраф від п'ятнадцяти до двадцяти п'яти (за повторне – до п'ятдесяти) неоподатковуваних мінімумів доходів громадян, за статтею 8 Закону України «**Про боротьбу з корупцією**» – адміністративне стягнення у вигляді штрафу з посадової особи, яка здійснила порушення, а за ст.10 цього ж Закону передбачена така ж відповідальність для керівників установ у разі умисного невжиття заходів до щодо припинення таких діянь. Також за **Законом «Про державну службу»** можливе застосування дисциплінарних стягнень (ст.14), звільнення службовця з державної служби (ст.30) та відшкодування збитків громадянам за судовим рішенням, як передбачено Законом «Про звернення громадян» (ст. 19, 25).

Більш детально висновки з цього приводу викладені у Додатку 2 до цього Коментаря.

Слід також зауважити, що передбачені Указом Президента України “Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування” заходи на виконання Закону України «Про звернення громадян», а саме: запровадження прийняття та розгляду звернень громадян до органів державної влади з використанням мережі Інтернет, внесення на розгляд ВР України розробленого Адміністративно-процедурного кодексу, законопроект про внесення змін до законодавчих актів щодо вдосконалення правового регулювання питань гарантування права громадян на звернення, єдиного загальнодержавного класифікатору звернень громадян та єдиної комп'ютерної системи обліку звернень громадян та контролю за вирішенням порушених у них питань в органах виконавчої влади та органах місцевого самоврядування, Кабінетом Міністрів України не виконано досі, хоча строки були встановлені не пізніше вересня 2008 року.

Відповідно до п.3 Постанови КМУ № 1453 повинні були бути розроблені та затверджені технічні умови (далі – ТУ) на систему електронного документообігу органу виконавчої влади Державним департаментом з питань зв'язку та інформатизації разом з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки за участю фахівців Секретаріату Кабінету Міністрів України. Однак у ТУ (ТУ У 30.0-33240054-001:2005 [23]) затверджені Наказом Держзв'язку від 7 червня 2005 р. № 70 (в останній редакції за Наказом Держзв'язку №52 від 10 квітня 2006 р.) використання електронного цифрового підпису є **необов'язковим** (п.3.17.3 - Інформаційна частина повідомлення про електронний

документ). Незрозуміло, чому в ТУ проігноровані вимоги Законів «Про електронний цифровий підпис» і «Про електронний документообіг» та Постанови КМУ № 1453 щодо обов'язковості ЕЦП для електронних документів і чи була погоджена така редакція ТУ визначеними вказаною Постановою співвиконавцями.

Таке нагромадження протиріч є одним з вагомих факторів гальмування розвитку систем електронного документообігу та застосування ЕЦП в Україні, а також є значною перешкодою для реалізації планів входження України до єдиного інформаційного простору Європи та світу.

«Стаття 6. Вимоги до сертифіката ключа

Сертифікат ключа містить такі обов'язкові дані:
найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
зазначення, що сертифікат виданий в Україні;
унікальний реєстраційний номер сертифіката ключа;
основні дані (реквізити) підписувача - власника особистого ключа;
дату і час початку та закінчення строку чинності сертифіката;
відкритий ключ;
найменування криптографічного алгоритму, що використовується власником особистого ключа;
інформацію про обмеження використання підпису.
Посилений сертифікат ключа, крім обов'язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.
Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.»

Автори цього коментаря звертають увагу на дуже суттєву помилку, якої припустилися законодавці у формулюванні вимог до сертифікату ключа. В переліку **фактично відсутня** вимога щодо обов'язковості **засвідчення чинності відкритого ключа** оскільки немає електронного цифрового підпису Центру сертифікації ключів, яким він повинен засвідчувати справжність таких даних в сертифікаті. Цей реквізит є **обов'язковим** у всіх національних та міжнародних законах, стандартах X.509, і більш того, відсутність серед обов'язкових елементів сертифікату цифрового підпису Центру сертифікації є порушенням вимог як Закону «Про електронний цифровий підпис» (стаття 1) у відповідності до визначення сертифікату як «документа» в електронному вигляді, так і вимог щодо «Електронного документа» за Законом «Про електронний документообіг» (ст. 6), який повинен обов'язково мати електронний цифровий підпис.

Зацікавленість авторів коментаря також викликало зазначення норми, що сертифікат виданий в Україні. Така норма є зрозумілою лише, якщо назва статті «Вимоги до сертифіката ключа» розуміється виключно як «Вимоги до сертифіката ключа, засвідченого (сформованого) в Україні».

Зважаючи на те, що створення національної інфраструктури електронного цифрового підпису в Україні декларується на базі комплексу міжнародних технічних стандартів X.509 в цій галузі (перший з необхідних стандартів впроваджений у 2006 році [20]), можна було б очікувати, що технічні специфікації будуть повністю відповідати таким стандартам. Однак цей базовий стандарт був прийнятий всього лише «за основу».

Вочевидь, що посилений сертифікат ключа технологічно відрізняється від звичайного сертифікату ключа лише ознакою, яка є необов'язковою у площині стандарту X.509.

Крім того, слід зауважити, що формулювання одного з обов'язкових реквізитів сертифікату «найменування криптографічного алгоритму, що використовується власником особистого ключа», за своєю технічною сутністю є **принципово не вірним**, бо за стандартами X.509 - це „ідентифікатор алгоритму підпису і його параметри, які використовуються центром сертифікації ключів під час створення сертифікату ключа”, тобто це той алгоритм, який використовується не власником особистого ключа, а центром

сертифікації ключів для засвідчення сертифікату (підпису сертифіката). Отже, і застосування якогось криптографічного алгоритму регулюється не самим власником, а центром сертифікації ключів, і як наслідок – можливостей підписувача використовувати криптографічні алгоритми для накладання цифрового підпису.

«Стаття 7. Права та обов'язки підписувача

Підписувач має право:

вимагати скасування, блокування або поновлення свого сертифіката ключа;

оскаржити дії чи бездіяльність центру сертифікації ключів у судовому порядку.

Підписувач зобов'язаний:

зберігати особистий ключ у таємниці;

надавати центру сертифікації ключів дані згідно з вимогами статті 6 цього Закону для засвідчення чинності відкритого ключа;

своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа.»

Стаття 7 Закону визначає права та обов'язки підписувача. Підписувач має право вимагати скасування, блокування або поновлення свого сертифіката ключа. На жаль, законодавець не надав однозначного тлумачення дій по скасуванню та поновленню сертифіката (ст. 13 Закону). Термін «блокування» визначений статтею 1 Закону.

Скасування сертифіката – процедура, виконання якої веде до безповоротної втрати чинності сертифіката.

Поновлення – процедура поновлення заблокованого сертифікату у статусі чинного.

Звертаючись до Постанови КМУ № 1452, слід звернути увагу на вимогу використання підписувачем тільки одного особистого ключа та відповідного йому сертифіката (п.17 Порядку) та обов'язковості в сертифікаті вказівки про найменування криптографічного алгоритму, який використовується (ст. 6 Закону). В Україні на даний час діють декілька алгоритмів криптографічних перетворень, які затверджені державними або міждержавними стандартами і будь-який з них може легально використовуватись: ДСТУ 4145-2002, ГОСТ 34.310-95, ГОСТ 34.311-95, ГОСТ 28147-89. В сертифікаті може бути вказаний лише один алгоритм з діючих в Україні, крім того, їх реалізації різними розробниками відрізняються. Для вдалої обробки електронних документів, підписаних ЕЦП іншої особи-відправника, отримувач (користувач) повинен мати програмне забезпечення накладання/перевірки ЕЦП, яке підтримує саме той алгоритм, який використаний для створення ЕЦП відправником. В іншому разі користувач буде не в змозі обробити та визначити дійсність отриманого електронного документу, або бути впевненим, що його власна кореспонденція/відповідь буде коректною та зрозумілою для адресата. Таким чином можна зробити висновок, що для успішного використання електронного цифрового підпису в Україні, суб'єкти правових відносин у сфері електронного цифрового підпису повинні мати універсальне програмне забезпечення для накладання/перевірки ЕЦП, яке повинно **підтримувати всі без виключення алгоритми криптографічних перетворень**, у тому числі їх специфічні реалізації, пов'язані з невизначеністю у технічних нормативних документах. Визначене Постановою КМУ № 1452 **обмеження** для службовців державної установи **лише одним ключем фактично є обмеженням на використання діючих в Україні криптографічних стандартів** в електронному документообігу. І одночасно, такого обмеження немає при використанні електронної печатки. Вказане обмеження може також суттєво вплинути на можливості у функціонуванні Центрів сертифікації ключів всіх рівнів, у тому числі – Центрального засвідчувального органу, що фактично зараз і відбувається.

«Стаття 8. Центр сертифікації ключів

Центром сертифікації ключів може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у

центральному засвідчувальному органі або засвідчувальному центрі з дотриманням вимог статті 6 цього Закону.

Обслуговування фізичних та юридичних осіб здійснюється центром сертифікації ключів на договірних засадах.

Центр сертифікації ключів має право:

надавати послуги електронного цифрового підпису та обслуговувати сертифікати ключів;

отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи у її уповноваженого представника.

Центр сертифікації ключів зобов'язаний:

забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;

забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;

встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених цим Законом;

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;

перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, заблоковані та поновлені сертифікати ключів;

цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;

вести електронний перелік чинних, скасованих і заблокованих сертифікатів ключів;

забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

надавати консультації з питань, пов'язаних з електронним цифровим підписом.

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

Статтями 4, 8 та 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3] від 5 липня 1994 року встановлено, що порядок доступу до інформації в системі та умови обробки інформації в системі визначаються власником системи, за що останній несе відповідальність згідно чинного законодавства, тобто Центр сертифікації ключів несе відповідальність за захист інформації, який він повинен забезпечувати відповідно до Закону «Про електронний цифровий підпис» та законодавства України.

На жаль ні цим Законом, ні іншими нормативними актами України не визначена процедура реєстрації відкритого ключа центру сертифікації ключів у центральному засвідчувальному органі або засвідчувальному центрі. Така процедура є тільки у Регламенті роботи ЦЗО, який є внутрішнім нормативним документом, та загалом потребує більшої деталізації.

«Стаття 9. Акредитований центр сертифікації ключів

Центр сертифікації ключів, акредитований в установленому порядку, є акредитованим центром сертифікації ключів.

*Акредитований центр сертифікації ключів має право:
надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів;*

отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника.

Акредитований центр сертифікації ключів має виконувати усі зобов'язання та вимоги, встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису.

Порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів, встановлюються Кабінетом Міністрів України.»

Порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів встановлені Постановою КМУ № 903 [11] від 13 липня 2004 р. Цією Постановою визначена добровільність акредитації Центрів сертифікації ключів (далі - центри), процедура акредитації центру, умови надання центром послуг електронного цифрового підпису, вимоги до його персоналу та захисту інформації у центрі. Серед умов акредитації слід відзначити **умову внесення коштів** на спеціальний рахунок, відкритий у банківській установі, у розмірі стократною мінімальною заробітної плати **для забезпечення відшкодування збитків, які можуть бути завдані підписувачам, користувачам або третім особам внаслідок неналежного виконання акредитованим центром своїх зобов'язань, крім центрів, що надають послуги виключно органам державної влади**, що є дискримінаційною умовою по відношенню до інших центрів та незрозуміло з точки зору можливості хоч якогось відшкодування можливих збитків органам державної влади неякісно діючими центрами. У Положенні досить детально описані всі необхідні процедури та умови для забезпечення проходження акредитації та подальшої діяльності центрів, у тому числі визначені права та обов'язки центрів; перелік основних організаційних умов функціонування центрів та документів для акредитації; основні вимоги щодо договорів між центром та підписувачем про надання послуг, у тому числі згоди підписувача на вільну публікацію його сертифікату; вимоги щодо точності часу формування, скасування, блокування та поновлення сертифікатів і встановлений граничний термін блокування сертифікату за запитом підписувача у 2 години; встановлені граничні строки дійсності сертифікатів: для акредитованого центру - 5 років, для підписувача – 2 роки.

