МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет імені М. Є. Жуковського
«Харківський авіаційний інститут»

С. Ф. Гуцу, А. В. Матвєєва, Г. О. Спіцина,
А. А. Стародубцев, Н. Є. Філіпенко, Н. А. Федосенко

ІТ-ПРАВО

Навчальний посібник

Харків
«ХАІ»
«Факт»
2022

УДК 347.772.3
Г 93

Рекомендовано до друку Вченою радою
Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авіаційний інститут»,
протокол № 1 від 25 серпня 2022 року

Рецензенти:

ЛУК'ЯНОВ Дмитро Васильович, доктор юридичних наук,
член-кореспондент Національної академії правових наук України,
завідувач кафедри міжнародного приватного права
та порівняльного правознавства
Національного юридичного університету імені Ярослава Мудрого

МОЖАЄВ Михайло Олександрович, доктор технічних наук,
завідувач сектору судово-експертної діяльності відділення-бюро
у м. Києві Національного наукового центру «Інститут судових
експертиз ім. Засл. проф. М. С. Бокаріуса»

Гуцу С. Ф., Матвєєва А. В., Спіцина Г. О. та ін.

Г 93 ІТ-право : навч. посіб. – Харків : Нац. аерокосм. ун-т
імені М. Є. Жуковського «Харків. авіац. ін-т»; «Факт»,
2022. – 220 с.
ISBN 978-617-8072-53-7

У посібнику досліджено основи правового регулювання цифрових відносин, охарактеризовано особливості правового статусу суб'єктів та об'єктів цих відносин, особливості правової охорони прав та інтересів у цифровому середовищі. Видання містить аналіз національного, європейського і міжнародного законодавства, судової практики та наукових поглядів на суть ІТ-відносин та інші питання впорядкування ІТ-сфери.

Посібник буде корисним для викладачів дисципліни «ІТ-право», аспірантів та студентів закладів вищої освіти, що вивчають курс «ІТ-право».

УДК 347.772.3

ISBN 978-617-8072-53-7

ЗМІСТ

РОЗДІЛ 11.
ПРАКТИЧНІ ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

ПЕРЕДМОВА

Сучасний світ переживає четверту промислову революцію, характерними рисами якої є побудова глобального цифрового світу. Стрімкий розвиток інноваційних технологій, що характеризує новий етап технічної революції тягне за собою зміни у правовій системі окремих держав і міжнародному праві. ІТ-право фактично супроводжує процес стрімкого технологічного розвитку, який відбувається з кінця XX та на початку XXI століття і пов'язаний з фазою швидкого зростання п'ятого технологічного укладу. Основним його ядром стають інформаційні та телекомунікаційні технології, робототехніка і програмне забезпечення. Найбільше зростання у світі демонструють сегменти програмного забезпечення, ІТ-послуг та Big Data [1]. Вважається, що початком оформлення в нашій державі цієї галузі права було прийняття низки законних та підзаконних нормативно-правових актів, зокрема таких законів України, як: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис».

Стрімкі темпи глобалізації світу, інформатизація всіх сфер функціонування суспільства і людини породжує створення нової реальності і якості життя. Інформаційні системи різних держав інтегруються до єдиної світової інформаційної системи, породжуючи єдиний інформаційний простір без кордонів, межі контролю. І в цьому світі істотно посилився вплив засобів масової комунікації. Створені на основі сучасних інформаційно-комунікаційних технологій та відповідного програмного забезпечення вони перетворюються в ефективні засоби інформаційно-психологічного впливу як на особистість, так і суспільні утворення. Ці засоби є невід'ємним компонентом так званого віртуального простору, або віртуальної реальності. Питання

необхідності й доцільності регулювання мережі Інтернет і відносин, що виникають з її допомогою неможливе без усвідомлення їх специфіки й неоднорідності. Інтернет це досить особливе середовище, що є віддзеркаленням сучасного розвитку суспільства, економіки, техніки. Це поєднання комунікативних відносин між офіційними установами й тими, що не визнають державних кордонів і юрисдикції; окремими особами і суспільними групами; підприємцями та споживачами.

Одним з важливих напрямів розвитку ІТ-права стала кібербезпека. На тлі інформаційних протистоянь, питання захисту національної безпеки нашої держави від кібернетичних атак стало рушійним для законодавчої діяльності. Наразі цю сферу врегульовано Указом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» від 15 березня 2016 року, Конвенцією про кіберзлочинність, законами України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 року та «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 [2], Кримінальним кодексом України (Розділ XVI) та іншими.

Про розвиток ІТ-права в Україні свідчать і останні законотворчі ініціативи. Так, 15.07.2021 року Верховною Радою України прийнято Закон «Про стимулювання розвитку цифрової економіки в Україні» [3].

У підготовці навчального посібника брали участь: кандидат юридичних наук, доцент С. Ф. Гуцу (Розділи 1-4, 7, 8, 9), доктор юридичних наук, професор Г. О. Спіцина (розділ 7, 11), доктор юридичних наук, доцент Н. Є. Філіпенко (розділ 10), доктор юридичних наук, доцент А. А. Стародубцев (розділ 10), кандидат юридичних наук, доцент А. В. Матвєєва (розділ 6), кандидат юридичних наук, доцент Н. А. Федосенко (розділ 5).

РОЗДІЛ 1.

ІТ-ПРАВО ЯК НОВА ПРАВОВА КАТЕГОРІЯ

У сучасному світі розвиток технологій є настільки стрімким, що певні терміни та поняття у практичному обороті виникають набагато раніше ніж в законодавстві. Свого часу цей шлях пройшло Інформаційне право, що на сьогодні вже має своє місце у правовій системі і з яким часто ототожнюють ІТ-право. Ще декілька років тому терміни «Інформаційне право», «Інтернет-право», «ІТ-право» для багатьох науковців і практиків мали характер синонімів. Крім того, зустрічаються і такі поняття, як: «комп'ютерне право», «програмне право», «цифрове право» тощо. Все це вносить непорозуміння і хаос у процес тлумачення і застосування правових норм. Сьогодні маємо низку наукових доробок з цієї теми, що доводять різницю, визначають суть і співвідношення зазначених понять.

Інформаційне право у XX ст. виникло як реакція на визнання інформації основним ресурсом нової економіки. В сучасному правовому світі воно має доволі сформований вигляд і є загальновизнаною галуззю права. Неодноразово підіймалося питання про впровадження Інформаційного Кодексу в національне законодавство. Суть ІТ-права, його структура, предмет і, навіть, саме існування як явища досі є предметом наукової дискусії. Існує навіть позиція, що ІТ-право це більш сучасна назва Інформаційного права. З такою точкою зору не можна погодитись. Так, О. Е. Сімсон вважає, що різниця між інформаційним та ІТ-правом не є суто термінологічним різночитанням, а стосується **змісту** відносин. Інформаційне право є більш широкою категорією за сферою правого регулювання. Воно регулює відносини, пов'язані з реалізацією конституційного права людини на інформацію і свободу інформації, відносини у сфері ЗМІ та інформаційні права їх учасників, цивільні

відносини охорони та захисту особистих немайнових інформаційних прав фізичних та юридичних осіб, відносини у сфері паперової інформації (архіви та бібліотеки), загальні питання правових режимів інформації, захисту прайвесі та персональних даних тощо. Відмінністю інформаційного права стосовно ІТ-права є потужний пласт публічно-правових відносин, таких як система управління інформацією в державі, цензура, доступ до публічної інформації, електронне управління або е-врядування та система електронних публічних сервісів (адміністративних послуг), електронна участь та електронні вибори, захист інформації у кіберпросторі та боротьба з кіберзлочинами, кібербезпека загалом тощо [4].

