УДК 342.9(004.9)+34.096
DOI https://doi.org/10.32844/2618-1258.2019.1-1.27

КОСТЕНКО О.В., КОСТЕНКО В.В.

ЕЛЕКТРОННІ ПІДПИСИ ТА ПОРЯДОК ВИЗНАННЯ ІНОЗЕМНИХ СЕРТИФІКАТІВ ЕЛЕКТРОННИХ ПІДПИСІВ У ЗАКОНОДАВСТВІ ОКРЕМИХ КРАЇН АЗІЇ

У статті проаналізовано досвід законодавчого регулювання правовідносин, які складаються під час застосування цифрових підписів та електронних довірчих послуг, окремих країн Азії. Досліджено понятійно-категоріальний апарат основних нормативно-правових актів сфери цифрового підпису. Вивчено норми права, що визначають порядки визнання іноземних електронних довірчих послуг і цифрових підписів у транскордонному режимі.

Узагальнено правотворчу діяльність країн Азії у сфері цифрового підпису та електронних довірчих послуг. Проаналізовано ключові дефініції законів «Про цифровий підпис» Малайзії, «Про електронні угоди» Сінгапуру, «Про електронні підписи» Китайської Народної Республіки, «Про інформаційні технології 2000 року» Індії, «Про електронні операції» Гонконгу та «Про електронний підпис і сертифікації підприємств» Японії.

Більш детально розглянуто норми Закону Індії «Про інформаційні технології 2000 року», що стосуються діяльності «Кіберапеляційного суду», а також класифікації кіберзлочинів і злочинів, що вчиняються із використанням цифрового підпису.

Проведено порівняльний аналіз національних нормативно-правових актів, окремих дефініцій до положень Типового закону ЮНСІТРАЛ «Про електронні підписи», «Регламенту (ЄС) № 910/2014 Європейського парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС», Закону України «Про електронні довірчі послуги» та законів інших країн.

Розглянуто досвід побудови законів, які одночасно регулюють у кількох правових напрямах, а також визначають види правопорушень, правопорушень і злочинів у сфері інформаційних технологій із запровадженням адміністративної та кримінальної відповідальності.

Проаналізовано фактичний стан українського законодавства на предмет наявності норм, що визначають відповідальність суб'єктів за порушення у сфері цифрового підпису та електронного документообігу. Констатовано, що нинішній стан національного законодавства в частині класифікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку обмежений статтями 361–363 Розділу XVI Кримінального кодексу України і не відповідає вимогам сьогодення.

Запропоновано рекомендації щодо вдосконалення вітчизняної нормативної бази.

Ключові слова: *цифровий підпис, електронний підпис, сертифікат, електронні довірчі послуги, транскордонний режим.*

The article analyzes the experience of legal regulation of legal relations, which are made during the use of digital signatures and electronic trust services, individual countries of Asia. The conceptual-categorical apparatus of the basic legal acts of the sphere of digital signature is investigated. The rules of law, which determine the procedures for recognition of foreign electronic trust services and digital signatures in the cross-border mode, are studied.

The law-making activities of Asian countries in the area of digital signatures and electronic trust services are summarized. The key definitions of the Malaysian "Digital Signatures Act",

© КОСТЕНКО О.В. – головний науковий співробітник (наукової установи) (Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України)

© КОСТЕНКО В.В. – старший науковий співробітник (Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України)

Singapore “Electronic Agreements”, “Electronic Signatures” of the People’s Republic of China, India’s “On Information Technology 2000”, Hong Kong “Electronic Transactions”, and “Electronic Signature and Certification of Enterprises” Japan.

More details are taken of the Indian law “On Information Technology 2000” relating to the Cyber Court of Appeal, as well as the classification of cybercrime and crime committed using a digital signature.

A comparative analysis of national legal acts, separate definitions of the provisions of the UNCITRAL Model Law on Electronic Signatures, Regulation (EC) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the domestic market and the repeal of the Directive have been carried out. 1999/93 / EC, the Law of Ukraine “On electronic trust services” and laws of other countries.

The experience of building laws that are simultaneously regulated in several legal areas is considered, as well as the types of offenses, offenses and crimes in the field of information technologies and the introduction of administrative and criminal liability. The actual state of Ukrainian legislation is analyzed for the presence of norms defining the responsibility of subjects for violations in the field of digital signature and electronic document circulation. It is stated that the current state of the national legislation regarding the classification of crimes in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks is limited by Articles 361–363 of Section XVI of the Criminal Code of Ukraine and does not meet the requirements of the present.