«Стаття 10. Засвідчувальний центр

Кабінет Міністрів України за необхідності визначає засвідчувальний центр центрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Інші державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання функцій, зазначених у частині першій цієї статті.

Засвідчувальний центр по відношенню до групи центрів сертифікації ключів, зазначених у частині першій цієї статті, має ті ж функції і повноваження, що й центральний засвідчувальний орган стосовно центрів сертифікації ключів.

Засвідчувальний центр відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Засвідчувальний центр реєструється, засвідчує свій відкритий ключ і акредитується у центральному засвідчувальному органі.

Положення про засвідчувальний центр центрального органу виконавчої влади затверджується Кабінетом Міністрів України.»

Цією статтею фактично визначено, що в Україні може функціонувати тільки трирівнева структура підпорядкованості Центрив сертифікації (ЦЗО-> засвідчувальний центр-> центр сертифікації), причому тільки для державних органів, а для комерційних та інших організацій та підприємств – виключно дворівнева модель. Для недержавних структур це може створити значні проблеми як з точки зору ефективності управління сертифікатами, так і можливостей забезпечити необхідний рівень відповідальності та безпеки в структурі організації захисту інформації. Це стосується не тільки великих корпоративних бізнес-структур, по типу банківської системи країни або розгалужених торгових мереж, але й для менших бізнес структур. Наприклад, для національної банківської системи, яка забезпечує функціонування переважної більшості платежів та фінансових інструментів, необхідна як мінімум чотирирівнева система (НБУ-> комерційні банки -> філії -> відділення та окрема інфраструктура для клієнтів) На відміну від визначених в Україні обмежень, міжнародна практика припускає значно більше рівнів підпорядкованості центрив (більше 10), що необхідно для більшої надійності систем електронного документообігу та переважної більшості сучасних бізнес-застосувань.

«Стаття 11. Центральний засвідчувальний орган

Центральний засвідчувальний орган визначається Кабінетом Міністрів України.

Центральний засвідчувальний орган:

формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів з дотриманням вимог статті 6 цього Закону;

блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрив та центрив сертифікації ключів у випадках, передбачених цим Законом;

веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрив та центрив сертифікації ключів;

веде акредитацію центрив сертифікації ключів, отримує та перевіряє інформацію, необхідну для їх акредитації;

забезпечує цілодобово доступ засвідчувальних центрив та центрив сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрив через загальнодоступні телекомунікаційні канали;

зберігає посилені сертифікати ключів засвідчувальних центрив та центрив сертифікації ключів;

надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов'язаних з використанням електронного цифрового підпису.

Центральний засвідчувальний орган відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Положення про центральний засвідчувальний орган затверджується Кабінетом Міністрів України.»

Положення про Центральний засвідчувальний орган (далі – ЦЗО) затверджено Постановою КМУ № 1451 від 28 жовтня 2004 р. [12]. Цим Положенням закріплені передбачені Законом функції ЦЗО та їх виконання покладено на Міністерство транспорту та зв'язку. Крім визначених Законом функцій Постановою закріплені права ЦЗО щодо забезпечення діяльності постійно діючої комісії з питань акредитації центрив сертифікації ключів (далі – центрив); зберігання сертифікатів ключів та їх реєстрив і документованої інформації, яка підлягає обов'язковій передачі центрами в разі припинення їх діяльності; розглядає заяви і скарги щодо неналежного функціонування центрив; подає пропозиції щодо забезпечення належного функціонування центрив та повідомляє контролюючий орган про обставини, які перешкоджають діяльності самого ЦЗО. Дуже важливо, що ЦЗО надані права залучення будь-яких спеціалістів до розгляду питань застосування ЕЦП, внесення пропозицій щодо удосконалення законодавства у відповідній сфері, проведення переговорів з іноземними

організаціями, що надають послуги електронного цифрового підпису, укладання з ними

відповідних договорів та право участі у підготовці та укладенні міжнародних договорів стосовно взаємного визнання сертифікатів ключів.

Слід зауважити, що оскільки, згідно зі статтею 9 Закону та п.3 вказаного Положення ЦЗО призначений для обслуговування виключно посилених сертифікатів, тобто таких, що видані та визнаються тільки в Україні, хиби чого були вказані раніше у цьому коментарі, це може стати перешкодою для технічної реалізації міжнародних договорів щодо транскордонного надання послуг електронного цифрового підпису та взаємодії з іншими центрами у світі.

«Стаття 12. Контролюючий орган

Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації.

Контролюючий орган перевіряє дотримання вимог цього Закону центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів.

У разі невиконання або неналежного виконання обов'язків та виявлення порушень вимог, встановлених законодавством для центру сертифікації ключів, засвідчувального центру, контролюючий орган дає розпорядження центральному засвідчувальному органу про негайне вжиття заходів, передбачених законом.»

Функції та повноваження Адміністрації Державної служби спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку), як контролюючого органу, визначені Наказом від 24.07.2007 № 143 і фактично не зачіпають діяльність деяких суб'єктів правових відносин у сфері послуг електронного цифрового підпису, визначених ст. 2 Закону, а саме: підписувачів та користувачів, за виключенням державних органів як юридичних осіб, а контроль за останніми обмежується лише погодженням нормативно-правових актів, які визначають порядок застосування ЕЦП державною установою (п. 3.9 Наказу). Тим самим контроль діяльності основних суб'єктів електронного цифрового підпису та електронного документообігу, які фактично і використовують ЕЦП, з боку контролюючого органу не передбачений.

При цьому перевірки державних установ стосовно дотримання вимог законодавства із захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, у тому числі під час застосування ЕЦП, здійснюються Держспецзв'язку в рамках державного контролю за станом криптографічного захисту інформації. Тобто фактично визнається, що застосування (використання) ЕЦП є ліцензійним видом діяльності.

Крім того, незрозуміло, чому у переліку суб'єктів позапланової перевірки, на підставах, пов'язаних із розглядом скарг та звернень, немає засвідчувальних центрів.

Відповідно до п.3.4 Наказу звітна інформація для контролюючого органу фактично повторює звіти Центрів сертифікації ключів для Центрального засвідчувального органу. При цьому відокремлені пункти реєстрації можуть перевірятися лише у акредитованих Центрів сертифікації ключів (п.3.7 Наказу).

Перевірка здійснюється з обов'язковим повідомленням по перевірку за 10 днів до початку перевірки та не може перевищувати 10 робочих днів.

«Стаття 13. Скасування, блокування та поновлення посиленого сертифіката ключа.

Акредитований центр сертифікації ключів негайно скасовує сформований ним посилений сертифікат ключа у разі:

закінчення строку чинності сертифіката ключа;

подання заяви власника ключа або його уповноваженого представника;

припинення діяльності юридичної особи - власника ключа;

смерті фізичної особи - власника ключа або оголошення його померлим за рішенням суду;

*визнання власника ключа недієздатним за рішенням суду;
надання власником ключа недостовірних даних;
компрометації особистого ключа.*

Центральний засвідчувальний орган негайно скасовує посилений сертифікат ключа центру сертифікації ключів, засвідчувального центру у разі:

*припинення діяльності з надання послуг електронного цифрового підпису;
компрометації особистого ключа.*

Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно блокують посилений сертифікат ключа:

*у разі подання заяви власника ключа або його уповноваженого представника;
за рішенням суду, що набрало законної сили;
у разі компрометації особистого ключа.*

Скасування і блокування посиленого сертифіката ключа набирає чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції.

Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника.

Блокований посилений сертифікат ключа поновлюється:

*у разі подання заяви власника ключа або його уповноваженого представника;
за рішенням суду, що набрало законної сили;
у разі встановлення недостовірності даних про компрометацію особистого ключа.»*

Законодавцем не визначено – яким чином центр сертифікації може своєчасно та достовірно отримати інформацію про підписувача, якому він видав сертифікат, у випадках його смерті, або визнання власника ключа недієздатним або припинення діяльності юридичної особи - власника ключа. Також необхідно було б чітко визначити, що припинення чинності (блокування та скасування) сертифікату у випадку компрометації можливе лише за особистим зверненням підписувача.

За текстом цієї статті можливо скасувати або блокувати сертифікат, якщо внести відповідну інформацію до реєстру, проте помилковим є твердження, що такий реєстр має якесь відношення до **чинних** сертифікатів, оскільки технічно реалізується тільки реєстр сертифікатів, які втратили чинність - тимчасово (блоковані) або назавжди (скасовані). Більше того, підписувач може визначити згідно статті 6 Закону, що його сертифікат не підлягає публікуванню, тому надалі виникає колізія в таких випадках і з публікацією факту блокування або скасування такого сертифікату.

«Стаття 14. Припинення діяльності центру сертифікації ключів

Центр сертифікації ключів припиняє свою діяльність відповідно до законодавства.

Про рішення щодо припинення діяльності центр сертифікації ключів повідомляє підписувачів за три місяці, якщо інші строки не визначено законодавством. Підписувачі мають право обирати за власним бажанням будь-який центр сертифікації ключів для подальшого обслуговування, якщо інше не передбачено 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.

Центр сертифікації ключів, 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.

Акредитований центр сертифікації ключів додатково повідомляє про рішення щодо припинення діяльності центральний засвідчувальний орган або відповідний засвідчувальний центр.

Акредитований центр сертифікації ключів протягом доби, визначеної як дата припинення його діяльності, передає посилені сертифікати ключів, відповідні реєстри

посилених сертифікатів ключів та документовану інформацію, яка підлягає обов'язковій передачі, відповідному засвідчувальному центру або центральному засвідчувальному органу.

Порядок передачі акредитованим центром сертифікації ключів посилених сертифікатів ключів, відповідних реєстрів посилених сертифікатів ключів та документованої інформації, яка підлягає обов'язковій передачі, встановлюється Кабінетом Міністрів України.»

«Стаття 15. Відповідальність за порушення законодавства про електронний цифровий підпис

Особи, винні у порушенні законодавства про електронний цифровий підпис, несуть відповідальність згідно з законом.»

«Стаття 16. Розв'язання спорів

Спори, що виникають у сфері надання послуг електронного цифрового підпису, розв'язуються в порядку, встановленому законом.»

«Стаття 17. Визнання іноземних сертифікатів ключів

Іноземні сертифікати ключів, засвідчені відповідно до законодавства тих держав, де вони видані, визнаються в Україні чинними у порядку, встановленому законом.»

«Стаття 18. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2004 року.

2. До приведення законів України та інших нормативно-правових актів у відповідність із цим Законом вони застосовуються у частині, що не суперечить цьому Закону.

3. Пункт 14 статті 9 Закону України "Про ліцензування певних видів господарської діяльності" (Відомості Верховної Ради України, 2000 р., N 36, ст. 299) після слів "надання послуг в галузі криптографічного захисту інформації" доповнити словами "(крім послуг електронного цифрового підпису)".

4. Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом:

підготувати та внести до Верховної Ради України пропозиції про внесення змін до законів України, що впливають із цього Закону;

забезпечити приведення своїх нормативно-правових актів, а також нормативно-правових актів міністерств та інших центральних органів виконавчої влади у відповідність з цим Законом;

визначити центральний засвідчувальний орган;

забезпечити прийняття нормативно-правових актів, передбачених цим Законом.

5. Національному банку України протягом шести місяців з дня набрання чинності цим Законом привести свої нормативно-правові акти у відповідність з цим Законом.

6. Кабінету Міністрів України разом з Національним банком України, іншими органами державної влади протягом шести місяців з дня набрання чинності цим Законом розробити та внести на розгляд Верховної Ради України програму заходів щодо впровадження електронного документа, електронного документообігу та електронного цифрового підпису.»

Законом "Про ЕЦП" затверджена норма, що послуги електронного цифрового підпису не підлягають ліцензуванню, що необхідно для забезпечення вільного використання засобів

застосування електронного чи електронного цифрового підпису в Україні і, особливо, безперешкодного функціонування діючі системи електронних платежів банківської системи України. На наш погляд, ця вимога явно недостатня, оскільки функція надання послуг є лише управлінською функцією, яка відноситься до центрів сертифікації, та не зачіпає громадськості, тобто клієнтського середовища. Більш того, переслідуючи мету наближення українського законодавства до Європейського та міжнародного, побічно була введена норма **обов'язковості ліцензування на використання електронного цифрового підпису** юридичними та фізичними особами, які є **підписувачами та користувачами** електронного підпису **в електронному документообігу**, замість того, щоб полегшити використання ними електронних документів та цифрового підпису. Це впливає з вимог Закону України «Про ліцензування певних видів господарської діяльності» № 1775-III від 1.06.2000 р., та «Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису», затвердженого Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 141 від 20.07.2007 р. В останньому визначено, що обмеження на використання електронного цифрового підпису стосуються **експлуатації** засобів криптографічного захисту конфіденційної інформації, а також **відкритої інформації з використанням електронного цифрового підпису**, що призводить до зарегульованості ринку електронного документообігу та значних ускладнень у використанні електронного цифрового підпису всіма суб'єктами.

Джерела:

1. Закон України «Про електронний цифровий підпис» від 22.05.2003 № **852-IV**;
2. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № **851-IV**;
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № **80/94-ВР**;
4. Закон України «Про звернення громадян» від 2 жовтня 1996 року № 393/96-ВР;
5. ЦИВІЛЬНИЙ КОДЕКС УКРАЇНИ від 16.01.2003 № 435-IV;
6. Указ Президента України «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування» від 7 лютого 2008 року № 109/2008;
7. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства (*Офіційний журнал L 013, 19/01/2000 с.0012-0020*);
8. Директива 2000/31/ЄС Європейського парламенту та Ради від 8 червня 2000 року про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку (*Офіційний журнал L 178, 17.07.2000, с.0001-0016*);
9. Постанова КМУ «Про затвердження типового порядку здійснення електронного документообігу в органах виконавчої влади» від 28 жовтня 2004 р. № 1453;
10. Постанова КМУ «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;
11. Постанова КМУ «Про затвердження Порядку акредитації центру сертифікації ключів» від 13 липня 2004 року № 903;
12. Постанова КМУ «Про затвердження Положення про центральний засвідчувальний орган» від 28 жовтня 2004 р. № 1451;
13. Постанова КМУ «Про затвердження Порядку акредитації центру сертифікації ключів» від 13 липня 2004 р. № 903;
14. Постанова КМУ «Про затвердження Порядку обов'язкової передачі документованої інформації» від 28 жовтня 2004 р. № 1454;
15. Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 р. № 373;
16. Постанова КМУ «Про затвердження Порядку підключення до глобальних мереж передачі даних» від 12 квітня 2002 р. № 522;
17. Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29 березня 2006 р. № 373;
18. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (ДСТСЗІ СБ України). «Про затвердження Правил посиленої сертифікації» від 10 травня 2006 р. № 50;
19. Наказ ДССЗІ України «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту конфіденційної інформації та відкритої інформації з використанням електронного цифрового підпису» від 20.07.2007 №141;
20. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України «Національна система електронного цифрового підпису. Технічні специфікації форматів представлення базових об'єктів» від 11 вересня 2006 р. № 99 /166;

21. Наказ ДССЗЗІ України «Про затвердження Положення про порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису» від 24.07.2007 № 143;
22. Інструкція про порядок вчинення нотаріальних дій нотаріусами України (Наказ Міністерства юстиції України № 20/5 від 03.03.2004);
23. Система електронного документообігу органу виконавчої влади. ТУ У 30.0-33240054-001:2005, Наказ Держкомзв'язку № 52 від 10 квітня 2006 р.;
24. Аналітичний огляд проблем електронного права в Україні (станом на 2005 рік);
25. Наказ Держкомпіприємництва та ДССЗЗІІ України «Про затвердження Ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації і Порядку контролю за додержанням Ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації» від 26.01.2008 № 8/216;
26. Наказ Держкомпіприємництва та ДССЗЗІІІ України «Про затвердження Порядку контролю за додержанням Ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації» від 26.01.2008 № 8/216.

Пропозиції та зауваження прохання надсилати за адресою: amb@itsway.kiev.ua

до науково-практичного Коментаря до Закону України «Про електронний цифровий підпис»

(щодо оцінки вимог Постанови КМУ № 1453 про «Типовий порядок здійснення електронного документообігу в органах виконавчої влади» та визначення терміну «підпис»).

1. Щодо поняття «підпис». Хоча він і не визначений чітко в українському законодавстві, проте визначення його існують, наприклад:

Великий бухгалтерський словник:

Підпис - Реквізит документа, що представляє собою власноручний розпис повноважної посадової особи.

Проте, звичайно, підпис у широкому розумінні визначає персональну специфічну характеристику та притаманну властивість не тільки для посадової особи, але й для будь-якої особи взагалі. Інше визначення:

Подпись - 1. надпись под чем-нибудь; 2. собственноручно написанная фамилия (російською мовою) (<http://opredelenie.info/buhgalterskiy-slovar/>).

В юридичній практиці під підписом часто розуміється **дві обов'язкові частини** – власне «підпис» або «автограф» та розшифровка цього підпису, яка включає: повну або скорочену (прізвище та ініціали) форму ідентифікації особи що підписалася та, **можливо**, повну (скорочену) **назву посади**, яку займає ця особа, якщо накладання/здійснення підпису пов'язане з виконанням цією особою посадових обов'язків.

Існують також декілька еквівалентів поняття «підпис», які застосовуються у звичайній та юридичній практиці:

АВТОГРАФ (гр. autos сам + grapho пишу) - *собственноручная подпись*, надпись или рукопись. (*Литературный словарь. Термины. Определения*), в перекладі з російської – **власноручний підпис, напис або рукопис**.

Тлумачний словник Ожегова характеризує автограф як «собственноручную, обычно памятную надпись или подпись», а підпис – як «собственноручно написанную фамилию». Розглядаючи ці поняття в ключі особистого підпису людини, очевидні схожість і відмінності. За загальною думкою великої різниці між поняттями «автограф» і «підпис» немає, однак поняття «підпису» носить більш формальний характер. У випадку, якщо людина підписує офіційні документи, її підпис є саме «підписом» в буквальному розумінні цього слова. Тут є важливий юридичний «момент»: особистий підпис людини часто є останнім «штрихом» при оформленні операцій, обов'язкова її наявність в різних документах, договорах, на кредитних картах.

парафування (від франц. parafe- скорочений підпис, розчерк) - форма підтвердження згоди з виробленим в результаті переговорів текстом договору шляхом нанесення представниками сторін своїх ініціалів у кінці погодженого тексту, а іноді на кожній його сторінці (*Словник підприємця*).

У юридичній та повсякденній практиці, що склалася, як підпис звичайно використовується монограмна абrevіатура у вигляді поєднання перших букв імені і по батькові і частини прізвища, тобто поєднання ініціалів, або тільки частини прізвища з невеликою модифікацією та додаванням художніх елементів. Згідно словнику Уебстера **параф** – це розчерк, звичайно чинений вслід за підписом. Мета чинення парафу – створити додатковий захист підпису від підробки за рахунок більшої складності розчерку. У ЦК України таке визначено у п.2 ст. 294.: «Фізична особа має право на **транскрибований запис її прізвища та імені** відповідно до своєї національної традиції».

Із вказаними особливостями пов'язана суперечка (Журнал "Домашний адвокат" № 22, 2008. ПАРАФ НЕ ПОДПИСЬ!) про легітимність підпису особи при виконанні правочинів в Росії та Україні, де гідно п.1 ст.19 ЦК РФ «гражданин по общему правилу приобретает и осуществляет права и обязанности под своим именем, включающим фамилию, собственно

им'я, а также отчество» (що тотожно визначенню ст.28 ЦК України). Тобто акт підписання документа означає власноручне написання громадянином свого повного імені (тобто імені, по батькові і прізвища) і лише власноручно написане повне ім'я громадянина може бути визнано його підписом в точному правовому значенні цього слова за законодавством РФ та України. Будь-яке інше або іншим способом виконане позначення може у відповідних випадках бути розцінено лише як аналог підпису, що допускається тільки згідно до п. 2 ст.160 ГК РФ (п.3 ст.207 ЦК України) лише у випадках та в порядку, передбаченому законодавством або угодою сторін і в загальному випадку є формальні підстави вважати документ, на якому проставлений параф або аналог підпису, але відсутній сам власноручний підпис (повний вид підпису), виконаний відповідно до правил правопису мови, не підписаним, що на пряму стосується і практики вчинення нотаріальних дій.

Є також приклади застосування поняття «підпис», які використовуються в комп'ютерних технологіях, за словником іншомовних слів (російською мовою):

signature (Сигнатура, підпись) – Список типов, включений в определение метода, поля, свойства или локальной переменной. Для метода сигнатура включает его имя, количество параметров, их типы, тип возвращаемого результата и соглашения по вызову. Сигнатура для свойства аналогична сигнатуре метода. Сигнатура для поля и локальной переменной – это просто их тип

evidence (Доказательство) – Свойства кода, такие как цифровая подпись, зона, сайт, которые используются политикой безопасности, чтобы предоставить права данному коду

У Цивільному Кодексі України (далі – ЦК) є визначення **застосування власноручного підпису** у ст. 207 та частково у ст.1248 (засвідчення заповіту нотаріусом). В інших статтях визначається необхідність письмової форми правочину та підписання документів (без визначення форми підпису) і фактично є посиланням саме на ст.207 ЦК.

Стаття 207 ЦК України вводить ряд норм щодо письмової форми вчинення правочину, зокрема визначення форми підпису та аналогів власноручного підпису вказане у п.3:

«3. Використання при вчиненні правочинів факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, електронно-числового підпису або **іншого аналога власноручного підпису** допускається у випадках, встановлених законом, іншими актами цивільного законодавства, або за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів.»

2. На підтвердження тези у Коментарі про те що «**вимога щодо обов'язковості фізичній особі або юридичній особі мати посиленій сертифікат ключа**», яка впливає з Постанови КМУ № 1453 є неправомірною, наведемо такі міркування та норми законодавства:

2.1. Вказане обмеження щодо обов'язковості мати надійні засоби ЕЦП **фактично відмінняє норму**, визначену останнім абзацом ст.3 Закону, **про неможливість невизнання електронного підпису** виключно через його електронну форму чи тому, що він не ґрунтується на посиленому сертифікаті ключа підписувача (та користувача), по крайній мірі для державних органів та їх службовців.