ІТ-право вчений визначає як галузь права, предметом якої виступають відносини у цифровому середовищі, а саме відносини з приводу створення, зберігання, передачі та захисту інформації в електронному вигляді, обробка якої відбувається з використанням інформаційних технологій у глобальних та локальних інформаційних системах.

Своєю чергою О. І. Харітонова надає наступне визначення ІТ-праву: «це сукупність норм і правил, що опосередковують діяльність по забезпеченню безпеки інформаційних технологій та інформаційної активності в мережі Інтернет» [5].

Професорка О. С. Яворська вважає, що ІТ-право — це комплексна галузь права, що регулює відносини у цифровому середовищі [6].

У чому тоді полягає відмінність категорій «ІТ-право» і «Інтернет-право»? Інтернет-право являє собою комплексний правовий інститут — сукупність правових норм, націлених на розв'язання системних правових проблем суспільних відносин, що виникають у зв'язку і з приводу інформаційно-телекомунікаційної мережі Інтернет, що і складає предметну єдність Інтернет-права.

Своєю чергою професор Є. О. Харитонов розглядає Інтернет-право у широкому та вузькому значенні. Під «Інтернет-правом» у широкому значенні пропонується розуміти всю сукупність норм і правил, які стосуються

інформаційно-комунікаційної активності в Інтернеті. Його структура виглядає як достатньо інтегрована система багаторівневого порядку, що включає приватноправові та публічно-правові елементи. Під «Інтернет-правом» у вузькому значенні розуміють лише ті правові норми, що стосуються правомірної (у тому числі «юридично-байдужої») діяльності в мережі передусім регулятивні норми (переважно — цивільно-правові), що забезпечують функціонування «Інтернет-відносин» [7].

Відповідно «Інтернет-відносини», визначають як частину відносин у віртуальному просторі, що є лише частиною більш загальної категорії «ІТ-відносини», під якими науковці розуміють всю сукупність суспільних відносин, що виникають у процесі (в результаті) створення і використання інформаційних технологій. Отже, «ІТ-відносини» є загальною категорією, що охоплює також і відносини, які складаються в Інтернет. Разом із тим, останні можуть і не бути «інформаційними», у точному значенні цього слова. Так, до сфери «ІТ-права» відносять відносини надання послуг програмного забезпечення або його розробки; правового захисту web-сторінок і контенту; юридичної допомоги у відкритті ІТ-бізнесу; юридичного аудиту ІТ-компаній тощо. Таким чином, категорія «ІТ-право» є ширшою, ніж «Інтернет-право», оскільки стосується також відносин, що складаються поза Мережею.

Наразі постає принципове питання: чи можна вважати ІТ-право галуззю права? Для відповіді на це питання, згадаємо, що з точки зору правової доктрини, для виокремлення галузі у правовій системі має значення наявність власного предмета, методу, принципів правового регулювання, правового режиму тощо.

Предмет регулювання — це той елемент, що повинен мати певні особливості для кожної галузі права. Адже будь-які зусилля зі створення нової галузі права не можуть завершитися успішно, якщо предметом регулювання слугують різнорідні відносини. Отже, і «ІТ-відносини» повинні мати цілісний предмет правового регулювання, а

також певні прийоми і методи впливу на нього правових норм.

У науковій літературі зазначається, що в ІТ-праві відсутній єдиний предмет правового регулювання, оскільки, фактично, йдеться не про «ІТ-відносини», а про відносини, що пов'язані зі сферою інформаційних технологій або суміжними сферами. Такі відносини є різнорідними та за своїм змістом можуть бути цивільними, адміністративними, фінансовими, корпоративними тощо.

Також дуже складно віднайти єдиний метод правового регулювання ІТ-відносин, в якому було б відображено засади, властиві відповідній галузі. Нагадаємо, що метод правового регулювання є одним з основних критеріїв виокремлення галузі права, під яким розуміють сукупність специфічних прийомів юридичного впливу на учасників суспільних відносин у певній сфері буття суспільства. Науковці Є. Харитонов і О. Харитонова вважають, що: «Оскільки до ІТ-сфери належать відносини, які за своєю сутністю є соціальними зв'язками «по горизонталі» та «по вертикалі», природним убачається те, що для їхнього впорядкування використовують як диспозитивний, так і імперативний методи. Ця обставина дає підстави для висновку про відсутність єдиного методу правового регулювання відносин в ІТ-сфері. Натомість залежно від типу відносин, що регулюються, і конкретних завдань може застосовуватися цивільно-правовий чи адміністративно-правовий метод». Виходячи з цього робиться висновок про те, що з позицій нормативістського праворозуміння галузі ІТ-права (так само й Інтернет-права, інформаційного права як галузей права) не існує [8].

З усього вище сказаного можна зробити висновок, що ІТ-право ще не сформовано як система правових норм. Воно не має ознак, за якими правова наука виокремлює окремі самостійні галузі й правові інститути. Коли ми говоримо про ІТ-відносини, ми маємо на увазі специфіку функціонування певних суспільних відносин в цифровому середовищі й, відповідно, специфіку застосування юридичних норм у цій сфері. Але правова наука постійно розвивається і змінюється підлаштовуючись під потреби

цифрового суспільства. Наприклад, чинним законодавством не регулюються відносини за участю роботів та автоматичних систем управління, Інтернету речей, віртуальної реальності тощо. А потреба в цьому величезна, бо наявність цих елементів економіки визначає конкурентоспроможність підприємств і країни. Тому так активно формуються доктринальні підходи до права інформаційних технологій, яке фактично супроводжує процес стрімкого технологічного розвитку сучасної економіки і суспільства. Тому ІТ-право має бути визначено і виокремлено в самостійний правовий інститут.

Запитання для самоконтролю і самостійного опрацювання:

1. Яка позиція науковців щодо визначення місця ІТ-права у правовій системі України?
2. Як співвідносяться поняття «ІТ-право», «Інтернет-право», «Інформаційне право»?
3. Визначте юридичну природу ІТ-права.
4. Назвіть основні джерела ІТ-права.
5. Який, на вашу думку, державний орган в Україні має повноваження щодо розвитку інформатизації та регулювання ІТ-відносин в Україні? Обґрунтуйте свою позицію.

