ПРИКЛАДНА МАТЕМАТИКА

УДК 004.9:357.741

Николайчук Л. М., к.ю.н., доцент (Івано-Франківський національний технічний університет нафти і газу)**, Николайчук Я. М., д.т.н, професор** (Тернопільський національний економічний університет)

ІНФОРМАЦІЙНА МОДЕЛЬ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРАВА НА ОСНОВІ СТЕГАНОГРАФІЇ ТА ШИФРУВАННЯ

Викладена методологія побудови моделей взаємодії суб'єктів права в умовах сучасного інформаційного суспільства. Запропонована нова модель взаємодії десяти інтелектуальних суб'єктів права.
Ключові слова: **інформаційні моделі, юриспруденція, цифровий підпис.**

Вступ. Глибоке дослідження характеристик юридичної інформації, в тому числі розробка теоретичних засад моделювання процесів правочину та подання юридичних знань є актуальною проблемою. Успішне вирішення цієї проблеми може суттєво впливати на досконаліть, оперативність та результативність формалізації юридичних законів, особливо комп'ютерно-інформаційному супроводженні взаємодії фізичних та юридичних осіб на основі відповідних інструментальних засобів експертної та телекомунікаційної техніки, а також прогресивних інформаційних технологій.

Інститут права приватної власності є важливою галуззю цивільного права України і правовою формою, яка є головною основою забезпечення різноманітних матеріальних та духовних потреб громадян України.

Трансформація цього інституту в умовах переходу до ринкової економіки на основі нового Цивільного Кодексу від 16 січня 2003 року поставила ряд нових теоретичних та практичних питань, зокрема щодо юридичних підстав виникнення права приватної власності фізичних осіб [1]. Реформування цивільного та господарського законодавства викликало потребу в переосмисленні сутності та значення цілого ряду правових понять і категорій, зокрема категорії цивільно-правового договору, який є основним джерелом виникнення у громадян права приватної власності на майно, а в окремих випадках на інтелектуальну власність, інформацію та ін.

Важливість наукової розробки питань щодо значення та ролі цивільно-правових договорів у виникненні права приватної власності фізичних осіб обумовлена також процесами інтеграції нашої держави до Європейського та світового співтовариства, стратегії вступу України до СОТ і необхідністю врахування позитивного зарубіжного досвіду в цих питаннях. Успішність реалізації цих завдань на сучасному етапі суттєво залежить від того, наскільки цивільне законодавство України відповідатиме сучасним світовим тенденціям розвитку юриспруденції. Особливо це передусім стосується врахування ролі інформаційних суспільних відносин, стрімкого розвитку інформаційних технологій збору, формування, передавання, опрацювання, перетворення, захисту та зберігання інформаційних даних у сучасному постіндустріальному інформаційному суспільстві.

Аналіз останніх джерел. Сучасне суспільство стає інформаційним зростає роль інформації, інформаційних технологій і комп'ютерних знань, збільшується частка товарів у вигляді інформаційних продуктів та послуг, удосконалюється інформаційно-комунікаційна інфраструктура, формується глобальний світовий інформаційний простір. Інформація у сучасному суспільстві стала об'єктом права власності, і отже, об'єктом різних цивільно-правових правочинів. Інформація стала особливим товаром. В той же час в Україні законодавство про інформацію перебуває у стані свого становлення.

Професійний правознавець повинен знати, як можна застосувати інформаційні технології у своїй діяльності, які правові інформаційні системи вже створено, та які перспективи їх розвитку та застосування. Інформатизація суспільства ставить також нові проблеми правознавства та правового регулювання взаємодії суб'єктів суспільства. При цьому виникають нові види юриспруденції, такі як «право з інформаційних технологій», «комп'ютерне авторське право», право інтелектуальної власності та ін. [2, 3].

Юридичні питання електронного документообігу, користування мережею Internet, застосування криптографічних засобів і цифрової готівки, забезпечення таємниці та захисту даних – це сфера діяльності новітньо-кваліфікованих юристів, готових до перспективи розвитку та впровадження інформаційних технологій у всі сфери діяльності суспільства.

Сьогодні високорозвинені країни світу перебувають у стадії переходу до постіндустріальної фази свого розвитку – інформаційного суспільства, основою якого стане глобальна інформаційна інфраструктура.