Таке обмеження є технічним обмеженням, яке включає такі обов'язкові елементи:

- використання виключно криптографічних стандартів, які діють в Україні;
- використання засобів ЕЦП, які мають сертифікат відповідності або позитивний експертний висновок регулюючого органу (ДССЗЗІ України);
- використання виключно сертифікатів, які видані акредитованими центрами сертифікації ключів.

У Європейській Директиві ЄС 1999/93/ЄС також є аналогічна норма (п.2 ст.5 Директиви), але вона дає можливість більш вільного застосування електронного підпису, тому що електронний підпис не може бути відхилений з таких причин:

«2. Держави-члени забезпечують, неможливість позбавлення електронного підпису юридичної сили і прийнятності в якості доказу у судочинстві лише на тій підставі, що він:

- виконаний у електронній формі, чи
- не заснований на чинному сертифікаті, чи
- не заснований на чинному сертифікаті, виданому акредитованим постачальником послуг по сертифікації, чи
- не створений за допомогою безпечного механізму створення підпису.»

Широке застосування електронних підписів можливе лише в умовах мінімізації обмежень та дотримання єдиних технічних стандартів у цій сфері, а також лібералізації законодавства щодо застосування електронного документообігу у цивільних та громадських відносинах.

2.2. Використання будь-яких аналогів власноручного підпису є правомірним при здійсненні правочинів в Україні згідно до п.1 Статті 204. Презумпція правомірності правочину: «1. Правочин є правомірним, якщо його недійсність прямо не встановлена законом або якщо він не визнаний судом недійсним», а використання ЕЦП, що не ґрунтується на надійних засобах ЕПЦ або на посиленому сертифікаті, не тільки **не заперечується** Законом «Про електронний цифровий підпис» або будь-яким іншим, а і **напрямую дозволено** ст.5 Закону про ЕЦП.

2.3. Договірна форма відносин між підписувачами та центрами сертифікації ключів, передбачена Законом «Про ЕЦП» і яка на практиці фактично регулює взаємовідносини між ними у відповідності до ст.5 вказаного Закону, **повністю задовольняє вимогу п.3 Ст.207 ЦК** щодо дозволу вчиненні правочинів «за письмовою згодою сторін, у якій мають міститися зразки відповідного аналога їхніх власноручних підписів» і **не передбачає будь-яких додаткових обмежень**. Центри сертифікації ключів, які зареєстровані в Україні або в інших державах згідно законодавства, виконують функції **документального засвідчення** чинності і належності відкритого ключа підписувача (ст.1 Закону «Про ЕЦП») і **діють завжди на договірних засадах**, і виступають гарантами для усіх користувачів ЕЦП, у тому числі – державних органів, ідентифікації підписувача та цілісності підписаного ним документу, якщо перевірка ЕЦП завершилася успішно (перевірка ЕЦП виконана без помилок).

2.4. Питання використання ЕЦП стосується не тільки спілкування з органами державної влади юридичних та фізичних осіб, але й забезпечення прав людини у відповідності з законодавством, у тому числі міжнародним, яке ратифіковане Україною та міжнародними угодами України. В цій частині держава Україна відіграє найсуттєвішу роль у забезпеченні прав та свобод громадян у цивільних відносинах. Вказані права ґрунтуються на Конституції України, Законах та інших законодавчих актах.

За цими законами Україна та її державні органи та організації зобов'язані максимально сприяти впровадженню міжнародних норм та стандартів у практиці взаємовідносин між державою, особами різних форм власності та громадянами, а також імплементації міжнародних та європейських умов визнання правочинів у практичну діяльність в Україні в галузях електронного документообігу та електронної комерції.

Конституцією України визначено (ст.9), що «**чинні міжнародні договори**, згода на обов'язковість яких надана Верховною Радою України, є **частиною законодавства України**». Звернемося до змісту міжнародних договорів, якими визначаються загальні принципи, до яких прагне Україна:

«**Декларація прав людини**» ООН, членом якої Україна є з 24 жовтня 1945 року

Стаття 22. Кожна людина, як член суспільства, має право на соціальне забезпечення і на здійснення необхідних для підтримання її гідності і для вільного розвитку її особи прав у економічній, соціальній і культурній галузях за допомогою національних зусиль і міжнародного співробітництва та відповідно до структури і ресурсів кожної держави.

Стаття 28. Кожна людина має право на соціальний і міжнародний порядок, при якому права і свободи, викладені в цій Декларації, можуть бути повністю здійснені.

Угода про формування Єдиного економічного простору (Дата набуття чинності: 20.05.2004 р.):

В Концепції, яка затверджена цією Угодою вказано, що (розділ I. Цілі та завдання): Держави-учасниці прагнуть сприяти:

«розвитку торгівлі та інвестицій між державами-учасницями, що забезпечуватиме сталий розвиток економік держав-учасниць на основі загально визнаних норм і принципів міжнародного права;

створенню можливостей для розвитку підприємницької діяльності шляхом **встановлення гармонізованих систем регулювання та інтегрування інфраструктурного комплексу;**»

а у розділі II (**Основні принципи**), вказано, що: «Принцип забезпечення вільного руху капіталу передбачає поетапне зняття всіх обмежень на рух капіталу з держав-учасниць у рамках ЄЕП та проведення узгодженої політики в галузі розвитку ринку капіталів за умови забезпечення макроекономічної стабільності» та

«Неучасть або часткова участь будь-якої держави-учасниці в окремих напрямках розвитку інтеграції чи окремих інтеграційних заходах не повинна бути перешкодою для інших держав-учасниць у здійсненні зазначених напрямів розвитку інтеграції чи окремих інтеграційних заходів».

Розділ IV (**Взаємодія при проведенні переговорів щодо приєднання до СОТ**) визначає, що: «Формування і діяльність ЄЕП здійснюються з урахуванням норм і правил СОТ».

Законом України «**Про ратифікацію Угоди про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами**» (№ 237-94-ВР від 10.11.1994) визначені основні засади, які стосуються саме використання цифрових підписів для електронного документообігу та здійснення ділової діяльності:

За Преамбулою:

беручи до уваги бажання Сторін встановити тісні стосунки, побудовані на існуючих історичних зв'язках між ними

будучи переконаними у надзвичайній важливості верховенства закону та поваги до прав людини, особливо прав меншин, створення багатопартійної системи з вільними і демократичними виборами та економічної лібералізації з метою створення ринкової економіки

беручи до уваги корисність Угоди у справі поступового зближення між Україною і більш широкою сферою співробітництва в Європі та сусідніх регіонах та поступову інтеграцію України у відкриту міжнародну систему торгівлі

будучи переконаними, що прогрес у напрямку ринкової економіки буде прискорений завдяки співробітництву між Сторонами у формах, встановлених у цій Угоді

Розділ VI. **Конкуренція, захист інтелектуальної, промислової і комерційної власності та співробітництво в галузі законодавства** Стаття 49. п.2.4:

«Стосовно державних монополій комерційного характеру Сторони заявляють про свою готовність, починаючи з четвертого року від дати набуття чинності цією Угодою (авт. -з 1998 року), забезпечити недопущення дискримінації громадян Сторін щодо умов, за яких товари закупаються або продаються».

Стаття 51:

«...галузях: закон про митницю, закон про компанії, закон про банківську справу, бухгалтерський облік компаній і податки, інтелектуальна власність, охорона праці, фінансові послуги, правила конкуренції, державні закупки, охорона здоров'я та життя людей, тварин і рослин, навколишнє середовище, захист прав споживачів, непряме оподаткування, **технічні правила і стандарти**, закони та інструкції стосовно ядерної енергії, транспорт»

Розділ VII. Економічне співробітництво Стаття 52 п.3:

«...співробітництво зосереджується, зокрема, на промисловій кооперації, заохоченні та захисті інвестицій, державних поставках, зближенні політики стандартизації в гірничовидобувній та сировинній галузях, науці та техніці, освіті та навчанні, АПК і сільському господарстві, енергетиці, цивільній ядерній галузі, галузі охорони навколишнього середовища, транспорті, космосі, телекомунікаціях, фінансових послугах, "відмиванні" грошей, валютній політиці, регіональному розвитку, соціальній кооперації, туризмі, малому та середньому підприємстві, засобах інформації та зв'язку, захисту прав споживачів, митній справі, співробітництві в галузі статистики, економіці та боротьбі з наркотичним бізнесом»

Стаття 56 Співробітництво в галузі оцінки стандартів та оцінки відповідності

«Співробітництво між Сторонами сприяє створенню відповідності з міжнародно узгодженими критеріями, принципами та орієнтирами, у тому числі:

сприяти застосуванню технічних правил Співтовариства та європейських стандартів і процедур оцінки відповідності»

Стаття 74 Інформація та зв'язок.

«Сторони підтримують розвиток сучасних методів обробки інформації, в тому числі засобів інформації, та сприяють ефективному взаємному обміну інформацією. Першочергова увага приділяється програмам, які мають за мету ознайомлення широкої громадськості з основною інформацією про Співтовариство і Україну, включаючи, коли це можливо, взаємний доступ до баз даних на основі повної поваги до прав на інтелектуальну власність»

Крім того, **Директивою ЄС 1999/93/ЄС щодо застосування цифрових підписів в межах Співтовариства**, визначено, що:

(4) Електронний зв'язок та комерція обумовлюють використання "електронних підписів" та суміжних послуг, що роблять можливим засвідчення достовірності інформації; суперечливі норми щодо правового визнання електронних підписів та акредитації постачальників послуг по сертифікації в державах-членах можуть створити значну перешкоду для використання електронного зв'язку та електронної комерції; з іншого боку, чітка система умов, що застосовуються до електронних підписів в межах Співтовариства, зміцнить впевненість та загальне визнання нових технологій; законодавство держав-членів не повинно перешкоджати вільному переміщенню товарів та послуг на внутрішньому ринку;

(5) Має забезпечуватись функціональна сумісність продукції для електронного підпису; відповідно до статті 14 Договору (про заснування Європейської спільноти), внутрішній ринок включає в себе територію без внутрішніх кордонів, в межах якої забезпечується вільне переміщення товарів;

(9) Електронні підписи будуть використовуватись у великій кількості випадків, що мають своїм наслідком виникнення широкого спектра нових послуг та продукції, яка відноситься до чи використовує електронні підписи; визначення такої продукції та послуг не повинно зводитись лише до видачі та організації сертифікатів, але має також включати в себе будь-які інші послуги та продукцію, що використовує чи є допоміжною до електронних підписів,

(17) ... положення щодо юридичної сили електронних підписів мають без перешкод застосовуватись до вимог щодо форми укладення контрактів чи норм, які визначають місце укладення контракту, передбачених внутрішнім законодавством;

(19) Електронні підписи будуть використовуватись в державному секторі виконавчими органами влади окремих держав та Співтовариства в цілому та у зв'язках між такими виконавчими органами та громадянами й економічними операторами, наприклад, при державних закупівлях, оподаткуванні, системі соціальної безпеки, системі охорони здоров'я та системі правосуддя;

(20) Узгоджені критерії юридичної сили електронних підписів будуть забезпечувати послідовну правову систему в Співтоваристві; внутрішнє законодавство передбачає різні вимоги щодо юридичної чинності підписів, написаних власноручно; враховуючи, що сертифікати можуть використовуватись для підтвердження ідентичності особи, яка поставила електронний підпис; вдосконалені електронні підписи, засновані на чинних сертифікатах, мають на меті підвищення рівня безпеки; вдосконалені електронні підписи, засновані на чинних сертифікатах, та які створені за допомогою безпечних засобів створення підпису, можуть вважатись з правової точки зору еквівалентними підписам, написаним власноручно у випадку, якщо виконані вимоги до підписів, написаних власноручно;

(21) З тим, щоб сприяти загальному прийняттю методів електронного засвідчення, необхідно передбачити використання електронних підписів в якості доказів в судочинстві в усіх державах-членах; юридичне визнання електронних підписів має засновуватись на об'єктивних критеріях та не бути пов'язане із отриманням дозволу відповідним постачальником послуг по сертифікації;

Стаття 3 Доступ до ринку

7. Держави-члени можуть накласти на використання електронних підписів у державному секторі додаткові вимоги. Такі вимоги є об'єктивними, прозорими, пропорційними і недискримінаційними і стосуються виключно специфічних характеристик при відповідному застосуванні. Такі вимоги можуть не створювати перешкод для надання транскордонних послуг громадянам.