Рекомендована література:

1. Основи ІТ-права : навч. посіб. / Т. В. Бачинський, Р. І. Радейко, О. І. Харитонова. — Київ : Юрінком Інтер, 2021. — 244 с.
2. ІТ-сфера в Україні. Законодавство. Судова практика. Коментар / Бачинський Т. В. — Київ : Юрінком Інтер, 2018. — 360 с.
3. ІТ-право: теорія та практика : навч. посіб. / Харитонов Є. О., Харитонова О. І. — Одеса : Фенікс, 2017. — 472 с.
4. ІТ-право: поняття та сутність : монографія / За ред. д.ю.н., проф. О. І. Харитонової, д.ю.н. проф. Харитонова Є. О. — Одеса : Фенікс, 2017. — 316 с.

РОЗДІЛ 2.

ПРАВОВЕ РЕГУЛЮВАННЯ МЕРЕЖІ ІНТЕРНЕТ

2.1. Визначення поняття «Інтернет»

Сьогодні у світі існує безліч локальних і декілька глобальних (INTERNET, Bitnet, DECnet та інші) комп'ютерних мереж. Мережа Інтернет це найбільша і найпопулярніша глобальна комп'ютерна мережа. За даними Міжнародного союзу електрозв'язку при ООН, кількість користувачів Інтернету зросла з 25,8% населення Землі у 2009 році до 53,6% у 2019-му і складала 4,1 мільярда людей у світі. До початку 2021 року їхня кількість збільшилася ще на 280 млн користувачів. Кількість українських Інтернет-користувачів, за даними компанії GlobalLogic, також зросла на 2 млн у 2020 році, що на 33% більше, ніж у 2019 році, і на початку 2021-го становила майже 30 млн осіб, тобто приблизно 67% населення країни [9]. Отже, саме ця комп'ютерна мережа як об'єкт правового регулювання представляє інтерес для законодавців, фахівців-практиків і науковців.

Як ми вже зазначали у попередній темі, Інтернет відносини є частиною ІТ відносин. Вони виникають, розвиваються і здійснюються у віртуальному (цифровому) середовищі. Отже, поняття «цифрове середовище» і «мережа Інтернет» не є тотожними. Як зазначає Л. Л. Тарасенко, цифрове середовище – це ширше поняття, ніж мережа Інтернет. Цифрове середовище включає у себе не лише веб-сайти (і веб-сторінки як складові веб-сайтів), а й електронні документи, файли, в тому числі оцифровані об'єкти інтелектуальної власності, які використовуються на відповідних пристроях, що не передбачають паперової форми документообігу (комп'ютери, ноутбуки, планшети, телефони, інші види так званих «гаджетів») [6].

Визначення поняття «цифрове середовище» у чинному законодавстві України не наводиться. Але у Проєкті Національної стратегії захисту дітей в цифровому середовищі на 2021 – 2026 роки, що запропонована Міністерством цифрової трансформації, під поняттям «**Цифрове середовище**» розуміється таке, що охоплює інформаційно-комунікаційні технології (ІКТ), включаючи Інтернет, мобільні та пов'язані з ними технології та пристрої, а також цифрові мережі, бази даних, контент та послуги [10].

Отже, надалі будемо говорити про мережу Інтернет як складову частину цифрового середовища (простору).

Глобальна комп'ютерна мережа Інтернет існує понад 50 років, але досі в міжнародному праві та національному законодавстві не має єдиного розуміння і підходів до визначення поняття «Інтернет». В науковій літературі також існують різні підходи й позиції щодо розуміння його природи. Отже, і предмет регулювання є досить розпливчастим і неоднорідним. Наприклад, в одних випадках Інтернет визначається як інформаційна, комп'ютерна або телекомунікаційна мережа, в інших інформаційний, віртуальний простір або середовище.

Так, С. В. Петровський сформулював поняття Інтернету як міжнародної мережі електрозв'язку загального користування, призначеної для обміну повідомленнями (даними), тобто відомостями про навколишній світ, його об'єкти, процеси і явища, що об'єктивувалися у формі, яка дозволяє провести їх безпосередню машинну обробку. Іншими словами, Інтернет є міжнародною телекомунікаційною мережею загального користування [11].

А. А. Тедєєв вважає, що Інтернет – це «електронна комунікаційна мережа, що зв'язує комп'ютери в усьому світі через телефонні лінії й кабелі з оптичних волокон» [12]. І. В. Невзоров визначив Інтернет як здійснюване з використанням електрозв'язку для передачі закодованої інформації з'єднання максимального (найбільшого) на конкретний момент часу числа електронно-обчислювальних машин (ЕОМ). К. С. Шахбазян визначає

поняття мережі Інтернет для міжнародного права як міжнародної телекомунікаційної мережі загального користування, призначеної для обміну повідомленнями (даними), яка є комплексним предметом правового регулювання різноманітних суспільних відносин в єдиній системі, що існує завдяки глобальній комп'ютерній мережі і призначена для обміну даними, які зчитуються машиною та представлені у вигляді, зрозумілому для людини.

Своєю чергою К. В. Єфремова визначає Інтернет як глобальний інформаційний простір, який не визнає державних кордонів, що робить цю систему якісно новим явищем у світовій спільноті, він є унікальним за своїми можливостями засобом доступу до інформації щодо будь-яких видів діяльності чи інтересів людини, а також виступає об'єктом розробки й застосування новітніх програмних та інструментальних технологій, що робить його сферою бурхливого розвитку в майбутньому [13].

Одне із *законодавчих* визначень поняття «Інтернет» сформульовано в Законі США 1998 р. Про інтерактивну безпеку дітей (Children's Online Privacy Protection Act). Відповідно до норм цього закону **Інтернет** є об'єднанням безлічі комп'ютерів і телекомунікаційних засобів, включаючи устаткування і програмне забезпечення, що утворюють пов'язану міжнародну мережу мереж, яка ґрунтується на протоколі міжмережевої взаємодії. У Законі України «Про електронні комунікації» [14] надано таке визначення **Інтернету**: це глобальна електронна комунікаційна мережа, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами.

Отже, бачимо, що в основу визначення терміну «Інтернет» покладено технічний і соціальний критерії. Майже так саме в літературі та законодавстві розділяють і об'єкти правового регулювання мережі Інтернет: 1) технічне регулювання, пов'язане з визначенням основних принципів та параметрів роботи мережі; 2)

регулювання відносин, що виникають при використанні Інтернет в діяльності фізичних та юридичних осіб.

2.1. Історія виникнення і розвитку мережі Інтернет

Четвертого жовтня 1957 року Радянський Союз успішно запустив перший штучний супутник на орбіту Землі. Ця подія безпосередньо призвела до того, що в 1969 році за ініціативою Пентагона було створено Агентство передових дослідницьких проектів Міністерства оборони США – DARPA (Department of Defence ARPA – Advanced Research Projects Agency). Перед американськими науковцями поставили нелегке завдання: створити комп'ютерну мережу, якою могли б користуватися військові під час ядерного нападу на країну. Мережа мала забезпечувати зв'язок між командними пунктами системи оборони США. Головним критерієм мережі мала бути її захищеність у разі ядерної атаки. Навіть за руйнації деяких гілок і вузлів повідомлення повинні були потрапляти до адресата. Єдиним способом формування такої комп'ютерної мережі було особливе з'єднання комп'ютерів, за якого комунікація не залежала б від центрального сервера. У разі втрати одного, кількох чи навіть багатьох комп'ютерів підсистеми повинні були працювати, гарантуючи можливість удару у відповідь.