Виходячи зі стратегічного курсу України на інтеграцію з Європейським Союзом і входження її у світовий інформаційний простір, Державний комітет зв'язку та інформатизації України визначив цю стратегію основним пріоритетним завданням. При цьому інфраструктура зв'язку та інформатизації на державному рівні повинні бути модернізовані та змінені відповідно до світових стандартів. Можна констатувати, що українська держава вже має достатній інтелектуальний, науково-технічний та правовий потенціал, щоб забезпечити процес та реформування даної галузі.

Однією з вирішальних умов забезпечення законності при використанні інформаційних технологій є формалізація правових норм, удосконалення методів моделювання та аналізу правової інформації. Вже виникає необхідність перейти від правозастосовних аспектів взаємодії комп'ютиризованих інформаційних систем та права до правотворчого аспекту, тобто пропозиції змін до діючого законодавства.

Тому глибоке дослідження характеристик юридичної інформації, в тому числі розробка теоретичних засад моделювання процесів правочину та подання юридичних знань є актуальною проблемою. Успішне вирішення цієї проблеми може суттєво впливати на досконаліть, оперативність та результативність формалізації юридичних законів, особливо комп'ютерно-інформаційному супроводженні взаємодії фізичних та юридичних осіб на основі відповідних інструментальних засобів експертної та телекомунікаційної техніки, а також прогресивних інформаційних технологій.

Методика досліджень. Інформатика належить до фундаментальних природничих наук, а поняття «інформація» стало загальнонауковим. Інформатика вивчає інформаційну складову соціальної комунікації, власне її змісту.

В той же час у конкретних галузях знань, наприклад юриспруденції, вивчення властивостей юридичних знань є актуальним і потребує глибокого системного підходу як найбільш фундаментального і перспективного. Очевидно, що правова інформатика може розвиватись, коли є можливість, крім професійних галузевих ідей і методів, ефективно використовувати інтеграційні процеси різних галузей знань і новітні результати інших, особливо формалізованих і математизованих дисциплін, системного аналізу, дослідження операцій, теорії інформації, моделювання, наукознавства та документалістики.

Постановка завдання. Важливим класом таких інформаційних систем в юридичній діяльності є сховища даних, бази знань та систем підтримки прийняття рішень (СППР). Особливістю СППР є інтерактивна взаємодія, що реагує як на регламентні, так і на непередбачені інфор-

маційні запити, зорієнтована на проблемно-орієнтований тип рішень або на множину взаємозв'язаних рішень. Причому успішне створення СППР стосовно правоохоронної діяльності можливе, як зазначено в, тільки в разі взаємодії математиків, юристів, практиків та фахівців з інформаційних технологій.

Світовий досвід застосування СППР в різних галузях юриспруденції показує, що одним з перспективних напрямків організації інтерактивної взаємодії юристів з базами знань є побудова інформаційних моделей взаємодії інтелектуальних суб'єктів права (ISP) шляхом формалізації підкласів моделей подання юридичних знань.

До класів таких моделей, які підлягають математичній формалізації та дослідженню належать:

- матричні моделі взаємодії фізичних та юридичних осіб;
- юридичні логіко-статистичні інформаційні моделі (ЮЛСІМ);
- системні моделі взаємодії суб'єктів правочину;
- продукційні часові моделі подання юридичних знань.

Матричні моделі взаємодії ISP. Теоретичною та методологічною основою побудови таких моделей є інформаційна технологія формалізації руху даних в комп'ютерних системах. На рис. 1 показані приклади формалізації та пояснення атрибутів матричної моделі взаємодії фізичних та юридичних суб'єктів, яка супроводжується рухом предметів приватної власності, в тому числі інформаційних юридичних даних.

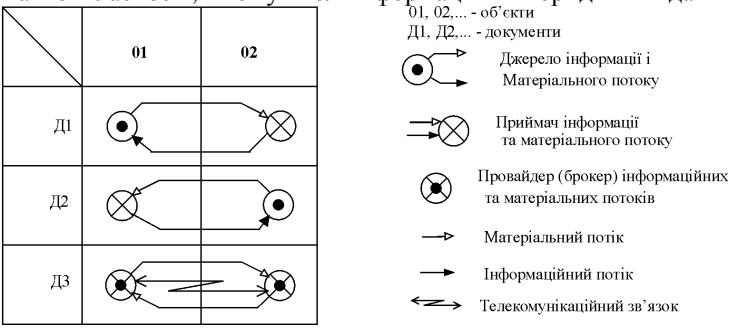

Рис. 1. Семантична матрична мережа моделі взаємодії суб'єктів ISP

Матрична модель взаємодії ISP характеризується обмеженими функціональними можливостями, оскільки не відображає диференціацію різних категорій суб'єктів приватної власності інформаційного суспільства, а також часові характеристики їх поведінки в умовах вступання та припинення дії.