Стаття 5 Юридична сила електронних підписів

1. Держави-члени забезпечують, щоб удосконалені електронні підписи, засновані на чинних сертифікатах і створені за допомогою безпечних механізмів створення підпису:

а) задовольняли юридичним вимогам до підписів стосовно даних, поданих у електронній формі, так само, як підпис, написаний власноручно (**handwritten**), задовольняє вимоги стосовно даних, нанесених на папір; і

б) були прийнятними в якості доказів у судочинстві.

Протокол про вступ України до Світової організації торгівлі 5 лютого 2008 року (Женева), визначив напрямки та принципи взаємодії з СОН за Генеральною угодою з тарифів і торгівлі (ГАТТ 1947), яка передбачає:

Стаття XXXVIII Спільні дії:

2. Зокрема, СТОРОНИ повинні

е) співпрацювати у пошуку можливих методів розширення торгівлі задля економічного розвитку шляхом міжнародної гармонізації та коригування національної політики та нормативних актів, через технічні та комерційні стандарти, що впливають на виробництво, транспортування та реалізацію, а також шляхом розвитку експорту за допомогою створення засобів для збільшення потоку торговельної інформації та проведення ринкових досліджень;

а також:

Генеральна угода про торгівлю послугами (ГАТС)

Стаття VI Внутрішнє регулювання

4. Для забезпечення того, щоб **заходи, які стосуються кваліфікаційних вимог і процедур, технічних стандартів та вимог ліцензування, не створювали невинуватених бар'єрів** у торгівлі послугами, Рада з торгівлі послугами повинна через відповідні органи, які вона може створити, встановити будь-які необхідні правила. Ці правила повинні бути спрямовані на забезпечення того, щоб вищезазначені вимоги, *inter alia*:

(а) базувалися на об'єктивних і прозорих критеріях, таких як компетентність і здатність надавати послугу;

(б) **не були більш обтяжливими, ніж необхідно для забезпечення якості послуги;**

(с) у випадку процедур ліцензування, - самі не були обмеженням на поставку послуги.

5. (а) У секторах, у яких Член взяв на себе конкретні зобов'язання, в очікуванні введення в дію дисципліни, встановленої у цих секторах згідно з параграфом 4, **Член не повинен застосовувати вимоги щодо ліцензування та кваліфікації і технічні стандарти, що зводять нанівець або ушкоджують конкретні зобов'язання** у спосіб,

(і) який не відповідає критеріям, визначеним у підпараграфі 4(а), (б) або (с);

(іі) якого не можна було очікувати з боку Члена, коли були прийняті конкретні зобов'язання в цих секторах;

(б) **при визначенні того, чи відповідають дії Члена зобов'язанням згідно з параграфом 5(а), слід враховувати міжнародні стандарти відповідних міжнародних організацій».**

Стаття VII **Визнання**

1. **З метою виконання, повністю або частково, своїх стандартів чи критеріїв щодо дозволів, ліцензування або сертифікації постачальників послуг, а також відповідно до умов параграфа 3, Член може визнати отримані знання або набутий досвід, виконані вимоги, або ліцензії чи сертифікати, видані в певній країні.** Таке визнання кваліфікації, яке може бути досягнуте шляхом гармонізації або в інший спосіб, може базуватися на угоді чи домовленості з країною, про яку йде мова, або може бути отримано автономно.

3. **Член не повинен надавати визнання кваліфікації таким чином, щоб воно стало засобом дискримінації між країнами у застосуванні його стандартів чи критеріїв дозволу, ліцензування чи сертифікації постачальників послуг або прихованим обмеженням у торгівлі послугами.**

4. Кожний Член повинен:

Там, де можливо, визнання кваліфікації, ліцензій тощо повинно базуватися на багатосторонньо погоджених критеріях. У відповідних випадках **Члени повинні працювати разом з відповідними міждержавними та недержавними організаціями у питаннях розробки та прийняття загальних міжнародних стандартів і критеріїв визнання загальних міжнародних стандартів практики відповідної торгівлі послугами та професійної практики.**

Стаття XVIII **Додаткові зобов'язання**

Члени можуть зробити предметом переговорів зобов'язання щодо заходів, які впливають на торгівлю послугами і які виходять за рамки положень Статей XVI або XVII, в тому числі і ті, що стосуються питань кваліфікації, стандартів та ліцензування. Такі зобов'язання повинні бути внесені до Розкладу Члена.

Додаток щодо телекомунікацій

4. Прозорість

При застосуванні Статті III Угоди **кожний Член повинен забезпечити загальнодоступність відповідної інформації про умови доступу та використання телекомунікаційних мереж та послуг загального користування, включаючи: тарифи та інші умови надання послуг; специфікації технічних інтерфейсів з такими мережами та послугами; інформацію про органи, що відповідають за підготовку та прийняття стандартів, що стосуються такого доступу і використання; умови, стосовно під'єднання терміналів або**

іншого обладнання, а також вимоги щодо повідомлення, реєстрації або ліцензування, якщо вони необхідні.

7. Відношення до міжнародних організацій та угод

(а) **Члени визнають важливість міжнародних стандартів для глобальної сумісності і сполучення телекомунікаційних мереж та послуг і беруть на себе зобов'язання сприяти розповсюдженню таких стандартів через діяльність відповідних міжнародних органів, в тому числі Міжнародного союзу електрозв'язку та Міжнародної організація зі стандартизації;**

(б) Члени визнають роль, яку відіграють міжурядові і недержавні організації й угоди у забезпеченні ефективності функціонування національного та глобального телекомунікаційного обслуговування, особливо Міжнародний союз електрозв'язку. Члени повинні добиватися досягнення відповідних домовленостей там, де необхідно, для консультації з такими організаціями з питань, що виникають при впровадженні цього Додатка.

Договір про заснування Європейської спільноти (консолідована версія станом на 1 січня 2005 року) передбачається, що (ст.44):

«(с) скасовувати ті адміністративні процедури та звичаї, що впливають із національного законодавства чи угод між державами-членами, укладених раніше, та що перешкоджають свободі підприємницької діяльності;»

Також статтею 155 визначено, що для досягнення мети «дати громадянам Союзу, учасникам економічної діяльності, регіональним та місцевим спільнотам змогу **повною мірою скористатися перевагами створюваного простору без внутрішніх кордонів**, Спільнота сприяє створенню та розвитку транс'європейських мереж транспортної, телекомунікаційної та енергетичної інфраструктури», для чого **Європейська Спільнота:**

«- виконує будь-які заходи, що можуть виявитися потрібними, щоб забезпечити взаємодію мереж, зокрема у сфері технічного стандартування»

3. Також вважаємо за потрібне звернути увагу на ще декілька цікавих моментів, пов'язаних з практикою використання електронного та електронного цифрового підпису.

3.1. Розповсюджена **практика** в банківській системі України (системах типу «Клієнт-банк» тощо) **передачі ключа ЕЦП та підписання документів по довіреності** (вчинення правочинів від імені) іншою особою **не відповідає вимогам ст.207 ЦК**, оскільки таке дозволяється тільки для осіб обмеженої дієздатності (хворобою або фізичною вадою), при цьому сам документ (правочин) повинен підписуватись у **ПРИСУТНОСТІ** цієї особи, що практично не виконується ніколи. Теж саме відноситься до передачі повноважень щодо отримання ключів ЕЦП в ЦСК іншою особою по довіреності.

3.2. Визначення «підпису», яке впливає з аналізу законодавства та практики, вказує на те, що для вчинення правочинів юридичними особами та накладання ЕЦП мало б регламентувати застосування таких даних, як **«посада, яку займає особа, що накладає підпис», у сертифікаті**, який видає та засвідчує Центр сертифікації ключів, однак ані Законом, ані іншим нормативним документом України це **не передбачено**. Крім того у **технічних специфікаціях**, які є міжнародними стандартами (X.509) або нормативним документом України (для національної системи електронного цифрового підпису), місце таких даних у сертифікаті не передбачене і можуть включатися виключно як додаткові дані (**необов'язкові**). Тому може виникнути колізія у визнанні дійсності ЕЦП в юридичній практиці всередині України та при взаємному визнанні виконаних правочинів у міждержавних відносинах України та в ділових відносинах суб'єктів України та інших держав.

до науково-практичного Коментаря до Закону України «Про електронний цифровий підпис»

(щодо оцінки наслідків ігнорування звернень громадян в електронному вигляді з електронним цифровим підписом до державних органів України)

Розглянемо вимоги законодавства України щодо роботи державних органів та органів місцевого самоврядування із зверненнями громадян: Закону України «Про звернення громадян» № 393/96-ВР від 2 жовтня 1996 року та Указу Президента України «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування» № 109/2008 від 7 лютого 2008 року, а також норми інших законодавчих актів, пов'язаних з цими функціями держави.

Норми, встановлені Законом України «Про звернення громадян»:

Ст.1 Звернення громадян

Громадяни України мають право звернутися до органів державної влади, місцевого самоврядування, об'єднань громадян, підприємств, установ, організацій незалежно від форм власності, засобів масової інформації, посадових осіб відповідно до їх функціональних обов'язків із зауваженнями, скаргами та пропозиціями, що стосуються їх статутної діяльності, заявою або клопотанням щодо реалізації своїх соціально-економічних, політичних та особистих прав і законних інтересів та скаргою про їх порушення.

Тут перелічені можливі типи звернень громадян до органів державної влади, місцевого самоврядування та будь-яких підприємств та організацій, а зміст таких звернень уточнений у ст.2 **Основні терміни** Закону «Про звернення громадян»: пропозиції (зауваження), заяви (клопотання) та скарги:

«Пропозиція (зауваження) - звернення громадян, де висловлюються порада, рекомендація щодо діяльності органів державної влади і місцевого самоврядування, депутатів усіх рівнів, посадових осіб, а також висловлюються думки щодо врегулювання суспільних відносин та умов життя громадян, вдосконалення правової основи державного і громадського життя, соціально-культурної та інших сфер діяльності держави і суспільства.

Заява (клопотання) - звернення громадян із проханням про сприяння реалізації закріплених Конституцією та чинним законодавством їх прав та інтересів або повідомлення про порушення чинного законодавства чи недоліки в діяльності підприємств, установ, організацій незалежно від форм власності, народних депутатів України, депутатів місцевих рад, посадових осіб, а також висловлення думки щодо поліпшення їх діяльності. Клопотання - письмове звернення з проханням про визнання за особою відповідного статусу, прав чи свобод тощо.

Скарга - звернення з вимогою про поновлення прав і захист законних інтересів громадян, порушених діями (бездіяльністю), рішеннями державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян, посадових осіб.»