Recommendations on improvement of the domestic normative base are offered.

Key words: *digital signature, electronic signature, certificate, electronic trust services, cross-border mode.*

Вступ. Сьогодні впровадження інформаційно-комунікаційних технологій у всі сфери діяльності є пріоритетним напрямом інноваційного розвитку всіх країн світу та сучасного інформаційного суспільства. Використання інформаційно-комунікаційних технологій стимулює модернізацію та цифровізацію всіх напрямів функціонування держави та створює нові види суспільних відносин у сферах електронного документообігу, електронного менеджменту, цифрового підпису, електронної медицини, електронного банкінгу тощо. Потужні інформаційні потоки охоплюють усі сфери соціальних відносин, що не тільки створює позитивний потенціал для розвитку людства, а й водночас дає сучасні інструменти для скоєння правопорушень. Така ситуація характеризується падінням довіри до електронних сервісів, транскордонних послуг, цифрових транзакцій. Одним із вагомих елементів цифрової безпеки є застосування технології цифрового підпису. Безперечно, ця технологія ідентифікації особи в цифровому просторі має переваги перед іншими, наприклад біометричною, перш за все, наявністю законодавчих актів і технологічно захищених рішень.

Протягом досить короткого часу переважна більшість країн світу розробила та запровадила законодавчі акти, які регулюють правовідносини під час використання електронних підписів і сервісів [1]. Однак сьогодні не вирішеною загалом та актуальною залишається проблема транскордонного визнання цифрових підписів.

Постановка завдання. Метою статті є шляхом порівняльного аналізу вивчити законодавчі акти країн Азії у сфері цифрового підпису та електронних довірчих послуг і режими транскордонної взаємодії цифрових підписів, заснованих на різних юридичних доктринах.

Результати дослідження. У наукових працях вітчизняними та зарубіжними технічними фахівцями та правознавцями більше уваги приділяється вирішенню проблем транскордонної інтероперабельності технологічних рішень і стандартів цифрового підпису, що відображено в працях О. Перевозчикової, І. Горбенка, О. Потія, І. Бачило, E. Elgar, Stephen Mason S., Carolina M. Laborde, Stephen E. Blythe, Moliang Jiang, Minyan Wang, Minju Wang та інших. Донедавна проблематика міждержавного та транскордонного регулювання електронних довірчих послуг і цифрових підписів детально не розглядалася, тому цьому напряму правового регулювання й досі не приділяється необхідна увага.

На нашу думку, досвід розроблення країнами Азії законодавчих актів щодо правового функціонування інфраструктур відкритого ключа заслуговує на окремий детальний розгляд.

Країнами Азії практично одночасно з країнами Західної Європи та США вжиті нормотворчі заходи та створено законодавчу базу [2], що регулює суспільні відносини у сфері електронних документів та електронних підписів. Відразу доцільно звернути увагу на те, що нормативно-правове середовище Азії досить складне і через регіональні особливості значно контрастує із звичайними для нас європейськими правовими актами, що створює певні геополітичні бар'єри.

Першою країною цього регіону, яка ухвалила 1 жовтня 1998 року відповідний Закон «Про цифровий підпис» [3], стала Малайзія. Метою Закону є законодавче закріплення поняття «цифровий підпис» і встановлення певного порядку використання цифрових підписів шляхом створення відповідної інфраструктури сертифікаційних центрів. Відповідно до Закону «цифровий підпис» визначається як перетворення повідомлення з використанням асиметричного криптоалгоритму так, що людина, яка має вихідне повідомлення і відкритий ключ підписувача, може точно визначити: чи було це перетворення створено з використанням відповідного закритого ключа та чи змінювалося повідомлення з моменту перетворення. Для позначення поняття «електронний документ» використано термін «message» – цифрове відтворення інформації. Також запроваджено поняття «сертифікат», що визначає документ в електронній формі, який містить таке: назву сертифікаційного центру, що видав сертифікат; ідентифікацію підписувача; відкритий ключ підписувача, завірений цифровим підписом сертифікаційного центру, який його видав. Слід зазначити, що частину визначень у Законі «Про цифровий підпис» імпортовано із законів про цифрові підписи деяких штатів США.