Проблеми формалізації інформаційної взаємодії ISP з врахуванням завдань шифрування та стеганографічного захисту інформації. На сьогоднішній день у всіх сферах народного господарства спостерігається широкомасштабне впровадження розподілених комп'ютерних мереж та сучасних автоматизованих технологій обробки інформації з використанням провідних та безпровідних телекомунікаційних систем. При цьому широко використовується технологія реалізації цифрових підписів при дистанційному укладанні та веденні договорів між юридичними особами. Проблема захисту інформації від несанкціонованого доступу виникає внаслідок наступних причин загроз [4, 5]:

– перехоплення інформації з ліній зв'язку та перехоплення паролів;
– спроба проникнення в систему, створення чи заміна записів бази даних;
– несанкціоноване одержання та використання привілеїв, несанкціонований доступ до набору даних;
– встановлення неперевірених програм з вірусними пошкодженнями;
– використання вузлів в мережі або портів для проникнення в бази даних;
– атака на алгоритми та ключі цифрових підписів.

Остання причина загрози потребує досконалих механізмів шифрування, які забезпечують конфіденційність даних, що передаються. Розрізняють два способи шифрування: канальний та кінцевий. У разі канального шифрування захищається вся інформація, що передається каналами зв'язку, включаючи службову. Кінцеве шифрування дає можливість забезпечувати конфіденційність даних, що передаються між двома об'єктами. Механізми цифрового підпису, які містять процедури закриття блоків даних та перевірки закритого блоку даних дозволяють на основі відповідного таємного ключа сформувати масив даних, який може розшифрувати тільки певний користувач. Механізми автентифікації об'єктів мережі використовують паролі, перевірку характеристик об'єкта та криптографічні методи захисту цифрових підписів. Механізми засвідчення (арбітражу) дозволяють забезпечити юридичний захист даних та реалізують правові механізми користування даними.

Особливі методи захисту використовують в різних класах комп'ютерних мереж: якщо мережа централізована, то і захист реалізується централізовано, якщо мережа розподілена, то захист повинен бути розподілений.

Правові аспекти криптографічного захисту цифрового підпису

За кордоном найбільш відомими стандартами є такі.

1. DES (Data Encryption Algorithm). Введений в дію у 1977 р., блочний алгоритм з секретним ключем. Довжина ключа 56 біт.

2. RSA (Rivest, Shamir, Adleman). Криптосистема з відкритими ключами, опублікована в 1978 р. Швидкість роботи значно менша, ніж у DES, тому використовується спільно з більш швидкими алгоритмами. Ефективний для цифрового підпису.

3. MAA (Message Autentification Algorithm). Розроблений у Великій Британії стандарт для захисту цілісності даних. Використовується для захисту фінансових повідомлень від махінацій.

4. MAC (Код перевірки достовірності даних – Message Autentification Code). Використовується в банківських системах для підтвердження достовірності повідомлень спільно з MAA.

Призначення MAC полягає в доведенні, що під час передачі повідомлення воно не було замінене або підмінене навіть тією людиною, яка також має секретний ключ.

5. Стандарт криптографічного перетворення інформації (ГОСТ 28147-89) було введено в дію у Росії 3 липня 1990 року. Він визначає правила шифрування даних та виготовлення імітовставки. Це блочний алгоритм з секретним ключем. Довжина ключа 265 біт.

6. Стандарти цифрового підпису (ГОСТ Р34.10-94 і ГОСТ Р34.11-94). Стандарт установлює процедуру вироблення і перевірки повідомлень, що передаються по незахищених телекомунікаційних каналах загального користування в системах обробки інформації різного призначення, на базі асиметричного алгоритму з застосуванням функції хешування.

Ідентифікація цифрового підпису на основі різних алгоритмів

Існує ряд алгоритмів формування цифрових підписів, які забезпечують достовірність і конфіденційність відповідних повідомлень, в тому числі :

– алгоритм SIGN, який, використовуючи повідомлення M і таємний ключ KA1, створює деяке слово $S = \mathrm{SIGN}(M, KA1)$, яке називається підписом абонента A у повідомленні M. У випадку, коли абонент A хоче послати повідомлення M з завіренням того, що воно послано тільки ним, то він дистанційно передає пару (M, S);

– алгоритм підпису CHECK, в якому перевірка ідентичності підпису виконується за умовою $\mathrm{CHECK}(M,S,KA) = 1$, де KA – відкритий ключ;

– алгоритм підпису системи RSA, в якому кожний абонент володіє парою ключів: відкритий – числа **n** і **e** і таємний ключ – число **d**.