Особливу увагу звертаємо на норму цього Закону щодо прав осіб, які не є громадянами України, яка сформульована у частині 3 статті 1 Закону «Про звернення громадян»:

«Особи, які не є громадянами України і законно знаходяться на її території, мають таке ж право на подання звернення, як і громадяни України, якщо інше не передбачено міжнародними договорами.»

Ця норма встановлює, що іноземні громадяни мають право звертатися до державних та місцевих органів, підприємств та організацій із зверненнями, у тому числі в електронній

формі, та за власним підписом, у тому числі – електронним цифровим, цифровим тощо. Законом «Про електронний цифровий підпис» визначено, що електронні документи не можуть відхилятися на підставі того, що електронний підпис має електронну форму або не ґрунтується на посиленому сертифікаті (ст. 3 Закону «Про ЕЦП»), якщо всі інші реквізити на документі вірні та відповідають вимогам стт. 5 та 7 Закону «Про звернення громадян».

Для створення підпису на зверненні громадяни можуть використовувати засоби цифрового (електронного цифрового) підпису та сертифікати ключів, які засвідчені (надані) їм в країні громадянства, та які визнані там еквівалентними власноручному підпису, як мінімум – засоби кваліфікованого цифрового підпису за законодавством ЄС (Директива 1999/93/ЄС). Цей вид електронного підпису є особливо важливим для державних органів, оскільки саме такий вид цифрового підпису передбачений міжнародними стандартами як один з основних реквізитів електронних паспортів громадян, який вже є обов'язковими у США, Європі, Австралії тощо і плануються для застосування у більшості держав світу. **І цифровий підпис, еквівалентний власноручному, може створюватись з використанням саме офіційного міжнародно визнаного паспорту особи.**

Крім того, деякі держави (наприклад – США) визнають у якості власноручних електронні підписи, створені за технологіями оцифрування та фіксації напису рукою, яку наносить людина на електронний планшет як власноручний підпис, проте такий вид підпису поки що є унікальним і немає широкого вжитку.

Із сказаного випливає, що відсутність необхідного Закону, передбаченого ст.17 Закону «Про ЕЦП» щодо визнання іноземних сертифікатів ключів засвідчених відповідно до законодавства тих держав, де вони видані, взагалі ставить під питання можливості України, як європейської держави, хоч якось забезпечити взаємовідносини з іншими державами та їх громадянами на сучасному рівні комунікацій та електронного документообігу.

Обмеження на використання електронного цифрового підпису та виключно посилених сертифікатів особами (громадянами України та іноземцями), які звертаються до державних та місцевих органів, можуть викликати безліч скарг, оскільки таке передбачене ст.4 Закону «Про звернення громадян»:

«До рішень, дій (бездіяльності), які можуть бути оскаржені, належать такі у сфері управлінської діяльності, внаслідок яких:

- порушено права і законні інтереси чи свободи громадянина (групи громадян);*
- створено перешкоди для здійснення громадянином його прав і законних інтересів чи свобод;*
- незаконно покладено на громадянина які-небудь обов'язки або його незаконно притягнуто до відповідальності.»*

Вимоги до звернень громадян та можливі підстави повернення звернення викладені у стт. 5 та 7 Закону «Про звернення громадян», а мова звернення та відповіді на нього можуть бути будь-яка, у тому числі – українська (ст.6). Визначення звернень, які не підлягають розгляду та вирішенню надане у ст. 8 Закону «Про звернення громадян».

Обов'язковими реквізитами звернень (ст.5) у письмовому вигляді є:

- *прізвище, ім'я, по батькові;*
- *місце проживання громадянина;*
- *суть порушеного питання, зауваження, пропозиції, заяви чи скарги;*
- *підпис заявника (заявників);*
- *дата складання звернення.*

Передача звернення можлива як самою особою, так і довіреною особою. тобто за довіреністю, оформленою відповідно до чинного законодавства.

Якщо будь-який реквізит відсутній, звернення повертається заявникові «з відповідними роз'ясненнями не пізніше як через десять днів від дня його надходження, крім випадків, передбачених частиною першою статті 7 цього Закону» (частина 5 ст. 5 Закону «Про звернення громадян»), а саме:

«Звернення, оформлені належним чином і подані у встановленому порядку, підлягають обов'язковому прийняттю та розгляду.»

До речі, тут, можливо, сталася помилка у тексті Закону «Про звернення громадян»: вказана частина 1 замість 2-ї частини, оскільки частина перша ст.7 стосується обов'язковості розгляду звернення, а от частина 2 ст. 7 стосується іншого терміну (5-тиденного) повернення звернення особі, яка його подала. За частиною 2 ст.7 Закону:

«Якщо питання, порушені в одержаному органом державної влади... не входять до їх повноважень, воно в термін не більше п'яти днів пересилається ними за належністю відповідному органу чи посадовій особі, про що повідомляється громадянину, який подав звернення. У разі якщо звернення не містить даних, необхідних для прийняття обгрунтованого рішення органом чи посадовою особою, воно в той же термін повертається громадянину з відповідними роз'ясненнями.»

Частини 1 та 2 **статті 8** цього ж Закону стосується випадку, коли звернення не підлягає розгляду та вирішенню, про що власне і йдеться у процитованій частині 5 ст.5 Закону «Про звернення громадян» - анонімні, від недієздатних осіб та за якими вже прийнято рішення по суті:

- якщо письмове звернення без зазначення місця проживання, не підписане автором (авторами), або з якого неможливо встановити авторство – анонімні;

- повторні звернення одним і тим же органом від одного і того ж громадянина з одного і того ж питання, якщо перше вирішено по суті;

а також ті звернення, терміни розгляду яких передбачено статтею 17 цього Закону, та звернення осіб, визнаних судом недієздатними.

Тут необхідно зауважити, що авторство електронного документу встановлюється за електронним цифровим підписом на основі сертифікату підписувача, який є обов'язковим елементом при перевірці самого підпису. Власне наявність сертифіката свідчить про те що підпису можна довіряти, оскільки сертифікат за Законом «Про ЕЦП» формується центром сертифікації ключів після перевірки даних підписувача (ст. 8), як і акредитованим центром сертифікації. Сертифікати центру сертифікації та акредитованого центру формуються центральним засвідчувальним органом за практично однаковими правилами, включаючи однакові договірні умови обслуговування сертифікатів таких центрів з боку центрального засвідчувального органу України. Тому підписувач, який має сертифікат від центру сертифікації ключів, анонімним бути не може.

Обов'язки органів, які розглядають звернення, визначені у статтях 10, 14, 15, 16, 19 та 20 Закону «Про звернення громадян», згідно яких можна сформулювати загальні обов'язки щодо розгляду звернень за таким переліком:

посадові особи зобов'язані розглянути пропозиції (зауваження) чи скарги об'єктивно, всебічно і вчасно розглядати їх, перевіряти викладені в них факти, приймати рішення відповідно до чинного законодавства і забезпечувати їх виконання;

звернення громадян, які мають встановлені законодавством пільги, розглядаються у першочерговому порядку;

письмово повідомляти громадянина про результати перевірки заяви чи скарги і суть прийнятого рішення, причому тим органом, який отримав ці заяви і до компетенції якого входить вирішення порушених у заявах (клопотаннях) питань, за підписом керівника або особи, яка виконує його обов'язки;

не допускати безпідставної передачі розгляду заяв чи скарг іншим органам; рішення про відмову в задоволенні вимог, викладених у заяві (клопотанні), доводиться до відома громадянина в письмовій формі з посиланням на Закон і викладенням мотивів відмови, а також із роз'ясненням порядку оскарження прийнятого рішення;

у разі прийняття рішення про обмеження доступу громадянина до відповідної інформації при розгляді заяви чи скарги скласти про це мотивовану постанову;

звернення розглядаються і вирішуються у термін не більше одного місяця від дня їх надходження, а ті, які не потребують додаткового вивчення, - невідкладно, але не пізніше п'ятнадцяти днів від дня їх отримання;

якщо в місячний термін вирішити порушені у зверненні питання неможливо, керівник відповідного органу, установи, або його заступник встановлюють необхідний термін для його розгляду, про що повідомляється особі, яка подала звернення. При цьому загальний термін вирішення питань, порушених у зверненні, не може перевищувати сорока п'яти днів. На обгрунтовану письмову вимогу громадянина термін розгляду може бути скорочено від встановленого цією статтею терміну;

на прохання громадянина запрошувати його на засідання відповідного органу, що розглядає його заяву чи скаргу;

скасовувати або змінювати оскаржувані рішення у випадках, передбачених законодавством України, якщо вони не відповідають закону або іншим нормативним актам, невідкладно вживати заходів до припинення неправомірних дій, виявляти, усувати причини та умови, які сприяли порушенням;

забезпечувати поновлення порушених прав, реальне виконання прийнятих у зв'язку з заявою чи скаргою рішень;

вживати заходів щодо відшкодування у встановленому законом порядку матеріальних збитків, якщо їх було завдано громадянину в результаті ущемлення його прав чи законних інтересів, вирішувати питання про відповідальність осіб, з вини яких було допущено порушення, а також на прохання громадянина не пізніше як у місячний термін довести прийняте рішення до відома органу місцевого самоврядування, трудового колективу чи об'єднання громадян за місцем проживання громадянина;

особисто організовувати та перевіряти стан розгляду заяв чи скарг громадян, вживати заходів до усунення причин, що їх породжують, систематично аналізувати та інформувати населення про хід цієї роботи.

Окремо у ст. 10 Закону «Про звернення громадян» вписана заборона розголошення ряду відомостей, що містяться у зверненнях:

«Не допускається розголошення одержаних із звернень відомостей про особисте життя громадян без їх згоди чи відомостей, що становлять державну або іншу таємницю, яка охороняється законом, та іншої інформації, якщо це ущемлює права і законні інтереси громадян. Не допускається з'ясування даних про особу громадянина, які не стосуються звернення. На прохання громадянина, висловлене в усній формі або зазначене в тексті звернення, не підлягає розголошенню його прізвище, місце проживання та роботи.»

Ця заборона не поширюється на випадки повідомлення інформації, що міститься у зверненні, особам, які мають відношення до вирішення справи.»

А статтею 21 Закону «Про звернення громадян» визначена безоплатність розгляду звернень:

«Органи державної влади, місцевого самоврядування, підприємства, установи, організації незалежно від форм власності, об'єднання громадян, посадові особи розглядають звернення громадян, не стягуючи плати»

це суттєво у зв'язку з заборонаю накладання додаткових обов'язків на громадян за ст. 4 Закону «Про звернення громадян» та тим фактом, що державні органи та органи місцевого самоврядування підприємства, установи та організації державної форми власності повинні використовувати тільки **посилені сертифікати, випущені лише одним акредитованим центром сертифікації ключів**, а отримання громадянами засобів накладання електронного цифрового підпису та посилених сертифікатів, які діють на протязі одного року, **передбачає оплату цих послуг** в акредитованих центрах сертифікації ключів.

Стаття 12. Сфера застосування цього Закону

Дія цього Закону не поширюється на порядок розгляду заяв і скарг громадян, встановлений кримінально-процесуальним, цивільно-процесуальним, трудовим законодавством і законодавством про захист економічної конкуренції.

Ця стаття 12 Закону «Про звернення громадян» визначає, що цей закон не застосовується у судовому розгляді справ, пов'язаними з кримінальними, цивільними правочинами, спорами за трудовими та конкурентними відносинами. Однак таке обмеження дії Закону «Про звернення громадян» не виключає можливості звернення громадян до суду відповідно до ст. 16 цього Закону.