З жовтня до грудня 1969 року відбулося об'єднання в одну комп'ютерних мереж чотирьох університетських центрів США – Каліфорнійського університету Лос-Анджелеса, Каліфорнійського університету Санта-Барбари, Стенфордського дослідницького інституту й Університету штату Юта. Спроба встановлення першого зв'язку через мережу була проведена 29 жовтня 1969 року. Чарлі Клайн з Каліфорнійського університету (р. Лос-Анджелес) пробував віддалено під'єднатися до ПК, що знаходиться на відстані 640 км у Стенфордському дослідницькому інституті, де Білл Дювалль в телефонному режимі підтверджував успішну трансляцію кожного символу. Однак з п'яти знаків слова «LOGON», яке було

спеціальною командою авторизації в системі, з першої спроби вдалося передати лише перші три знаки – «LOG», після цього в мережі стався збій. Однак після повернення ARPANET в робочий стан через кілька годин (біля половини на одинадцяту вечора) наступна спроба вчених встановити зв'язок на відстані увінчалася успіхом. Дата **22 жовтня 1969 р.** може по праву вважатися датою появи першого в світі Інтернету, основою для якого стала мережа ARPANET.

Після ARPANET у США та інших країнах створювалися комп'ютерні мережі, що з'єднували комп'ютерні центри наукових і державних організацій. Багато мереж стали використовувати протокол IP. Цей протокол був зручний тим, що можна було легко нарощувати мережу, приєднуючи скільки завгодно нових комп'ютерів. Але, крім IP-мереж, створювалися мережі, що працювали за іншими мережевими протоколами.

В 1972 році у Вашингтоні відбулася перша Міжнародна конференція комп'ютерних комунікацій**.** У конференції брали участь науковці з десяти країн. Учасникам конференції вперше в історії продемонстрували мережу ARPANET, вона перестала бути секретною розробкою. У тому ж 1972 р. було представлено первинне доповнення – електронну пошту. З цієї миті почалася епоха електронної пошти, що стало передвісником тієї «всесвітньої павутини», яку ми бачимо сьогодні, а саме стрімкого зростання усіх видів трафіку між людьми.

Після об'єднання в 1982 році двох протоколів TCP і IP в один протокол TCP/IP став стандартним протоколом об'єднаної мережі Інтернет. У цьому ж році з'явився термін «**Інтернет**».

Наступним етапом була розробка системи доменних імен (англ. Domain Name System, DNS), яка відбулася в 1984 році. Також в цьому році з'являється серйозний конкурент мережі ARPANET – Міжуніверситетська мережа NSFNet (англ. National Science Foundation Network). Ця мережа була об'єднанням безлічі дрібних мереж, мала пропускну здатність набагато більшу, ніж в

ARPANET, і більш високу динаміку підключення нових користувачів (близько 10 тисяч машин на рік). Отже, звання «Інтернет» перейшло до NSFNet.

У 1988 році був анонсований протокол миттєвої передачі текстових повідомлень Internet Relay Chat (IRC), внаслідок цього в Інтернеті стало можливим «живе» спілкування в чаті в реальному часі.

У 1989 році знаменитий британський вчений Тім Бернерс-Лі пропонує концепцію Всесвітньої павутини. Він так само за два наступні роки розробляє протокол HTTP, мову гіпертекстової розмітки HTML і ідентифікатори URI.

У 1990 році мережа ARPANET, програвши в конкурентній боротьбі NSFNet, припиняє своє існування. Так само в цьому році відбулося перше підключення до мережі Інтернет по телефонній лінії (Dialup access — «дозвін»).

У нашій країні роком впровадження Інтернету прийнято вважати 1990 рік, коли програміст київського наукового центру Технософт Юрій Янковський вперше під'єднався до вже наявної глобальної мережі. Надалі компанія Янковського стала першим Інтернет-провайдером України, після чого почалося підключення міст — спочатку Харків, потім інші. У 1991-1992 роках після переговорів з адміністрацією адресного простору павутини IANA Україна отримала власний домен **.ua**, що породило появу цілої низки нових провайдерів. Потужним поштовхом для розвитку вітчизняної павутини стала поява у 2008 році на ринку технологій оптоволокна. Як наслідок, сучасний Інтернет в Україні мало чим поступається світовому.

2.1. Регулювання мережі Інтернет

Питання необхідності й меж регулювання мережі Інтернет і відносин, які відбуваються за її допомогою постійно стають темою наукових і громадських диспутів. З одного боку говорять про неможливість правового регулювання Інтернет, про те, що фактично сама мережа створювалася для вільного доступу та спілкування без

правових обмежень, а основні правила поведінки в Інтернет встановлюються самими учасниками цих суспільних відносин. Тобто йдеться про самокеровану систему, яка має виключно внутрішні правила поведінки, прописані у різних кодексах поведінки, правилах користування тощо. З іншого боку Інтернет вже давно перетворився на альтернативне цифрове відображення матеріального світу якому властиві майже усі форми прояву економічних і суспільних зв'язків. А тому необхідність в державному регулюванні цих відносин важко заперечити. Як, влучно зазначив А. М. Новицький: «У більшості країн світу мережа Інтернет розвивалась академічними спільнотами, які розробляли та використовували внутрішні регулятивні інструменти. Досить незначне поширення та чіткі внутрішні правила поведінки давали можливість регулювати суспільні відносини на перших етапах розвитку мережі Інтернет. Проте поява та бурхливий розвиток комерційних відносин у мережі Інтернет, створення умов для вільного широкого доступу всіх людей, з різними намірами, бажаннями, особливостями виховання тощо загострили проблеми суспільного регулювання взаємозв'язків між окремими громадянами, групами осіб. Виникла потреба в регулюванні суспільних відносин, пов'язаних із підприємницькою діяльністю, з обігом цифрових продуктів (аудіо, відео, програмного забезпечення тощо). У мережі почали надаватися платні послуги. Усе це стало причиною необхідного впливу держави на правове регулювання суспільних відносин в Інтернет» [15]. Проте такий підхід не є прийнятним для більшості користувачів мережі, оскільки всі вони вже звикли отримувати необхідну їм інформацію у потрібний час вільно і безоплатно. Таким чином, вони підтримують концепцію свободи Інтернет-простору, яку висловив Дж. Барлоу у своїй «Декларації незалежності кіберпростору» [16].

До сьогодні сформувалося кілька рівнів правового регулювання відносин, що складаються в мережі Інтернет: міжнародний; регіональні (наприклад, у рамках Європейського союзу); національні.