Діяльність суб'єктів сфери електронного підпису в Малайзії регулюється спеціально уповноваженою особою – Контролером, який призначається Урядом. В його обов'язки входять створення і ведення бази даних, що містить відомості про ліцензовані сертифікаційні центри, а також здійснення публікації відомостей на спеціальному сайті. Діяльність ліцензованих сертифікаційних центрів додатково перевіряється незалежними недержавними аудиторами.

Майже одночасно із Малайзією законодавчо закріпив використання електронних документів і електронних підписів Сінгапур, прийнявши 10 липня 1998 року Закон «Про електронні угоди» [4]. Цим актом Сінгапур створив необхідні умови для розвитку національної електронної комерції та її виходу на міжнародний рівень. Дія Закону поширюється не тільки на укладення комерційних угод, але й на використання електронних документів державними установами і органами управління. Закон вводить такі поняття:

– «електронний підпис» – будь-які літери, числа або символи в цифровій формі, приєднані або логічно пов'язані з електронним документом, що використовує підписувач для посвідчення електронного документа;

– «цифровий підпис» – електронний підпис, отриманий унаслідок перетворення електронного документа з використанням асиметричної криптосистеми і хеш-функції так, що людина, яка має вихідний електронний документ і відкритий ключ, може точно визначити: чи був документ перетворений за допомогою закритого ключа підписувача та чи змінювався вихідний документ із моменту вчинення перетворення.

Отже, закон Сінгапуру запровадив одночасно дві дефініції: «електронний підпис» і «цифровий підпис». Електронний підпис – це базове поняття, яке визначає, що підписувач може використовувати будь-який метод створення електронного підпису, а цифровий підпис є одним із видів електронного підпису, для створення якого використовується певна технологія із закритим і відкритим ключами відповідно для створення і перевірки автентичності цифрового підпису.

Як і Малайзія, Сінгапур під час розробленняє національного закону використав досвід створення законів про цифрові підписи деяких штатів США: Флориди, Індіани, Орегону, Вашингтону.

Процедура визнання іноземних сертифікатів цифрового підпису має два рішення, одним з яких є добровільне взаємне визнання цифрових підписів під час укладання угод контрагентами, а другий полягає у визнанні Контролером закордонних сертифікатів дійсними в законодавчому полі Сінгапуру, якщо вони відповідають національним вимогам.

Закон «Про електронні угоди» привертає увагу тим, що законодавці в одному законодавчому акті поєднали загальні вимоги у сфері цифрового підпису, детальні вимоги до суб'єктів цифрового підпису, встановили окремі повноваження Контролера, який регулює діяльність цієї сфери та запровадили кримінальну відповідальність за певні види порушень. Наприклад, загальні заходи державного примусу полягають у застосуванні до правопорушників штрафів від 10 тис. до 50 тис. доларів та/або обмеженні волі на термін до 6 місяців.

Закон «Про електронні підписи» [5; 6] Китайської Народної Республіки (далі – КНР) прийнято на 11 засіданні Постійного комітету Десятого Національного з'їзду народних депутатів

28 серпня 2004 року, а чинності він набув 1 квітня 2005 року. Закон є частиною низки законодавчих актів, які призначені для регулювання електронної комерції, електронних договорів тощо [7].

Цим правовим актом визначено, що електронний підпис є даними в електронній формі, які містяться в повідомленні даних і додаються до них для ідентифікації особи, що підписує, чим встановлюється, що той, хто підписував, визнає зміст повідомлення. Повідомлення даних, як зазначено у цьому законі, означає інформацію, яка генерується, розсилається, приймається або зберігається електронними, оптичними, магнітними або подібними засобами. Також законом запроваджується поняття надійного електронного підпису. Таким уважається електронний підпис, який відповідає таким умовам: дані підписувача використовуються виключно для створення його електронного підпису; створення електронного підпису відбувається під контролем підписувача; є можливість виявлення будь-яких змін в електронному підписі; після застосування підпису може бути виявлена будь-яка зміна змісту та форми повідомлення даних. Сертифікатом електронного підпису вважається повідомлення даних або інші електронні записи, які можуть довести зв'язок між підписувачем і даними створення електронного підпису.

Слід зазначити, що Законом «Про електронні підписи» в КНР запроваджується процедура (послуга) перевірки/верифікації сертифікатів електронних підписів третьою стороною. Електронна перевірочна послуга повинна відповідати таким умовам: наявності кваліфікованого персоналу та доступних точок надання послуги верифікації; використанню технології та обладнання, що відповідають стандартам безпеки держави; наявності сертифікатів (ліцензій) щодо здійснення верифікації.