Права громадянина при розгляді заяви чи скарги визначені ст. 18 Закону «Про звернення громадян»:

«особисто викласти аргументи особі, що перевіряла заяву чи скаргу, та брати участь у перевірці поданої скарги чи заяви;

знайомитися з матеріалами перевірки;

подавати додаткові матеріали або наполягати на їх запиті органом, який розглядає заяву чи скаргу;

бути присутнім при розгляді заяви чи скарги;

користуватися послугами адвоката або представника трудового колективу, організації, яка здійснює правозахисну функцію, оформивши це уповноваження у встановленому законом порядку;

одержати письмову відповідь про результати розгляду заяви чи скарги;

висловлювати усно або письмово вимогу щодо дотримання таємниці розгляду заяви чи скарги;

вимагати відшкодування збитків, якщо вони стали результатом порушень встановленого порядку розгляду звернень.»

Відповідальність громадян за зміст звернень визначені у ст.26 Закону «Про звернення громадян»:

«звернення, яке містить наклеп і образи, дискредитацію органів державної влади, органів місцевого самоврядування, об'єднань громадян та їхніх посадових осіб, керівників та інших посадових осіб підприємств, установ і організацій незалежно від форм власності, заклики до розпалювання національної, расової, релігійної ворожнечі та інших дій, тягне за собою відповідальність, передбачену чинним законодавством.»

Законом «Про звернення громадян» чітко визначені підстави та порядок, коли звернення повертається громадянину, який його направив до установи (статті 5, 7) та відмов від розгляду (ст. 8), і серед таких підстав немає якихось обмежень щодо кваліфікації належності підпису. Також не є підставою для відмови розглядати звернення, якщо воно підписане з використанням не посиленого сертифіката, а будь-якого іншого сертифіката, за мотивом «неможливості встановити авторство» про що сказано вище у коментарі до статті 8 Закону «Про звернення громадян». Відмову у розгляді звернення за такими мотивами можна розглядати, як порушення Закону «Про звернення громадян» (стаття 24).

Стаття 24. Відповідальність посадових осіб за порушення законодавства про звернення громадян

Особи, винні у порушенні цього Закону, несуть цивільну, адміністративну або кримінальну відповідальність, передбачену законодавством України.

Законодавством України встановлений ряд норм, які обмежують свавілля чиновників та прямо передбачають відповідальність за протиправні дії: Кодекс України про адміністративні правопорушення, Закон «Про боротьбу з корупцією», Закон «Про державну службу».

Розглянемо детальніше відповідальність, передбачену вказаними законодавчими актами.

Кодекс України про адміністративні правопорушення

За статтею 212-3 «Кодексу України про адміністративні правопорушення» (далі – Кодекс) передбачена відповідальність у вигляді штрафу від п'ятнадцяти до двадцяти п'яти (за повторне – до п'ятдесяти) неоподатковуваних мінімумів доходів громадян,

Стаття 212-3. Порушення права на інформацію

Неправомірною відмовою в наданні інформації, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, у випадках, коли така інформація підлягає наданню на запит громадянина чи юридичної особи відповідно до законів України "Про інформацію", "Про звернення громадян" та "Про доступ до судових рішень", -

тягне за собою накладення штрафу на посадових осіб від п'ятнадцяти до двадцяти п'яти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення порушення з числа передбачених частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, -

тягне за собою накладення штрафу на посадових осіб від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Примітка. *Посадові особи, на яких поширюється дія Закону України "Про боротьбу з корупцією", притягаються до відповідальності за такі діяння відповідно до Закону України "Про боротьбу з корупцією".»*

Відповідальність посадових осіб за Законом «Про боротьбу з корупцією» розглянута далі.

В окремих випадках також можуть бути застосовані і інші статті цього Кодексу:

Стаття 82-3. *Приховування, перекручення або відмова від надання повної та достовірної інформації за запитом посадових осіб і зверненнями громадян та їх об'єднань щодо безпеки утворення відходів та поводження з ними: -*

тягне за собою накладення штрафу на посадових осіб від трьох до п'яти неоподатковуваних мінімумів доходів громадян.

Стаття 166-10. Порушення порядку видачі документа дозвільного характеру

Неповідомлення або несвоєчасне повідомлення дозвільним органом або адміністратором суб'єкта господарювання про прийняття рішення про відмову у видачі такого документа у строк, встановлений законом, -

тягне за собою накладення штрафу на посадових осіб від двадцяти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Порушення строків прийняття дозвільним органом рішення про видачу документа дозвільного характеру, неповідомлення адміністратором суб'єкта господарювання про одержання від дозвільних органів відповідних документів у строк, встановлений законом, -

тягне за собою накладення штрафу на посадових осіб від двадцяти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Дії, передбачені частиною першою або другою цієї статті, вчинені посадовою особою, яку протягом року було піддано адміністративному стягненню за такі ж порушення, -

тягнуть за собою накладення штрафу на посадових осіб від п'ятдесяти до сімдесяти неоподатковуваних мінімумів доходів громадян.

Безпідставна відмова дозвільним органом суб'єкту господарювання у видачі документа дозвільного характеру –

тягне за собою накладення штрафу на посадових осіб від двадцяти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Закон України «Про боротьбу з корупцією»

Стаття 5 цього Закону визначає спеціальні обмеження щодо державних службовців та інших осіб, уповноважених на виконання функцій держави, спрямовані на попередження корупції. Пунктом г) цієї статті визначено, що державний службовець або інша особа, уповноважена на виконання функцій держави, не має права:

«г) відмовляти фізичним та юридичним особам в інформації, надання якої передбачено правовими актами, умисно затримувати її, надавати недостовірну чи неповну інформацію;»

Дія цього пункту стосується і відмови у розгляді звернень громадян без законних на те підстав, визначених у Законі «Про звернення громадян» і які проаналізовані вище у цьому додатку до Коментарю.

За статтею 8 Закону України «Про боротьбу з корупцією» передбачається можливість накладання адміністративного стягнення у вигляді штрафу з посадової особи, яка здійснила порушення спеціальних обмежень, встановлених для осіб, уповноважених на виконання функцій держави, у тому числі пункту г) статті 5:

«Порушення особою, уповноваженою на виконання функцій держави, будь-якого із зазначених у статті 5 цього Закону обмежень, якщо воно не містить складу злочину, тягне за собою адміністративне стягнення у вигляді штрафу від п'ятнадцяти до двадцяти п'яти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року порушення будь-якого із зазначених у статті 5 цього Закону обмежень тягне за собою адміністративну відповідальність у вигляді штрафу від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян»

Для керівників установ, у разі умисного невжиття заходів до щодо припинення таких діянь, у тому числі пункту г) ст. 5, за ст.10 цього ж Закону передбачена аналогічна відповідальність.

«Керівники міністерств і відомств, державних підприємств, установ та організацій чи їх структурних підрозділів у разі виявлення чи отримання інформації про вчинення підлеглим корупційного діяння або порушення спеціальних обмежень, встановлених статтею 5 цього Закону, в межах своєї компетенції зобов'язані вжити заходів до припинення таких діянь та негайно повідомити про їх вчинення будь-який з державних органів, зазначених у пунктах "а", "а-1" і "б" статті 4 цього Закону.

Умисне невжиття такими керівниками заходів, передбачених частиною першою цієї статті, тягне за собою адміністративну відповідальність у вигляді штрафу від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.

Повторне протягом року вчинення діяння, передбаченого частиною другою цієї статті, тягне за собою адміністративну відповідальність у вигляді штрафу від двадцяти п'яти до п'ятдесяти неоподатковуваних мінімумів доходів громадян.»

Порядок вжиття заходів керівниками передбачає складання Протоколу про вчинення корупційного діяння або іншого правопорушення, пов'язаного з корупцією та виконання адміністративного провадження з передачею матеріалів до суду відповідно до ст.12 цього закону. Невиконання вимог частини першої статті 10 Закону «Про боротьбу з корупцією» тягне за собою відповідальність для керівників або контролюючих органів, передбачену статтею 11 цього ж Закону:

«Умисне нескладення або невчасне складення протоколу про вчинення корупційного діяння чи іншого правопорушення, пов'язаного з корупцією, за наявності для цього підстав, або умисне неподання до суду протоколу про вчинення корупційного діяння чи іншого правопорушення, пов'язаного з корупцією, особою, на яку покладено ці обов'язки, тягне за собою адміністративну відповідальність у вигляді штрафу від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян.»

Закон «Про державну службу»

Основні обов'язки державних службовців (стаття 10) за Законом «Про державну службу» передбачають:

«додержання Конституції України та інших актів законодавства України; забезпечення ефективної роботи та виконання завдань державних органів відповідно до їх компетенції;

недопущення порушень прав і свобод людини та громадянина;

збереження державної таємниці, інформації про громадян, що стала їм відома під час виконання обов'язків державної служби, а також іншої інформації, яка згідно з законодавством не підлягає розголошенню;

сумлінне виконання своїх службових обов'язків, ініціатива і творчість в роботі.

Державний службовець повинен діяти в межах своїх повноважень. У разі одержання доручення, яке суперечить чинному законодавству, державний службовець зобов'язаний невідкладно в письмовій формі доповісти про це посадовій особі, яка дала доручення, а у разі наполягання на його виконанні - повідомити вищу за посадою особу.»

Стаття 16 Закону «Про державну службу» включає обмеження, пов'язані з проходженням державної служби і описані вище щодо Закону «Про боротьбу з корупцією»:

«Державний службовець не має права вчиняти дії, передбачені статтями 1 і 5 Закону України "Про боротьбу з корупцією".»

До державних службовців можуть бути застосовані інші заходи впливу та припинення протиправних діянь, аналіз яких наведений вище, за **Законом «Про державну службу»**: ст.14 - застосування дисциплінарних стягнень, ст.22 - відсторонення від виконання повноважень за посадою, ст.30 - звільнення службовця з державної служби, а також обов'язковість відшкодування збитків громадянам за судовим рішенням, як передбачено Законом «Про звернення громадян» (ст. 19, 25).

Стаття 14. Особливості дисциплінарної відповідальності державних службовців

Дисциплінарні стягнення застосовуються до державного службовця за невиконання чи неналежне виконання службових обов'язків, перевищення своїх повноважень, порушення обмежень, пов'язаних з проходженням державної служби, а також за вчинок, який порочить його як державного службовця або дискредитує державний орган, в якому він працює.

До службовців, крім дисциплінарних стягнень, передбачених чинним законодавством про працю України, можуть застосовуватися такі заходи дисциплінарного впливу:

попередження про неповну службу відповідність;

затримка до одного року у присвоєнні чергового рангу або у призначенні на вищу посаду.

Стаття 22. Відсторонення від виконання повноважень за посадою

Невиконання службових обов'язків, що призвело до людських жертв або заподіяло значної матеріальної чи моральної шкоди громадянину, державі, підприємству, установі, організації чи об'єднанню громадян, є підставою для відсторонення державного службовця від виконання повноважень за посадою із збереженням заробітної плати. Рішення про відсторонення державного службовця від виконання повноважень за посадою приймається керівником державного органу, в якому працює цей службовець.

.....

Стаття 30. Підстави припинення державної служби

Крім загальних підстав, передбачених Кодексом законів про працю України, державна служба припиняється у разі:

1) порушення умов реалізації права на державну службу (стаття 4 цього Закону);

2) недотримання пов'язаних із проходженням державної служби вимог, передбачених статтею 16 цього Закону;

.....

5) виявлення або виникнення обставин, що перешкоджають перебуванню державного службовця на державній службі (стаття 12 цього Закону);

.....