Попри очевидність того, що мережа вже давно втратила можливість самостійно повністю забезпечувати безпеку її учасників, спори з приводу необхідності державного втручання в її роботу не вщухають. Міжнародна спільнота має позитивний досвід правового регулювання «технічного» боку функціонування Інтернет-мережі. Так, вперше на міжнародному рівні питання управління Інтернет були обговорені тимчасовим органом – «Робочою групою з управління Інтернет», що діяла протягом 2004-2005 років при Генеральному секретарі ООН. На підставі аналітичних матеріалів, підготовлених Робочою групою, були розроблені вихідні документи WSIS, що визначили подальші напрямки вдосконалення і покращення роботи мережі. Управління мережею Інтернет на сьогодні відбувається в рамках діяльності кількох провідних міжнародних організацій, до яких відносяться ICANN, IANA, ISOC, IETF, IGF та інші. Дані організації використовують підхід багатоаспектного формування системи управління мережею Інтернет. Так, наприклад IGF є міжнародною організацією, створеною як базис для проведення політичних діалогів стосовно методів і напрямів розвитку мережі Інтернет та можливості управління даним процесом. Корпорація ICANN, яка є неприбутковою публічною корпорацією відповідає за управління Інтернет-протоколами адресного простору (IPv4 та IPv6), надання адресних блоків регіональним реєстраторам та управління адресним простором доменів вищого рівня (включаючи контроль за кореневими серверами). Загалом, більша частина роботи зосереджена на розробці та запровадженні нових користувацьких доменів вищого рівня, тоді як усі технічні аспекти роботи перекладаються на організацію IANA [15]. ICANN управляє системою нумерації і адресації, визначає протоколи і правила роботи мережі в цілому. Розподіл IP-адрес здійснюється міжнародними організаціями, що діють на принципах самоуправління: RIN, ARIN, APNIC, AfriNIC, LACNIC і RIPE NCC. Управління національними доменами делеговано корпорацією ICANN відповідним країнам. В

більшості випадків – це організації самоуправління, що діють відповідно до національного законодавства.

В межах Європейського Союзу не має єдиного спеціального органу з регулювання Інтернет. Але у 2004 році було створено європейське агентство по мережевій і інформаційній безпеці (ENISA), що виступає в ролі консультанта і центру передових технологій у сфері мережевої й інформаційної безпеки для країн-членів і інститутів Євросоюзу. У січні 2013 року сформовано Європейський центр боротьби з кіберзлочинністю, завдання якої є припинення діяльності організованих злочинних мереж. На території ЄС діє Конвенція Ради Європи «Про кіберзлочинність» 2001 р., Директива «Про приватність і телекомунікації» (2002 р.), Директива щодо мережевої та інформаційної безпеки (2016), метою якої є встановлення загальних стандартів кібербезпеки та покращення співпраці між країнами Європейського Союзу.

Для України проблема правового регулювання Інтернет-відносин є надзвичайно актуальною. В країні продовжується процес становлення національного інформаційного суспільства, інтеграції до світового інформаційного суспільства. Стабільно позитивною в Україні є динаміка розповсюдження Інтернету і формування онлайн-аудиторії.

Протягом 2016-2017 років в Україні відбулась активна робота з розвитку профільної нормативно-правової бази та вдосконалення державного регулювання ІТ-сфери. Було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р., спрямований на визначення правових та організаційних основ забезпечення захисту інтересів людини й громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основних цілей, напрямів та принципів державної політики у сфері кібербезпеки України, повноважень і обов'язків державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основних засад координації їх діяльності із забезпечення кібербезпеки України, а також дефініції базових термінів у сфері кібербезпеки.

Прийнято Закон України «Про електронні довірчі послуги» від 05.10.17 р., метою якого є реформування законодавства у сфері електронного цифрового підпису з урахуванням досвіду Європейського Союзу, розбудови єдиного простору довіри на основі системи електронних довірчих послуг, визнання в Україні електронних довірчих послуг, які надаються іноземними постачальниками електронних довірчих послуг, що забезпечать активний розвиток транскордонного співробітництва та інтеграцію України у світовий електронний інформаційний простір.

Підписавши Угоду про асоціацію з ЄС, Україна поступово наближала національне законодавство до європейських стандартів. Так, в березні 2017 року було внесено зміни до Закону України «Про авторське право і суміжні права», що стало спробою спростити процедуру визначення особи порушника, а разом і зробити ефективнішим захист порушених прав. Закон зобов'язав власників веб-сайтів і хостинг-провайдерів оприлюднювати інформацію про назву, адресу, електронну пошту і контактний номер телефону для зв'язку. Сама ж процедура захисту прав передбачає звернення до власника веб-сайту, на якому здійснюється порушення, або до хостинг-провайдера. Праву на звернення кореспондує обов'язок власника або провайдера відреагувати на протиправний контент у визначений строк.

Порядок висвітлення роботи державних органів в цифровому просторі регламентує Постанова Кабінету Міністрів України «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади». Державний комітет інформаційної політики, телебачення та радіомовлення України разом з Державним комітетом зв'язку та інформатизації України у 2002 році затвердили «Порядок функціонування веб-сайтів органів виконавчої влади». З 01.01.22 року набрав чинності Закон України «Про електронні комунікації», що замінив собою Закон «Про телекомунікації» від 2004 року. Серед іншого цей документ визначає такі базові поняття як: «мережа Інтернет», «послуга доступу до мережі Інтернет», «адреса мережі Інтернет», «домен» тощо.

Отже, можна зробити висновок про те, що Інтернет варто розглядати одночасно як технічну і соціальну систему. Відповідно до цього, державне регулювання мережі має здійснюватися з урахуванням інтересів усіх зацікавлених учасників правових відносин. Управління мережею Інтернет повинне відбуватися за принципом розподілу відповідних повноважень між державними органами і громадськими організаціями. Це дозволить уникнути монополізації технічних ресурсів мережі, зайвої цензури контенту, доступу до баз даних. Метою правового регулювання роботи мережі Інтернет має стати досягнення розумного балансу між свободою і безпекою всіх її учасників.

Запитання для самоконтролю і самостійного опрацювання:

1. Що таке мережа Інтернет?
2. Назвіть етапи створення мережі Інтернет?
3. З чого складається свобода Інтернет?
4. Які методи регулювання Інтернет діють у світі?
5. На основі чого здійснюється передача даних у мережі?
6. Які існують міжнародні документи, що регулюють діяльність Інтернет?
7. Які існують вітчизняні документи, що регулюють діяльність Інтернет?
8. Що таке IP-адреса. Чи кожен комп'ютер, що знаходиться в мережі має IP адресу?
9. Як і в яких межах, на вашу думку, слід регулювати мережу Інтернет та відносини які складаються у неї?

Рекомендована література:

1. Гуцу С. Ф. Правове регулювання мережі Інтернет: міжнародний і вітчизняний досвід. *Вісник НТУУ "КПІ". Політологія. Соціологія. Право.* 2018. Вип. 2 (38). С. 114–118.

2. Бортник Н., Єсімов С. Відносини в мережі Інтернет як об'єкт правового регулювання. *Вісник Національного університету «Львівська політехніка».* Випуск 6, № 22, 2019. — С.147-153.

3. Тарасенко Л. Л. Право на доступ до Інтернету. *Вісник Львівського університету. Серія юридична.* 2020. Випуск 71. С. 53-61.