Процес підписування двох абонентів А і В відбувається наступним чином:

1. А посилає В повідомлення $C = eB[dA(M)]$;
2. Абонент В читає повідомлення $M = eA[dB(C)]$.

Коректність даної системи цифрового підпису забезпечується виконанням відношення

$$eA\,[dB(C)] = eA\,[dB(eB(dA(M)))] = eA\,[dA(M)],$$

де М – ім'я підпису.

Вказане співвідношення можна записати у розгорнутому виді:

$$(M\text{^}eA)\text{^}dA \bmod n\ A = (M\text{^}dA)\text{^}eA \bmod n\ A = M;$$

$$(M\text{^}eB)\text{^}dB \bmod n\ B = (M\text{^}dB)\text{^}eB \bmod n\ B = M.$$

Алгоритм RSA забезпечує високу надійність та конфіденційність цифрового підпису. Найбільш широкого застосування на практиці отримала система цифрового підпису, розроблена в 1991 році DSA (Digital Signature Algorithm), яку часто називають DSS (Digital Signature Standart).

В основу алгоритму DSA покладена процедура:

1. Вибирається випадкове число $r(0 < r < q - 1)$, обчислюється $r1 = r1(-1) \bmod q$;
2. Визначається $S1 = (h1r \bmod P) \bmod q$, визначається $S2 = (r1 * (f(M) + a * fS1)) \bmod q$;
3. Підпис формулюється як пара чисел: $S = (S1, S2)$.

Символ * – ознака вкорочуючої функції довжиною 160 біт.

При цьому вибирається велике просте число Р таке, що Р-1 має дільник q. Потім вибирається число h, порядок якого співпадає з порядком числа q. Числа p, q, h – не є таємні і колективно використовуються абонентами в телекомунікаційній мережі. Щоб отримати відкритий і таємний ключі абонент А вибирає випадкове таємне число а і обчислює відкрите число $b = (h\text{^}a) \bmod P$.

Особливості захисту інформації в сучасних хмарних та телекомунікаційних системах. Важливим новим аспектом юридичних відносин в інформаційному суспільстві є правова інформація проблеми, пов'язаної із захистом інтелектуальної власності та атаками несанкціонованого доступу до даних.

Діючим захистом від атак на інформаційні комунікаційні системи є маскування файлу передавання інформації методом стеганографії та шифрування цифрового підпису [5]. У безпровідних комп'ютерних мережах для такого захисту використовується 128-бітне AES шифрування. Для захисту інформації в мережах (WLAN) на MAC – рівні передбачений механізм захисту даних, який містить аутентифікацію абонентських станцій, суб'єктів права та шифрування інформації згідно алгоритмів WEP, WPA, та WPA2 (захищений доступ до Wi-Fi).

У загальнодоступних хмарних комп'ютерних мережах суттєву загрозу складає людина – суб'єкт права, яка здійснює неавторизований і несанкціонований доступ до даних. З метою протидії такому несанкціонованому доступу застосовується взаємна аутентифікація між двома інтелектуальними суб'єктами права (ISP). Тобто особливу небезпеку при цьому здійснює «людина посередник» (man-in the middle attacks) [5], яка використовує протокол перекодування адресів (Adress resolution protocol, ARP).

Класифікація та формалізація комунікаційних процесів юридичної взаємодії ISP. В роботі [6] запропонована наступна класифікація суб'єктів приватного права (рис. 2), де взаємодію дев'яти об'єктів можна однозначно описати 9x9=81 бінарною парою матриці взаємодії.

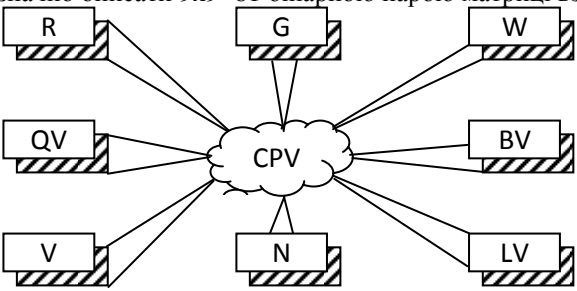

Рис. 2. Системні об'єкти руху власності: R – відчужувач; G – створювач; W – набувач; QV – користувач; CPV – перевізник; BV – зберігач; V – об'єкт власності; LV – ліквідатор; N – реєстратор

Аналіз моделей такого класу показує, що вони характеризуються функціональними обмеженнями, оскільки не враховують характеристик нейромоделі ISP та його взаємодії з іншими суб'єктами права.