Також статтею 38 Закону «Про державну службу», передбачено, що: «Особи, винні у порушенні законодавства про державну службу, несуть цивільну, адміністративну або кримінальну відповідальність згідно із чинним законодавством.»

Кримінальний Кодекс України

Вказані вище закони України передбачають, що дії державних службовців, які перешкоджають здійсненню громадянами, юридичними особами чи їх законними представниками прав і свобод, які охороняються законом, тягнуть за собою відповідальність цих осіб згідно статей Кримінального Кодексу України (далі – КК України). Такі дії можна кваліфікувати як: перевищення влади або службових повноважень (ст. 365 КК України) або зловживання владою або службовим становищем (ст. 364 КК України), чи службова недбалість (ст. 367 КК України). Відповідальність за цими статтями КК України передбачає різні види покарання: штрафи, виправні роботи, позбавлення волі або заборону займати відповідні посади чи займатись певною діяльністю. Наведемо відповідні пункти статей КК України:

Стаття 364. Зловживання владою або службовим становищем

1. Зловживання владою або службовим становищем, тобто умисне, з корисливих мотивів чи в інших особистих інтересах або в інтересах третіх осіб, використання службовою особою влади чи службового становища всупереч інтересам служби, якщо воно заподіяло істотну шкоду охоронюваним законом правам, свободам та інтересам окремих громадян або державним чи громадським інтересам, або інтересам юридичних осіб, -

карається виправними роботами на строк до двох років або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років, із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

2. Те саме діяння, якщо воно спричинило тяжкі наслідки, -

карається позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

3. Дії, передбачені частинами першою або другою цієї статті, якщо вони вчинені працівником правоохоронного органу, -

караються позбавленням волі на строк від п'яти до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та з конфіскацією майна.

Примітка. 1. Службовими особами є особи, які постійно чи тимчасово здійснюють функції представників влади, а також обіймають постійно чи тимчасово на підприємствах, в установах чи організаціях незалежно від форми власності посади, пов'язані з виконанням організаційно-розпорядчих чи адміністративно-господарських обов'язків, або виконують такі обов'язки за спеціальним повноваженням.

2. Службовими особами також визнаються іноземці або особи без громадянства, які виконують обов'язки, зазначені в пункті 1 цієї примітки.

3. Істотною шкодою у статтях 364, 365, 367, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян.

4. Тяжкими наслідками у статтях 364-367, якщо вони полягають у заподіянні матеріальних збитків, вважаються такі, які у двісті п'ятдесят і більше разів перевищують неоподатковуваний мінімум доходів громадян.

Стаття 365. Перевищення влади або службових повноважень

1. Перевищення влади або службових повноважень, тобто умисне вчинення службовою особою дій, які явно виходять за межі наданих їй прав чи повноважень, **якщо вони заподіяли істотну шкоду охоронюваним законом правам та інтересам окремих громадян, або державним чи громадським інтересам, або інтересам юридичних осіб,**

- карається виправними роботами на строк до двох років або обмеженням волі на строк до п'яти років, або позбавленням волі на строк від двох до п'яти років, із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

.....

3. Дії, передбачені частинами першою або другою цієї статті, **якщо вони спричинили тяжкі наслідки,** -

караються позбавленням волі на строк від семи до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

Стаття 367. Службова недбалість

1. Службова недбалість, тобто невиконання або неналежне виконання службовою особою своїх службових обов'язків через **несумлінне ставлення до них, що заподіяло істотну шкоду охоронюваним законом правам, свободам та інтересам окремих громадян, або державним чи громадським інтересам, або інтересам окремих юридичних осіб,** -

карається штрафом від п'ятдесяти до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.

2. Те саме діяння, якщо воно спричинило **тяжкі наслідки,** -

карається позбавленням волі на строк від двох до п'яти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років та зі штрафом від ста до двохсот п'ятдесяти неоподатковуваних мінімумів доходів громадян або без такого.

Дії службовців, які приймають та розглядають звернення громадян, ігноруючи при цьому вимоги законодавства України, тягнуть за собою відповідальність за ст. 356 КК України:

«Самоправство, тобто самовільне, всупереч установленому законом порядку, вчинення будь-яких дій, правомірність яких оспорується окремим громадянином або підприємством, установою чи організацією, якщо такими діями була заподіяна значна шкода інтересам громадянина, державним чи громадським інтересам або інтересам власника, -

карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до трьох місяців.»

Крім того, у випадку здійснення вказаних дій службовцем **щодо законного представника громадянина за зверненням**, таких службовець може бути притягнутий до відповідальності за ст. 397 КК України:

Стаття 397. Втручання в діяльність захисника чи представника особи

1. **Вчинення в будь-якій формі перешкод до здійснення правомірної діяльності захисника чи представника особи по наданню правової допомоги або порушення встановлених законом гарантій їх діяльності та професійної таємниці** -

карається штрафом від ста до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені службовою особою з використанням свого службового становища, -

караються штрафом від трьохсот до п'ятисот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.

В залежності від сутності звернень, з якими громадяни звертаються до державних органів, органів місцевого самоврядування, організацій, підприємств тощо, дії службовців, що перешкоджають здійсненню охоронюваним законом правам, а також свободам та інтересам окремих громадян або державним чи громадським інтересам, чи інтересам юридичних осіб, можуть підпадати під відповідальність, передбачену такими статтями КК України:

- Умисне перешкоджання законній діяльності професійних спілок, політичних партій, громадських організацій або їх органів (**Стаття 170**) - карається виправними роботами на строк до двох років або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років;

- Умисне перешкоджання законній професійній діяльності журналістів (**Стаття 171**) - карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років;

- Протидія законній господарській діяльності згідно (частини 3 **Стаття 206**) - караються позбавленням волі на строк від п'яти до десяти років;

- Примушування до антиконкурентних узгоджених дій (**Стаття 228**) - карається позбавленням волі на строк від двох до п'яти років.

Слід також відзначити, нормою статті 25 Закону «Про звернення громадян» передбачено відшкодування можливих збитків громадянину у зв'язку з порушеннями при розгляді його скарги:

«У разі задоволення скарги орган або посадова особа, які прийняли неправомірне рішення щодо звернення громадянина, відшкодовують йому завдані матеріальні збитки, пов'язані з поданням і розглядом скарги, обґрунтовані витрати, понесені у зв'язку з виїздом для розгляду скарги на вимогу відповідного органу, і втрачений за цей час заробіток. Спори про стягнення витрат розглядаються в судовому порядку.

Громадянину на його вимогу і в порядку, встановленому чинним законодавством, можуть бути відшкодовані моральні збитки, завдані неправомірними діями або рішеннями органу чи посадової особи при розгляді скарги. Розмір відшкодування моральних (немайнових) збитків у грошовому виразі визначається судом.»

Контроль за дотриманням законодавства про звернення громадян покладений на державні органи, місцеві органи самоврядування та Прокуратуру України за статтями 28 та 29 Закону «Про звернення громадян»:

«Контроль за дотриманням законодавства про звернення громадян відповідно до своїх повноважень здійснюють Верховна Рада України, народні депутати України, Президент України, Кабінет Міністрів України, Уповноважений з прав людини Верховної Ради України, Верховна Рада Автономної Республіки Крим, обласні, Київська та Севастопольська міські, районні, районні в містах Києві та Севастополі державні адміністрації, сільські, селищні, міські ради та їх виконавчі комітети, депутати місцевих

рад, а також міністерства, інші центральні органи виконавчої влади щодо підпорядкованих їм підприємств, установ та організацій.

Нагляд за дотриманням законодавства про звернення громадян здійснюється Генеральним прокурором України та підпорядкованими йому прокурорами. Відповідно до наданих їм чинним законодавством повноважень вони вживають заходів до поновлення порушених прав, захисту законних інтересів громадян, притягнення порушників до відповідальності.»

З метою упорядкування питання щодо впровадження в Україні засобів електронного цифрового підпису, як невід'ємної частини документообігу, було видано **Указ Президента України “Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування”** від 7 лютого 2008 року №109/2008, яким Кабінету Міністрів України було запропоновано у шестимісячний строк (тобто до **вересня 2008 року**) підготувати законопроект щодо внесення змін до існуючих законодавчих актів, в тому числі – щодо гарантування прав громадян на звернення до органів державної влади з використанням мережі Інтернет.

Установчою частиною цього Указу передбачено, зокрема пунктами 1 та 4, таке:

1. Кабінету Міністрів України, міністерствам, іншим центральним органам виконавчої влади, Раді міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським, районним державним адміністраціям та органам місцевого самоврядування вжити невідкладних заходів щодо забезпечення реалізації конституційних прав громадян на письмове звернення та особистий прийом, обов'язкове одержання обґрунтованої відповіді, неухильного виконання норм Закону України "Про звернення громадян", упорядкування роботи зі зверненнями громадян, зокрема, щодо:

недопущення надання неоднозначних, необґрунтованих або неповних відповідей за зверненнями громадян, із порушенням строків, установлених законодавством, безпідставної передачі розгляду звернень іншим органам;

викоренення практики визнання заяв чи скарг необґрунтованими без роз'яснення заявникам порядку оскарження прийнятих за ними рішень;

вжиття заходів для поновлення прав і свобод громадян, порушених унаслідок недодержання вимог законодавства про звернення громадян, притягнення винних осіб у встановленому порядку до відповідальності, в тому числі до дисциплінарної відповідальності за невиконання чи неналежне виконання службових обов'язків щодо розгляду звернень громадян;

4. Кабінету Міністрів України:

завершити підготовку та внести в шестимісячний строк у встановленому порядку до Верховної Ради України **проект Адміністративно-процедурного кодексу**, забезпечити його супроводження під час розгляду парламентом;

Цей проект Адміністративно-процедурного кодексу розроблений та затверджений Кабінетом Міністрів України, проте у ньому фактично не відображені в достатній мірі поставлені Указом Президента задачі, і загалом він має недоліки, які наведені у висновках Верховного Суду України².

розробити та подати в шестимісячний строк у встановленому порядку на розгляд Верховної Ради України законопроект про внесення змін до законодавчих актів щодо вдосконалення правового регулювання питань гарантування права громадян на звернення, поновлення порушених прав і свобод заявників, запровадження нових форм взаємодії між органами державної влади та органами місцевого самоврядування, фізичними і юридичними особами, в тому числі можливості

² <http://www.scourt.gov.ua/clients/vs.nsf/81b1cba59140111fc2256bf7004f9cd3/739a68cb0691b465c22574ff004d2e28?OpenDocument>

реалізації громадянами права на звернення до органів державної влади та органів місцевого самоврядування шляхом подання звернень із використанням мережі Інтернет;

забезпечити після набрання чинності відповідними змінами до законів запровадження прийняття та розгляду звернень громадян, що подаються з використанням мережі Інтернет;

затвердити у тримісячний строк єдиний загальнодержавний класифікатор звернень громадян;

запровадити до 1 січня 2009 року єдину комп'ютерну систему обліку звернень громадян та контролю за вирішенням порушених у них питань в органах виконавчої влади та органах місцевого самоврядування;

забезпечити впровадження у шестимісячний строк єдиної методики оцінки організації роботи зі зверненнями громадян в органах виконавчої влади та органах місцевого самоврядування;

Нажаль, Указ Президента України від 7 лютого 2008 року № 109/2008 станом на кінець січня 2009 року залишається у значній частині, яка вказана вище, не реалізованим, тобто звернення громадян України до органів державної влади, надіслані з використанням електронних засобів, навіть незважаючи на дію законодавчих актів залишаються для державних органів та багатьох інших організацій «річ у собі» (terra incognita).