4. Про основні засади забезпечення кібербезпеки України : Закон України. *Відомості Верховної Ради України*, 2017, № 45. Ст.403. https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Національна стратегія захисту дітей в цифровому середовищі на 2021 – 2026 роки // https://thedigital.gov.ua/regulations/natsionalna-strategiya-zakhistu-ditey-v-tsifrovomu-seredovishchi-na-2021-2026-roki

6. «Інтернет-свобода в Україні 2020: дотримання прав людини та основоположних свобод в Інтернеті». Звіт ГО «Лабораторія цифрової безпеки» і Американської Асоціації Юристів Ініціативи з Верховенства Права (ABA ROLI) в Україні. 15.09.2021р. // https://dslua.org/wp-content/uploads/2021/09/Internet-svoboda-2020.pdf

7. Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 // https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

8. Bylaws for internet corporation for assigned names and numbers / A California Nonprofit Public-Benefit Corporation // https://www.icann.org/

РОЗДІЛ 3.

ДОМЕННІ ІМЕНА

3.1. Як виникла система доменних імен (DNS)

Система Доменних Імен, або DNS призначена для того, щоб комп'ютери, що працюють у всесвітній мережі, буквеному імені – домену – могли визначити IP-адресу сервера і звернутися до нього за контентом. Це унікальна буквена або буквено-цифрова адреса (доменне ім'я) кінцевого мережевого обладнання для ідентифікації відповідного ресурсу. Ця система була запроваджена у 1983 році на заміну написання числових IP-адрес, які важко запам'ятовувати й використовувати для ідентифікації.

За часів зародження всіх сучасних технологій (70-80-і роки XX століття) комп'ютерні мережі були зовсім невеликими, а адреси всіх комп'ютерів в мережі можна було легко занести в список. Згодом мережа виросла, файл з іменами комп'ютерів збільшувався стрімкими темпами, знайти що-небудь в ньому стало складно, оновлення записувалися не відразу. Незабаром прийшли до висновку, що запам'ятовувати цифри не зручно, набагато зручніше використовувати деякі осмислені назви. Тому вирішили назвати всі комп'ютери по іменах і записати відповідності мережевих адрес і зрозумілих людині імен в спеціальному файлі. Отже, користувач вводив ім'я потрібного йому комп'ютера, а комп'ютер дивився в файлі, яка мережева адреса йому відповідає і запитував потрібну інформацію. Для внесення змін до цього файлу був призначений співробітник, який записував всі зміни й поширював актуальну версію всім бажаючим.

Використання більш простого імені, що запам'ятовується, замість числової адреси хоста належить епосі ARPANET. Стенфордський дослідницький інститут

(тепер SRI International) підтримував текстовий файл HOSTS. TXT, який зіставляв імена вузлів із числовими адресами комп'ютерів в ARPANET. Підтримка числових адрес, названих списком присвоєних номерів, було опрацьовано Джоном Постілем в Інституті інформаційних наук Університету Південної Каліфорнії (ISI), команда якого тісно співпрацювала з НДІ у публікації «Структура і делегування системи доменних імен» (RFC 1591) [17] (Domain Name System Structure and Delegation), концепцію якої відображено в технологічному документі RFC 1034 «Domain Names — Concepts And Facilities». У той час адреси призначалися вручну. Щоб запросити ім'я хоста та адресу та додати комп'ютер до головного файлу, користувачі зв'язувалися з мережним інформаційним центром (NIC) SRI, керованим Елізабет Фейнлер, телефоном у робочий час. Згодом мережі, що розвивалася, була потрібна автоматична система іменування для вирішення технічних і кадрових питань. У 1984 році чотири студенти Каліфорнійського університету в Берклі (UC Berkeley) написали першу версію сервера імен BIND (Berkeley Internet Name Daemon). У 1985 році Кевін Данлеп з DEC суттєво переглянув реалізацію DNS. У листопаді 1987 року було прийнято специфікації DNS — RFC 1034 і RFC 1035. Після цього було прийнято сотні RFC, які змінюють і доповнюють DNS.

Першого грудня 1992 року Джон Постел делегував домен .UA, додавши відповідну інформацію на кореневі сервери. Цей момент і став днем народження домену, символу України в глобальній мережі. Того ж року з'явилися публічні домени для регіонів України. За три роки, в 1995-му, були делеговані публічні домени «com.ua», «gov.ua» і «net.ua». 1997-го з'явилися короткі публічні домени регіонів, а 2001-го — «Хостмастер», що забезпечує підтримку реєстру домену «.UA». Тоді ж було зареєстровано перше приватне ім'я другого рівня (business.ua для газети «Бізнес»). 2004 року стала застосовуватися хмарна технологія Anycast для серверів домену «.UA».

Знаковим в історії розвитку домену «.UA» став 2010 рік. Саме тоді кількість зареєстрованих доменних імен

подолала межу в півмільйона. Крім того, з'явилися підтримка IPv6 і перше дзеркало кореневого сервера L-root в Україні. Цього ж року з'явилася можливість реєстрації кириличних доменних імен третього рівня. 2011 р. запам'ятався впровадженням технології EPP, генерацією DNSSEC-ключа домену «.UA». За чотири роки «Хостмастер» підписав угоду з Міжнародною корпорацією з розподілу доменних імен ICANN і з'явився перший іноземний реєстратор. За офіційною статистикою станом на серпень 2022 р. в доменній зоні UA зареєстровано понад 571541тисяч імен [18].

3.2. Правова природа доменних імен

Головною метою домену є ідентифікація та адресація веб-сайту в мережі Інтернет, що реалізується завдяки системі доменних імен (DNS), яка являє собою розподільчий механізм перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в Ір-адресу [19].

Правове положення доменів визначається правилами Інтернет-корпорації з присвоєння імен та номерів (Internet Corporation For Assigned Namesand Numbers, далі — ICANN) та низкою вітчизняних нормативно-правових актів. Наприклад «Регламент публічного домену» від 24 січня 2020, що був розроблений спільно ТОВ «Хостмайстер», адміністраторами публічних доменів та реєстраторами визначає *Домен* як символьне позначення областей в мережі Інтернет, що базується на ієрархічній структурі, що дозволяє визначити доменні імена, а *Доменне ім'я* як символьне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі [20]. Своєю чергою «Концепція впровадження та розвитку домену .УКР» визначає *Домен .УКР* як кириличний загальнодоступний національний домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування частини адресного простору українського сегмента мережі

Інтернет, і який делегований Україні в рамках процедури впровадження інтернаціоналізованих доменних імен (IDN) для представлення України в глобальній системі доменних імен.

Легальне визначення поняття доменного імені міститься у ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг», де доменне ім'я — це ім'я, яке використовується для адресації комп'ютерів і ресурсів в Інтернеті, і більш деталізовано у ст. 2 Закону України «Про електронні комунікації», відповідно до якої **домен — це частина ієрархічного адресного простору мережі Інтернет, що має унікальну назву (доменне ім'я), що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється** [21].

В науковій літературі питання юридичної природи домену розкривається в дослідженнях Н. М. Булат, К. Г. Некіт, Ю. Є. Атаманова, Д. Жуванова, Є. Стогнія, О. Смотрова, Р. Смірнова. Однак дискусії навколо цього питання продовжуються, зокрема, активно дискутується питання щодо правової природи доменного імені.