Процедурою верифікації передбачено видачу сертифіката, в якому зазначається назва електронної служби верифікації, власник сертифіката, серійний номер сертифіката, термін дії сертифіката, дані перевірки електронного підпису власника сертифіката, електронний підпис служби електронної перевірки, інші відомості, необхідні для верифікації. Електронна служба перевірки гарантує, що дані в сертифікаті електронного підпису є повними і точними протягом терміну його дії, а також гарантує стороні, яка посилається на електронний підпис, можливість довести або знати дані, зазначені в сертифікаті електронного підпису, та іншу інформацію. Законом вводиться відповідальність для служби електронної перевірки за надання недостовірних послуг верифікації. Також вводиться кримінальна відповідальність за підробку, копіювання або привласнення електронного підпису іншої особи.

Визнання іноземних сертифікатів цифрового підпису здійснюється електронною службою перевірки – державним верифікаційним центром на підставі відповідних угод або принципу взаємності. Принцип взаємності полягає в тому, що сертифікати електронних підписів, видані іноземними верифікаційними центрами за межами КНР, мають однакову юридичну силу з тими, що видаються електронними службами верифікації, за умови відповідності законодавству КНР.

Розглядаючи законодавство КНР, слід враховувати відомий історичний факт, пов'язаний із районом КНР Гонконг, який має статус спеціального адміністративного району і сьогодні є одним із ключових фінансових центрів Азії та світу. Наприклад, у 1842 році Гонконг захопило Сполучене Королівство Великобританії та утримувало його як колонію згідно з Нанкінським договором. Починаючи із 1997 року, відповідно до спільної китайсько-британської декларації та Основному закону, Гонконгу надана широка автономія до 2047 року за формулою «Одна країна, дві системи», тому на території Гонконгу діє власне законодавство.

На відміну від Закону «Про електронні підписи» КНР, у Гонконзі діє Указ «Про електронні операції» [8], який має розширену структуру. Указом визначено такі поняття, як сертифікат, електронний запис (дані), цифровий підпис, електронний підпис, хеш-функція, інформаційна система тощо. Зокрема, сертифікатом є документ, виданий сертифікаційним органом із метою забезпечення легітимності цифрового підпису, який передбачає підтвердження ідентичності або інших значущих характеристик особи, яка має певну пару ключів, а також ідентифікує орган, який видав сертифікат, і особу, що підписувала, та містить публічний ключ особи, якій він виданий. Відповідно до зазначеного нормативно-правового акта:

– «електронний запис» (дані) означає запис, створений у цифровій формі інформаційною системою, який може передаватися в інформаційній системі від однієї інформаційної системи до іншої та зберігатися в інформаційній системі або в іншому середовищі;

– «електронний підпис» означає будь-які літери, символи, цифри або інші символи в цифровій формі, прикріплені до електронного запису або логічно пов'язані з ним, а також створені чи прийняті з метою автентифікації або затвердження електронного запису.

«Цифровим підписом» щодо електронного запису є електронний підпис підписувача, отриманий шляхом перетворення електронного запису з використанням асиметричної крипто-

системи та хеш-функції, особою, яка має початковий нетрансформований електронний запис і відкритий ключ підписувача, та дає змогу визначити, що генеровані перетворення здійснено за допомогою закритого ключа, який відповідає відкритому ключу підписувача, та може визначити наявність або відсутність змін початкового електронного запису після генерування.

Політиками в сфері електронного підпису керує урядова уповноважена особа – головний інформаційний директор Уряду. В його обов'язки входить забезпечення процедури сертифікації фізичних та юридичних осіб, які мають наміри здійснювати діяльність із надання послуг цифрового підпису. Головний інформаційний директор Уряду зобов'язаний здійснювати заходи перевірки, а саме: встановлювати, чи має фізична особа засудження в Гонконзі або в інших місцях за шахрайство та корупцію або не є банкрутом; що юридична особа не перебуває у стані ліквідації або банкрутства.

Указ «Про електронні операції» містить кілька досить цікавих рішень. Наприклад, запроваджено норму «межа довіри», якою орган сертифікації, що видає сертифікат, може вказати обмеження довіри в сертифікаті, встановлювати різні обмеження в різних сертифікатах або в різних типах, класах або описі сертифікатів. Встановлюється адміністративна та кримінальна відповідальність за вчинення із застосуванням цифрового підпису дій, пов'язаних із шахрайством.