Інформаційна нейромодель ISP формується на принципах групування зовнішніх впливів по ознаках системної єдності та охоплення різних класів такої сукупності інформаційно-впливових груп і показана на рис. 3.

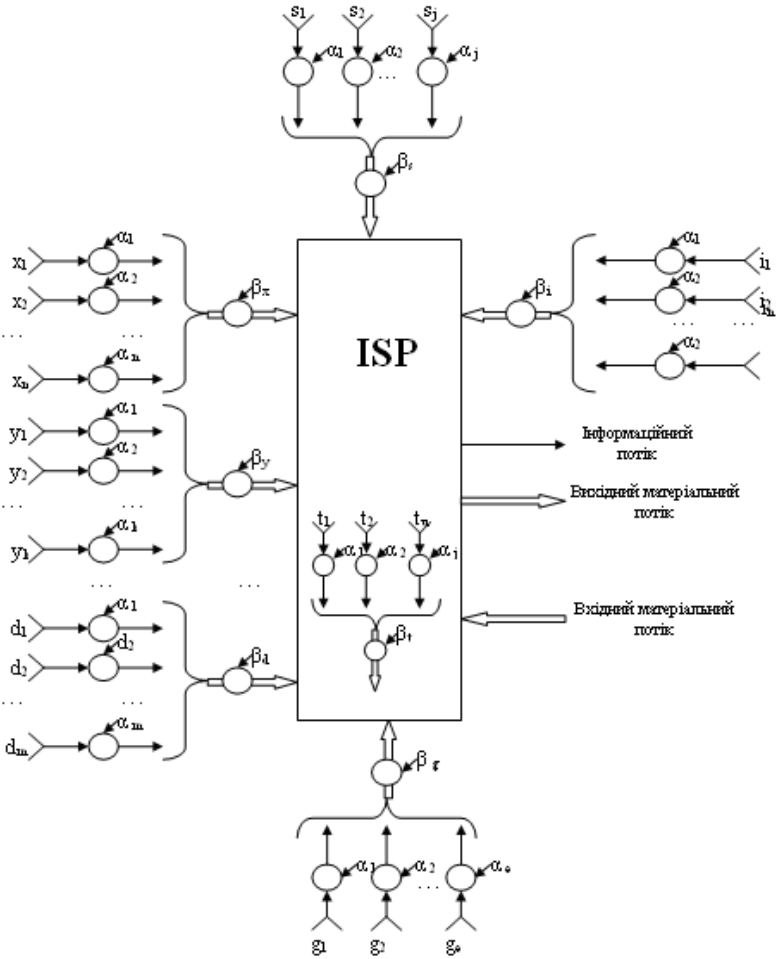

Рис. 3. Інформаційна нейромодель суб'єкта права

На основі групування зовнішніх впливів та теорії формальних нейронів побудована модель суб'єкта права, яка показана на рис. 4.

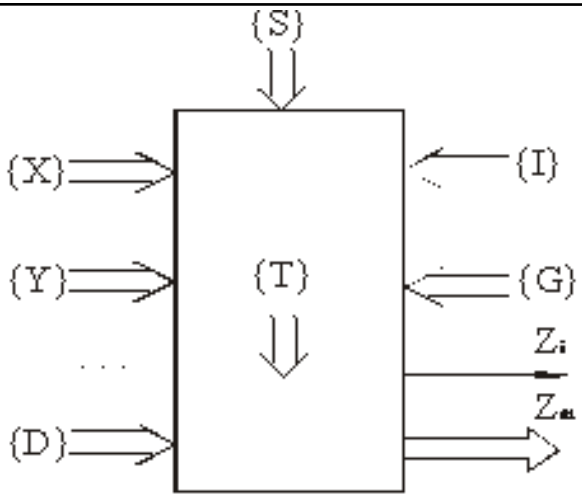

Рис. 4. Модель суб'єкта права

На рис. 3, 4 застосовані наступні атрибути зовнішніх комунікаційних зв'язків:

X – хаотичні впливи та взаємодії;

Y – управлінські та законодавчі впливи;

D – доцільні взаємодії з навколишнім середовищем;

I – інформаційні зовнішні впливи;

S – функція страху, оцінка результатів своєї реакції на зовнішні впливи;

G – життєві фактори виживання;

T – таємна інформація, яка несвідомо або цілеспрямовано не відображається у вихідних інформаційних чи матеріальних потоках;

Z_i, Z_m – реакція у вигляді відповідних інформаційних та матеріальних потоків.