Так, Н. М. Булат пропонує наступне визначення терміну «доменне ім'я» — це унікальний набір символів, який використовується для адресації комп'ютерів і є засобом індивідуалізації Інтернет-ресурсу [22]. Науковець виділяє такі ознаки доменного імені:

1. Доменне ім'я являє собою **унікальний набір символів**. Так, розглядаючи доменне ім'я з позиції права інтелектуальної власності, не можна відійти від його інформаційно-технологічної природи, за якою доменне ім'я є саме унікальним набором символів;

2. Доменне ім'я використовується для **адресації комп'ютерів**, адже однією з двох основних функцій доменного імені з інформаційно-технічного погляду є адресація комп'ютерів у мережі;

3. Доменне ім'я є **засобом індивідуалізації** інформаційних ресурсів у мережі Інтернет.

Необхідно зазначити, що з точки погляду науковця обидві основні функції доменного ім'я тісно пов'язанні одна з одною. З інформаційно-технічного погляду перша

функція полягає в адресації ресурсів у мережі. Проте з погляду права інтелектуальної власності доменні імена не просто слугують для адресації ресурсів, вони не тільки позначають адреси сайтів і надають доступ до них, їхня роль полягає в індивідуалізації Інтернет-ресурсів, наданні останнім унікальності [22].

Схожу позицію має і А. В. Попцов, який робить висновок, що «доменне ім'я здатне виконувати дві важливі функції – функцію адресації в мережі Інтернет та індивідуалізації інформаційного ресурсу (веб-сайту)» [23].

Наразі неможливо точно схарактеризувати правову природу прав на доменне ім'я. Але існують різні точки зору щодо цього питання. Так, сьогодні ведуться дискусії щодо того, чи слід вважати доменне ім'я майном, і, відповідно, об'єктом права власності, чи це є об'єкт права інтелектуальної власності, а деякі дослідники розглядають доменне ім'я як особливий об'єкт виключних прав, який не можна віднести до об'єктів права інтелектуальної власності. Висловлюються й думки, що доменне ім'я взагалі не є об'єктом цивільних прав натомість об'єктом цивільних прав є право адміністрування доменного імені, яке належить особі на підставі договору про надання послуг, що надаються реєстратором доменних імен [24].

Частина юристів вважає, що оскільки права на доменне ім'я виникають на підставі договору з відповідним реєстратором і в рамках умов такого договору, а саме доменне ім'я – всього лише послуга реєстратора за укладеним договором. У зв'язку з цим, такий підхід називатиметься *процедурним*. Інша частина юристів вважає, що доменне ім'я – це майно, а права на доменні імена є абсолютними майновими правами. В літературі такий підхід називають *майновим*.

Процедурний підхід до природи прав на доменні імена

Розподілу доменних імен серед кінцевих користувачів присвячені правила ICANN RFC 1591 «Політика делегування доменних імен верхнього рівня». По суті відбувається процедура реєстрації нового

доменного імені. Реєстратором доменних імен при цьому виступає організація, що має повноваження створювати (реєструвати) нові доменні імена і продовжувати термін дії вже наявних доменних імен у домені, для якого встановлена обов'язкова реєстрація.

Правила реєстрації в міжнародних доменах встановлюються ICANN. Правила реєстрації в національних доменах встановлюються їхніми реєстраторами та/або органами влади відповідних країн (В Україні це такі документи, як: Регламент публічного домену, Регламент особливостей реєстрації приватних доменних імен другого рівня в домені **.UA**, Регламент особливостей реєстрації приватних доменних імен третього рівня в доменах kyiv.ua та kiev.ua тощо). Прихильники даного підходу обґрунтовують свою позицію тим, що права і обов'язки виникають в рамках договору реєстрації доменного імені, доменне ім'я лише **делегується певній особі для користування**. По суті доменне ім'я — це символ, за допомогою введення якого користувач одержує доступ до того або іншому Інтернет-ресурсу. Право на доменне ім'я триває доки триває чинність договірних відносин користувача з реєстратором. Отже, говорити про набуття абсолютних прав власника в таких випадках не коректно. Відповідно до Регламенту публічного домену доменні імена мають «життєвий цикл». Життєвий цикл складається з таких основних етапів:

1) період фактичної реєстрації (Registered);

2) період автоматичного продовження (Auto Renew Grace Period);

3) період відновлення домену після видалення (Redemption Grace Period);

4) період фактичного видалення (Pending Delete).

Кожен етап містить набір операцій та дій, які можна виконувати стосовно доменного імені. Тому, на думку прихильників даного підходу, *доменне ім'я, як і будь-яка інша адреса, не може бути об'єктом права власності.* Підтверджує таку позицію ст. 418 Цивільного кодексу України, згідно з якою об'єктом права інтелектуальної власності може бути визнаний тільки той об'єкт, що

визначений цим Кодексом та іншими законами. Немає доменного імені й у списку об'єктів права інтелектуальної власності, зазначеному у ст. 420 ЦК України.

Майновий підхід до природи прав на доменні імена

Прихильники майнового підходу відносять право на доменне ім'я до об'єктів права власності. Аргументується така позиція тим, що права на доменне ім'я набуваються з **метою вільного користування, володіння й розпорядження доменним іменем**. Доменне ім'я розглядається як об'єкт, як товар, що має економічну цінність. Це характеризує право на нього як майнове і таке, що має абсолютний характер. Не є об'єктом права власності тільки сама IP-адреса, що є простим набором цифр. Позначення ж цієї IP-адреси (доменне ім'я) може бути об'єктом права власності. Нагадаємо, що об'єктом права власності відповідно до ст. 316 ЦК України є річ (майно). А відповідно до ст. 190 ЦК України, майном як особливим об'єктом вважаються окрема річ, сукупність речей, а також майнові права та обов'язки. Майнові права є неспоживчою річчю. Майнові права визнаються речовими правами. Доменні імена є об'єктами цивільного обороту. Вони мають нематеріальну складову, асоціюючись із відомістю та репутацією особи, яка стоїть за інформаційним ресурсом, до якого адресує доменне ім`я. Це певний нематеріальний актив, який має свою вартість у грошовому еквіваленті та може приносити прибуток.

Своєю чергою і серед прихильників матеріального підходу немає єдності. В науковій літературі доменне ім'я визначають як:

- різновид майна;

- об'єкт інтелектуальної власності (і тут також є спори: а) ототожнення зі знаками для товарів і послуг; б) самостійний об'єкт ІВ (засіб індивідуалізації).

Оскільки домен має буквене чи словесне вираження, він може бути ідентичним чи схожим з різними об'єктами права інтелектуальної власності (наприклад, знаки для товарів і послуг, фірмові (комерційні) найменування, географічні зазначення походження товару, та інші). Разом

з тим ще у 1994 році Джон Постел не виключав можливості збігу доменних імен і торговельних марок, і покладав відповідальність за добросовісне використання на реєстрантів доменних імен як передумову для використання DNS. Якщо дослівно, то пп. 1 п. 4 RFC 1591 стверджує, що «The registration of a domain name does not have any Trademark status».Законодавча невизначеність правового статусу доменного імені на практиці призводить до виникнення правової колізії між правами на доменні імена та правами на інші, схожі за виразом об'єкти права інтелектуальної власності.