З приводу визнання іноземних сертифікатів цифрового підпису та електронних довірчих послуг, то законодавство Гонконгу віддає перевагу користувачам самостійно вибирати різні форми підписів і налаштовувати їх у бізнес-процесах, заснованих на формі, яка є найбільш зручною та відповідною для кожного випадку використання. Для цього користувачі узгоджують між собою порядок ведення бізнесу електронними технологіями.

17 жовтня 2000 року парламентом Індії прийнято Закон «Про інформаційні технології 2000 року» (також відомий як ITA-2000 або Закон № 21 від 2000 року). Цей акт є базовим законом в Індії у сферах цифрового підпису, кіберзлочинності та електронної комерції. Закон має вищу юридичну силу на всій території країни та стосується не тільки цифрового підпису, але й злочинів, пов'язаних із використанням цифрової інформації, комп'ютерів, мереж та інформаційно-комунікаційних технологій безпосередньо в Індії.

У літературі є цікаве визначення – «Long status» («довгий статут»). Це визначення застосовано вперше до закону штату ЮТА США «Про цифровий підпис», який не тільки визначає законний статус цифрового підпису, але й комплексно вирішує цілу низку питань і проблем, пов'язаних із використанням електронних документів і цифрового підпису.

На нашу думку, таке ж визначення можливо застосувати і до закону Республіки Індія, оскільки він складається із більш ніж 94 розділів, поділених на 13 глав, має 4 додатки із понад 50 правками, які внесені в різні розділи Кримінального кодексу Індії, закони «Про докази», «Про банківські свідчення» та «Про резервний банк Індії».

Відмінність закону Індії від переважної більшості законодавчих актів інших країн полягає в тому, що він не тільки визнає електронні записи і цифрові підписи, але й визначає та класифікує кіберзлочини і встановлює відповідні покарання за їх вчинення. Крім того, закон регламентує створення і функціонування «Кіберапеляційного суду», на який покладаються обов'язки вирішення спорів і розгляд справ про злочини в сфері цифрового підпису та інформаційно-комунікаційних технологій. Регулювання сфер діяльності, визначених законом, покладається на державний орган «Контролер», який має повноваження вчиняти дії примусового характеру, за невиконання яких інші суб'єкти можуть нести кримінальне покарання.

Законом запроваджується низка техніко-юридичних визначень, таких як:

– «дані» – представлення інформації, знань, фактів, документів, які готуються або були підготовлені у формалізованому вигляді та призначені для обробки, оброблені або оброблюються тепер у комп'ютерній системі або комп'ютерній мережі і можуть бути збережені в будь-якій формі (включно, з комп'ютерними роздруківками, магнітними або оптичними носіями, перфокартами, перфострічками) або зберігаються у внутрішній пам'яті комп'ютера;

– «комп'ютер» – будь-який електронний, магнітний, оптичний або інший високошвидкісний пристрій обробки даних або система, який виконує логічні, арифметичні і функції пам'яті, здійснює маніпуляції електронними, магнітними або оптичними імпульсами і включає в себе вхід, вихід, обробку, зберігання, комп'ютерне програмне забезпечення або засоби зв'язку, які пов'язані між собою або пов'язані з комп'ютером у комп'ютерні системи або комп'ютерні мережі;

– «комп'ютерна мережа» – це з'єднання одного або більше комп'ютерів через супутникові, радіо, проводові лінії або інші засоби зв'язку, а також термінали або комплекси, що складаються з двох або більше взаємопов'язаних комп'ютерів, взаємозв'язок між якими підтримується постійно;

– «інформація» – дані, текст, зображення, звук, голос, коди, комп'ютерні програми, програмне забезпечення та бази даних або мікрофільм, або згенерований комп'ютером машинний текст.

Законом встановлено низку визначень, які застосовуються для регулювання сфери цифрового підпису, а саме :

– «цифровий підпис» – автентифікація будь-якого електронного запису абонентом за допомогою електронного методу або процедура за законом;

– «сертифікат цифрового підпису» – цифровий сертифікат підпису, виданий відповідно до вимог закону»;

– «електронна газета» – офіційна газета, що опублікована в електронному вигляді;

– «електронний запис» – дані, запис або згенеровані дані, зображення або звук збережені, отримані або відправлені в електронній формі;

– «підписувач» – особа, від імені якої цифровий сертифікат підписується або видається.

Процедура визнання іноземних цифрових підписів і сертифікатів цифрових підписів полягає в тому, що будь-який іноземний сертифікаційний центр повинен здійснити державну реєстрацію в Індії, повідомлення про що публікується в національній електронній газеті. Водночас в Індії широкого впровадження в бізнесі набула перехресна сертифікація.

Що стосується питання юридичної відповідальності, то, на відміну від переважної більшості аналогічних законодавчих актів інших країн, Закон «Про інформаційні технології 2000 року» встановлює перелік правопорушень та злочинів у сфері інформаційних технологій і запроваджує за їх вчинення адміністративну та кримінальну відповідальність. До кримінальних проступків законом віднесено такі: підробку комп'ютерних вихідних кодів або документів, злом за допомогою комп'ютерної системи, отримання та зберігання вкраденого комп'ютера або пристрою зв'язку, шахрайство з використанням комп'ютерного ресурсу, публікація приватних зображень інших людей без їх відома, акти кібертероризму, публікація непристойної інформації в електронному вигляді, публікація зображень, що містять статеві акти або дитячу порнографію.

Також закон класифікує правопорушення та злочини у сфері цифрового підпису, такі як:

– отримання обманним шляхом і використання паролів, цифрового підпису або іншої унікальної інформації, що ідентифікує іншу особу;

– введення в оману Контролера або засвідчувального центру шляхом подачі неправдивої інформації з метою отримання ліцензії або сертифіката цифрового підпису;

– намагання отримати або отримання несанкціонованого доступу до захищених систем, які визначені шляхом опублікування в офіційному віснику Контролера – електронній газеті;

– відмова у наданні уповноваженому державному органу інформації та у дешифруванні даних, які передавалися або передаються через будь-який комп'ютерний ресурс.

Крім того, у 2008 році законом запроваджено поправку, яка й досі створює юридичні колізії та суперечки серед індійських правознавців. Наприклад, розділ 66А Закону вводить норму «публікація образливої, помилкової або загрозливої інформації», яку класифікує як відправлення будь-якою особою і будь-яким способом із комп'ютерного ресурсу будь-якої інформації, яка є надзвичайно образливою або має загрозливий характер, або є недостовірною і має за мету викликати образу або наругу.

Законом «Про інформаційні технології 2000 року» встановлено досить вагомі покарання за вказані вище злочини. Заходи державного примусу можуть полягати в обмеженні волі від трьох до десяти років та штрафі від 200 тисяч до 1 млн рупій. Злочини, які кваліфікуються як кібертероризм, караються довічним позбавленням волі.

В Японії Закон «Про електронний підпис і сертифікації підприємств» [9] (закон № 102) набув чинності 1 квітня 2001 року. Цей Закон включає в собі визначення тільки двох термінів «електронний підпис» і «засвідчення справжності», а також у ньому вказується, що організації, які підлягають конкретному виду сертифікації, потребують акредитації в компетентних міністерствах – Міністерстві з адміністративних справ і комунікацій, Міністерстві юстиції та Міністерстві економіки, торгівлі і промисловості. В Японії з квітня 2001 року створена та функціонує Державна інфраструктура відкритих ключів. Визнання іноземних цифрових підписів регулюється окремим розділом Закону «Про електронний підпис і сертифікації підприємств», яким передбачено можливість реєстрації іноземного сертифікаційного центру в Державній інфраструктурі відкритих ключів, а також здійснення процедур визнання в межах міждержавних угод.

Суспільні відносини у сфері цифрового підпису в Республіці Корея регулюються такими законами: «Актом про цифровий підпис» [10] від 5 лютого 1999 року та «Рамковим Актом на електронні документи та угоди» [11] від 1 червня 2012 року. Зазначені Закони запроваджують такі терміни:

– «електронне повідомлення» – частина інформації, яку згенеровано і відправлено, що приймається або зберігається в цифровому вигляді системою обробки інформації;

– «цифровий підпис» – частина інформації в цифровій формі, що прикріплено або логічно об'єднано з електронним повідомленням, яка може ідентифікувати підписувача і надає можливість перевірки того, що електронне повідомлення було підписано цим підписувачем;

– «сертифікований цифровий підпис» – цифровий підпис, який заснований на авторизованому сертифікаті і відповідає таким вимогам: ключ для створення цифрового підпису повинен зберігатися і бути відомим тільки підписувачу; підписувач повинен особисто контролювати створення цифрового підпису та використовувати ключ на момент підписання; можливість встановлення фактів змін у відповідному цифровому підписі з моменту його прикріплення, а також встановлення змін в електронному повідомленні, підписаному цифровим підписом;

– «сертифікат» – комп'ютерний запис, яким встановлюється і перевіряється те, що створений ключ цифрового підпису, зберігається і відомий тільки абоненту;

– «підписувач» – особа, яка має свій власний цифровий підпис і створює ключ і підпис від свого імені або від імені іншої особи.

Досить рідкісною є дефініція «інформація про людину». Інформація про людину означає частину інформації, яка стосується живої людини і яка є такими знаками, буквами, голосом, звуком, зображенням, фізичними характеристиками і т. п., що можуть служити для встановлення особи, яка асоціюється із документами, що посвідчують особу, реєстраційним номером резидента, страховим полісом тощо.

Регуляцію у сфері цифрового підпису та електронного документообігу здійснює уряд Республіки Корея в особі міністра державного управління та безпеки. Серед інших регуляторних функцій на міністра покладено обов'язки забезпечення досягнення внутрішньої інтероперабельності систем і технологій цифрового підпису шляхом вивчення та дослідження вітчизняних і закордонних стандартів для взаємного визнання та використання різноманітних сертифікатів цифрового підпису, а також встановлення та адаптації цифрового підпису та сертифікатів для взаємного визнання.

Слід зазначити, що, на відміну від вказаних вище нормативних актів, Закон «Акт про цифровий підпис» має спеціальну статтю 27-2 «Взаємне визнання». Законом визначено, що уряд може укласти угоду із урядом іншої країни щодо взаємного визнання цифрових підписів. Законом передбачено, що у разі укладання міждержавної угоди уряд може сформувати і видати іноземному сертифікаційному центру ліцензію та уповноважений сертифікат, які юридично легалізують обмін і визнання цифрових підписів між державами.

В «Акті про цифровий підпис» також визначено низку правопорушень у сфері цифрового підпису, за які покарання встановлено іншими нормативно-правовими актами.

Доцільно звернути увагу на те, що «Рамковим Актом на електронні документи та угоди» запроваджено систему довірчих органів, на які покладено функції третьої довірчої сторони, що забезпечує і гарантує цілісність та надійність електронних угод та електронних документів, посвідчених електронними та цифровими підписами, а також їх зберігання та надання для використання в судових спорах.

Загалом, законодавчі акти країн Азії спрямовані на технології та правові рішення по територіальному принципу. Водночас у цих країнах функціонують так звані наддержавні технології, які стимулюють людей використовувати певні інформаційні продукти транснаціональних корпорацій. Наприклад, Китай, Гонконг, Індія, Малайзія та Японія мають центри сертифікації та постачання електронних довірчих послуг у межах програми «Затверджений список довірених сертифікатів Adobe (AATL)», за допомогою якої користувачі продуктами компанії «Adobe Systems» (Adobe Acrobat Reader DC, Acrobat DC або Adobe Sign) можуть додавати цифровий підпис до документів в Adobe Document Cloud за допомогою довірених цифрових ідентифікаторів.

Висновки. Узагальнюючи нормотворчу діяльність окремих країн Азії у сфері цифрового підпису та електронних довірчих послуг, можемо зазначити таке.

Практично всі розглянуті нормативно-правові акти закріпили дефініції «електронний підпис», «цифровий підпис», «сертифікат», «підписувач» та інші. Для їх створення використані аналогічні норми Типового закону ЮНСІТРАЛ «Про електронні підписи» та закони деяких штатів США. Крім того, законодавчі акти країн Азії чітко визначають права, обов'язки і відповідальність усіх суб'єктів правовідносин у цій сфері. На відміну від українського законодавства, права державних органів, які здійснюють регуляцію у сфері цифрового підпису, посилені можливостями та правом застосовувати суттєві санкції та оперативного втручання в діяльність суб'єктів у разі загрози національним інтересам.

Електроні довірчі послуги в законодавстві країн Азії як такі, що не відповідають положенням «Регламенту (ЄС) №910/2014 Європейського парламенту та Ради щодо електронної

ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС» та Закону України «Про електронні довірчі послуги», а також не сформовані та чітко не визначенні на законодавчому рівні. Водночас у країнах Азії активно розвиваються електронна комерція, електронні послуги, електронна логістика та електронний документообіг, які використовують цифровий підпис, що формується за національними вимогами.

На відміну від переважної більшості законодавчих актів у цій сфері, які розроблені країнами Європи, Латинської Америки, США та України, закони країн Азії мають розділи, які визначають види правопорушень і встановлюють конкретні покарання.

Суттєвий науковий інтерес становить Закон Індії «Про інформаційні технології 2000 року» в частині розділів, присвячених функціонуванню «Кіберапеляційного суду», переліком правопорушень і злочинів у сфері інформаційних технологій і запровадженням адміністративної та кримінальної відповідальності. На нашу думку, такий підхід позитивно впливає на правову дисципліну в суспільних правовідносинах під час застосування цифрових підписів, покращує інформаційну гігієну та підвищує довіру до електронної комерції і цифрових сервісів.

Сьогодні в українському законодавстві фактично не має чіткого визначення та переліку правопорушень у сфері цифрового підпису та електронного документообігу. Оцінка прецедентів порушень законодавства, які пов'язані з використанням цифрового підпису, здійснюється в контексті статей 361–363 Кримінального кодексу України, причому цифровий підпис розглядається як об'єкт або знаряддя злочину, як технічний засіб несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Проблеми відповідальності та покарання за компрометацію цифрового підпису взагалі не розглядаються.

Як підсумок можна констатувати, що українське законодавство, а саме Закон України «Про електронні довірчі послуги», з юридично-технічного погляду є не досить досконалим. Наприклад, у Законі відсутні норми, що визначають відповідальність суб'єктів за порушення встановлених законом обов'язків. Також у законодавстві України відсутній перелік злочинів у сфері цифрового підпису, електронних довірчих послуг, електронного документообігу. Вважаємо, що саме в цьому напрямі доцільно зосередити зусилля правознавців і вжити заходів щодо наближення українського законодавство до сучасних світових правових доктрин.

Список використаних джерел:

1. Carolina M. Laborde. Electronic Signatures in International Contracts. Freiburg (Breisgau), Univ., Diss. 2008. URL: https://books.google.com.ua/books/about/Electronic_Signatures_in_International_C.html?id=Cne-igPOkhgC&redir_esc=y (дата звернення: 15.06.2018).

2. Stephen Mason. Electronic Signatures in Law. ISBN-13 978 1 911507 01 7 (Open Access PDF). 2012. URL: https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicsignatures (дата звернення: 25.02.2018).

3. Laws of Malaysia Act 562 Digital Signature Act 1997. 1997. URL: https://www.wipo.int/edocs/lexdocs/laws/en/my/my058en.pdf (дата звернення: 10.02.2019).

4. Electronic Transactions Act (Chapter 88). 2010. URL: https://sso.agc.gov.sg/Act/ETA2010 (дата звернення: 15.02.2019).

5. Law of the People's Republic of China on Electronic Signatures. 2010. URL: http://www.china.org.cn/business/2010-01/21/content_19281152.htm (дата звернення: 24.03.2019).

6. Minyan Wang, Minju Wang. Introduction to the Electronic Signatures Law of People's Republic of China. Digital evidenced electronic signatures Lawreview. 2004. URL: https://sas-space.sas.ac.uk/5445/1/1755-2375-1-SM.pdf (дата звернення: 23.04.2018).

7. Stephen E. Blythe. China's New Electronic Signature Law and Certification Authority Regulations: A Catalyst for Dramatic Future Growth of E-Commerce. *Chicago-Kent Journal of Intellectual Property.* 2007. URL: https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1059&context=ckjip (дата звернення: 15.05.2019).

8. Electronic Transactions Ordinance. 2000. URL: https://www.elegislation.gov.hk/hk/cap553 (дата звернення: 12.04.2019).

9. Act on Electronic Signature and Certification Business (Japan). 2000. URL: http://afyonluoglu.org/PublicWebFiles/e-imza/int-legislation/Japan-Act%20on%20Electronic%20Signature%20and%20Certification%20Business.pdf. (дата звернення: 12.04.2019).

10. Republic of Korea Digital Signatures Act. 1999. URL: http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN042823.pdf (дата звернення: 25.04.2019).

11. Framework Act on Electronic Documents and Transactions. 2002. URL: http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=27334&type=part&key=28 (дата звернення: 18.05.2019).