Розроблена **повнофункціональна модель взаємодії ISP** з іншими категоріями суб'єктів права в умовах становлення сучасного інформаційного суспільства, яка враховує сучасні хмарні IT-технології та умови захисту інформації на основі стеганографії та шифрування показана на рис. 5.

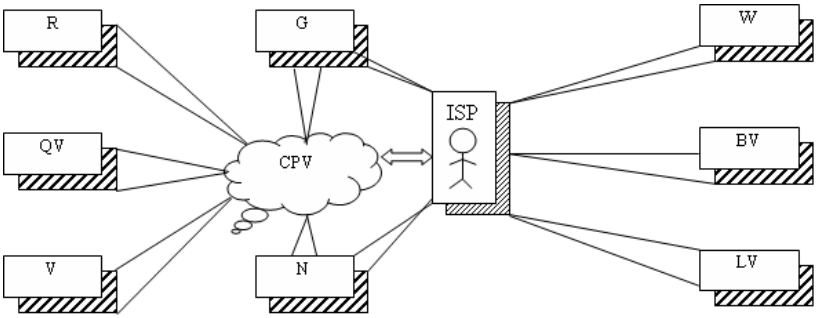

Рис. 5. Системні об'єкти руху власності

Висновки. Таким чином, сучасні телекомунікаційні та комп'ютерні системи володіють всіма алгоритмічними та технічними можливостями реалізації дистанційних процедур укладання та ведення угод як моменту виникнення права власності з використанням цифрового підпису та захисту даних від несанкціонованого доступу.

1. Луць В. В. Контракти у підприємницькій діяльності / В. В. Луць. – К. : Юрінком Інтер, 1999. – 560 с. **2.** Шишка Р. Б. Охорона права інтелектуальної власності: авторсько-правовий аспект / Р. Б. Шишка. – Харків : Видавництво національного університету внутрішніх справ. – 2002. – 368 с. **3.** Николайчук Л. М. Теоретичні основи юриспруденції приватної власності в контексті системних об'єктів комп'ютерних мереж / Л. М. Николайчук // Вісник Хмельницького національного університету. – № 4, – Ч. 1, – Т. 2. – 2005. – С. 56-58. **4.** Николайчук Я. М. Теорія джерел інформації / Николайчук Я. М. – Тернопіль : ТНЕУ, 2008. – 536 с. **5.** Задірака В. Методи захисту фінансової інформації / Задірака В., Олексюк О. – К. : Вища школа, 2000. – 458 с. **7.** Николайчук Л. М. Формалізація норм та часових характеристик юридичних законів на основі логіко-статистичних інформаційних моделей // Збірник наукових праць. – НАН України Інститут проблем проблем моделювання в енергетиці ім. Г. Є. Пухова. – Вип. 38. – Київ, 2006. – С. 44-50.

Рецензент: д.т.н., професор Березький О. М. (Тернопільський національний економічний університет)

Nykolaychuk L. M., Candidate of Juridical Sciences, Associate Professor (Ivano-Frankivsk National Technical University of Oil and Gas), **Nykolaychuk Y. M., Doctor of Engineering, Professor** (Ternopil National Economic University)

INFORMATION MODEL OF INTERACTION OF LAW ON THE BASIS OF STEGANOGRAPHY AND ENCRYPTION

The methodology of constructing models of interaction of law in today's information society. A new model of interaction intellectual ten subjects of law.
***Keywords*: information model, law, a digital signature.**

Николайчук Л. М., к.ю.н., доцент (Ивано-Франковский национальный технический университет нефти и газа),
Николайчук Я. М., д.т.н., профессор (Тернопольский национальный экономический университет)

ИНФОРМАЦИОННАЯ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ ПРАВА НА ОСНОВЕ СТЕГАНОГРАФИИ И ШИФРОВАНИЯ

Изложена методология построения моделей взаимодействия субъектов права в условиях современного информационного общества. Предложена новая модель взаимодействия десяти интелектувальних субъектов права.
***Ключевые слова*: информационные модели, юриспруденция, цифровая подпись.**