Прихильники віднесення доменних імен до об'єктів права інтелектуальної власності використовують наступні аргументи для обґрунтування своєї позиції:

- підбір та вибір позначення для реєстрації доменного імені можна вважати результатом інтелектуальної діяльності людини;
- комбінація літер, що складають доменне ім'я доволі часто сьогодні захищається за допомогою реєстрації доменного імені як торговельної марки, під якою згідно зі ст. 492 ЦК України розуміють будь-яке позначення або будь-яка комбінація позначень, які придатні для вирізнення товарів (послуг), що виробляються (надаються) однією особою, від товарів (послуг), що виробляються (надаються) іншими особами. Такими позначеннями можуть бути, зокрема, слова, літери, цифри, зображувальні елементи, комбінації кольорів.
- доменне ім'я володіє абсолютною (невідносною) унікальністю. При цьому у різних доменних зонах можлива реєстрація тотожних доменів, тобто домен володіє відносною унікальністю в рамках певної доменної зони, натомість доменне ім'я є абсолютно унікальним. Як наслідок, по-перше, тотожні доменні імена не можуть позначати різні Інтернет-ресурси, по-друге, з огляду на таку унікальність доменного імені право на його використання не може передаватися з одночасним збереженням такого права за первісним володільцем, адже одне доменне ім'я позначає лише один Інтернет-ресурс.

Використовувати тотожні доменні імена для різних ресурсів технічно неможливо [25].

Суб'єктивні права на доменні імена

Щодо визначення суб'єктів права інтелектуальної власності на доменне ім'я очевидно, що такими є реєстрант та реєстратор доменного імені за договором про реєстрацію доменного імені, а також інші особи, які набули прав на доменне ім'я за договором або законом.

Відповідно до Регламенту публічного домену **Реєстратор** – особа, що надає Реєстранту послуги з реєстрації та супроводу доменного імені. **Реєстрант** – особа, в інтересах якої здійснюється реєстрація та делегування приватного доменного імені.

З огляду на те, що більшість науковців розглядає доменне ім'я як особливий об'єкт права інтелектуальної власності й відносять його до засобів індивідуалізації, воно, як і комерційні найменування, торговельні марки, географічні зазначення, є результатом інтелектуальної, а не творчої діяльності, саме тому на доменне ім'я, як і на інші засоби індивідуалізації, існують **тільки майнові права.**

При розгляді питання щодо змісту права на доменне ім'я варто звернутися до ч. 1 ст. 424 Цивільного кодексу України, яка визначає майнові права на об'єкт права інтелектуальної власності, а саме: право на використання об'єкта права інтелектуальної власності, виключне право дозволяти використання об'єкта права інтелектуальної власності, виключне право перешкоджати неправомірному використанню об'єкта права інтелектуальної власності, у тому числі забороняти таке використання, інші майнові права інтелектуальної власності, установлені законом.

З огляду на вищенаведене, в науковій літературі коло майнових прав інтелектуальної власності на доменне ім'я окреслено так:

1) право на використання доменного імені;

2) виключне право дозволяти використання доменного імені;

3) виключне право перешкоджати неправомірному використанню доменного імені, у тому числі забороняти таке використання;

4) право делегувати домени нижчого рівня у своєму доменному імені;

5) право здійснювати адміністрування делегованих доменів.

Окрім цього, варто встановити, що майнові права інтелектуальної власності на доменне ім'я належать реєстранту доменного імені за договором про реєстрацію доменного імені, якщо інше не встановлено договором або законом [26].

3.3. Юридичний захист прав на доменне ім'я

Оскільки кількість Інтернет-користувачів з кожним роком зростає, збільшується і кількість доменних спорів, що, у свою чергу, потребує кваліфікованої допомоги у їх розгляді.

Доменний спір — це спір, який виникає щодо законності (недобросовісності) реєстрації та використання доменного імені між власником цього доменного імені та іншою зацікавленою особою.

Проблема з реалізацією права на захист під час розгляду доменних спорів у правовласників виникає в цілому з огляду на ту обставину, що право на використання доменного імені є універсальним і не перебуває в межах конкретної юрисдикції.

Крім того, у спорах про порушення прав у мережі Інтернет також виникає питання щодо юрисдикції судів, яким підвідомчий розгляд спору, з урахуванням наявності іноземного елемента в таких справах, установлення місця перебування відповідача, доступності веб-сайту, до якого адресує доменне ім'я, установлення дій чи подій, пов'язаних з неправомірним використанням доменного імені, які визначають місце вчинення порушення. У зв'язку з цим у кожному конкретному випадку територіальна юрисдикція суду визначається індивідуально, з урахуванням норм

міжнародного приватного права, локальних процесуальних норм [27].

Як засвідчує судова практика, основною категорією спорів, що виникають у зв'язку з реєстрацією та використанням імен доменів є спори про:

- заборону використання домену або його блокування;
- припинення використання позначень, що охороняються свідоцтвами на знаки для товарів і послуг у певному доменному імені та скасування реєстрації спірного доменного імені;
- передання спірного домену правовласнику ідентичних або подібних до ступеня змішування знаків для товарів та послуг (переделегування доменного імені);
- збереження домену за поточним його власником (реєстрантом);
- визнання права на використання комерційного найменування у доменних іменах.

Спори у даній категорії справ, зазвичай виникають у зв'язку з тим, що особа, якій належить торговий знак, найменування якого збігається з найменуванням домену, зареєстрованого іншою особою, вважає, що у зв'язку з такою реєстрацією та використанням домену порушуються майнові права інтелектуальної власності власника торгового знака, оскільки вона не лише позбавлена можливості зареєструвати аналогічний домен, але й зазнає збитків внаслідок використання сторонніми особами її ділової практики, імені та репутації для отримання вигоди (привернення уваги тощо).

Шляхи вирішення доменних спорів:

1. **Переговори або медіація**. Перший і найбільш поширений метод вирішення спору — це *досудове врегулювання*, яке найчастіше супроводжується надісланням відповідних претензій з чітким зазначенням видів відповідальності за продовження порушення прав та може бути ефективним важелем тиску на порушника, та проведенням переговорів. Але, як свідчить практика, у доменних спорах цей механізм не є достатньо дієвим і

далеко не завжди призводить до відновлення порушених прав.

2. **Звернення до Арбітражного суду із застосуванням процедури «Єдиної політики вирішення спорів про доменні імена» (Uniform Domain Name Dispute Resolution Policy, UDRP).** Якщо третя особа зареєструвала домен в зонах .Com, .Net, .Org, .Biz, .Info, .Name і т. д., а також в деяких національних зонах .Hk, .In, Ви можете звернутися до вищезазначеного органу з вимогою про скасування або передачу (переделегування) доменного імені. Зазначений спір вирішується на основі Єдиної політики вирішення спорів про доменні імена і специфікою таких спорів є те, що звернутись за захистом може власник лише такого об'єкта, як торговельна марка.

Спори за вказаною процедурою можуть розглядатись п'ятьма акредитованими організаціями, серед яких:

- Азійський центр з вирішення доменних спорів (Asian Domain Name Dispute resolution Centre);
- