

Також слід зазначити, що Закон регулює здійснення юридичними особами різноманітних операцій з криптовалютою: купівля, продаж, приймання оплати і сплата з прибутку 5-% податку.

Отже, в зв'язку із збільшенням масштабів використання цифрових форм закріплення прав, криптовалюта може розглядатися як самостійний об'єкт цивільного права. Хоча ця валюта віртуальна, проте об'єктивна та як матеріальне благо має свою цінність та оборотоздатність. Враховуючи проекти, які зареєстровані у Верховній Раді України, можна стверджувати, що правове регулювання криптовалюти знаходиться на шляху становлення.

ЛІТЕРАТУРА:

1. Савельев А.И. Криптовалюты в системе объектов гражданских прав // Журнал «Закон». № 8. 2017. С.136-154.
2. Украина узаконит криптовалюту и введет на нее налог. URL: <https://mycrypter.com/ukraine-uzakonit-kriptovalyutu-i-vved/>
3. Проект Закону про обіг криптовалюти в Україні №7183 від 06.10.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684
4. Проект Закону стимулювання ринку криптовалют та їх похідних в Україні №7183-1 від 10.10.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710
5. Проект Закону про внесення змін до Податкового кодексу України щодо оподаткування операцій з віртуальними активами в Україні №9083 від 14.09.2018. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64597

*Глуговська Аріна Анджейвна,
студентка 3 курсу факультету адвокатури
Національного університету «Одеська юридична академія»
Науковий керівник – к.ю.н., доцент Костова Н.І.*

РЕГУЛЮВАННЯ ВІДНОСИН ДОВІРИ ДО ЕЛЕКТРОННОГО ПІДПISУ В УКРАЇНІ

На сьогоднішній день розвиток глобальних комунікацій в житті людини привів до появи новітніх взаємовідносин, предметом яких є електронний обмін даними. У такому обміні даними можуть брати участь органи державної влади, підприємства, а також громадяни в своїх офіційних і особистих стосунках. Одним з найпопулярніших в світі засобів захисту електронного обміну є, так званий, електронний підпис, завдяки якому, за

допомогою спеціального програмного забезпечення, може підтверджувати правдивість інформації документу, його реквізитів і факту підписання конкретною особою.

Актуальними аспектами моєї теми є те, що ми, перш за все, отримуємо довіру, адже використовуючи електронний підпис (ЕП), громадяни можуть одержувати можливість шифрування документів. Завдяки надійним криптографічним алгоритмам забезпечується конфіденційність інформації, яка передбачає неможливість доступу до неї будь-якої особи, що не володіє секретним ключем. Ще однією найважливішою гарантією є те, що електронний підпис (ЕП) проходить обов'язкову експертизу в Державній службі спеціального зв'язку та захисту інформації в Україні. Також використання електронного підпису (ЕП) значно прискорює проведення численних комерційних операцій, виключає необхідність додаткових зустрічей і багатогодинних переговорів.

Однак із найважливіших правових проблем електронного підпису (ЕП) – це те, що впровадження ЕП йде повільніше, ніж очікувалося. Головною причиною є так звані стримуючі чинники, до яких можна віднести наступні: фальсифікація ЕП, незаконне здобуття влади та використання сертифікатів ЕП, передача ЕП іншій юридичній особі з порушенням встановлених правил; відсутність потреби використання ЕП в закритих інформаційних системах; рівень безпеки ЕП в Україні у порівнянні з цифровим підписом в ЄС, є значно заниженим на законодавчому рівні, що відбивається і та на інших нормах права.

Закон України «Про електронні довірчі послуги» закріплює, що електронний підпис – це можуть бути електронні дані, які долучаються підписувачем до інших електронних даних або послідовно з ними пов'язуються і використовуються ним як підпис.

Згідно з законом України «Про електронні довірчі послуги» електронний підпис може бути трьох категорій: простий електронний підпис та печатка – низький рівень довіри; удосконалений електронний підпис та печатка – середній рівень довіри; кваліфікований електронний підпис та печатка – високий рівень довіри.[1] Також до електронних підписів належать шифрування: симетричне та асиметричне шифрування. Симетричне шифрування передбачає наявність двох однакових ключів у кожної зі сторін: один «закриває», другий – «відкриває» передані дані. Такий спосіб захищає передачу даних від втручання (доступу) третьої сторони. Асиметричне шифрування передбачає наявність двох пар різних ключів: відкритого і секретного. Якщо шифрування відбувалося за допомогою відкритого ключа, то розшифровка можлива за допомогою таємного, і навпаки. Скористатися

ключами з різних пар неможливо, оскільки кожна пара невід’ємна ланка всієї системи.

Надання довіри та гарантії електронного підпису дає нам Центр сертифікації ключів. Даним центром може бути як юридична особа незважаючи на форму власності або фізична особа, яка може бути суб’єктом підприємницької діяльності, яка має надавати послуги електронного цифрового підпису та засвідчувати свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі. Центр зобов’язаний: забезпечувати захист інформації в автоматизованих системах відповідно до законодавства; здійснювати захист персональних даних, отриманих від підписувача, згідно з законодавством; вчасно заперечувати, блокувати та поновлювати сертифікати ключів; впроваджувати електронний перелік чинних, відмінених і блокованих сертифікатів ключів; постачати цілодобово доступ споживачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали та інше.[2] Саме центр сертифікації формує закритий ключ і власний сертифікат, засвідчує їх автентичність своїм цифровим підписом. І це є одним з найважливіших способів захисту електронних цифрових підписів від підробки.

Ще одним надійним гарантом довіри ЕП є, державна служба спеціального зв’язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку, а також інших завдань відповідно до закону. [3]

Одна із найважливіших правових проблем електронного підпису (ЕП) є сфальсифікація ЕП, або ще називають «атаки». На сьогоднішній день виділяють такі моделі атак: атака з використання відкритого ключа (особа, яка зламує, володіє відкритим ключем та набором підписаних повідомлень); атака на основі відомих повідомлень (правопорушник володіє тільки допустимим підписами набору електронних документів, які йому вже відомі, але які він не має можливості вибрати сам); адаптивна атака на основі вибраних повідомлень. [4] Найбільш зосередженим моментом є те, що рівень безпеки ЕП в Україні, у порівнянні з цифровим підписом в ЄС, є значно заниженим на законодавчому рівні, що відбивається і та на інших нормах права.

Для відповідності українських та міжнародних стандартів необхідно: класифікувати законодавство України щодо ЕП для того, щоб відповідало до міжнародних стандартів та розробити єдиний підхід до використовуваних алгоритмів створення ЕП.

Отже, можна зробити висновок, що ЕП відіграє найголовнішу роль в системі електронного документообігу, оскільки саме ЕП використовується фізичними, юридичними персонами з цілю ідентифікації підписувача та підтвердження цілісності даних в електронній формі. Маючи електронний підпис, він нам гарантує, що акт був створений саме цією людиною, тому цей акт з ЕП рівнозначний своєму паперовому аналогу. Переваги електронного числового підпису безумовні, а, якщо звернути увагу, що в режимах, використовуються електронні документи, пред'являються суворіші вимоги до цілісності та автентичності документів, то альтернативи для цифрового підпису немає.

ЛІТЕРАТУРА:

1. Закон України «Про електронні довірчі послуги» від 05.10.2017 за № 2155-VIII-[Електронний ресурс] -<https://zakon.rada.gov.ua/laws/show/2155-19>
2. Давидова І.В. Електронний цифровий підпис: порядок отримання та ступінь захисту/ Давидова І.В. – М.: Українське право, 2018. – ст.38
3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 за № 3475-IV –[Електронний ресурс]-<https://zakon.rada.gov.ua/laws/show/2155-19>
4. Трофименко О. Г. Електронне врядування в Україні у контексті розвитку інформаційного суспільства / Трофименко О. Г., Логінова Н.І., Буката Л.М. // Порівняльно-аналітичне право: електронне наукове фахове видання. – Ужгород, 2016. – № 1. – С. 231 – 234.

*Дарієнко Олександра Олександрівна,
студентка 3 курсу судово-адміністративного факультету
Національного університету «Одеська юридична академія»
Науковий керівник – к.ю.н., доцент Завальнюк С. В.*

ПЕРСПЕКТИВИ ФУНКЦІОНУВАННЯ В УКРАЇНІ ODR-ПЛАТФОРМ ЯК НОВІТНЬОЇ КОНЦЕПЦІЇ ВИРІШЕННЯ СПОРІВ

Електронне вирішення спорів – це сукупність методів врегулювання спорів (конфліктів) із застосуванням інтернет-технологій, спеціальних програм. Зростаюча популярність такого виду АВС зумовлена: а) можливістю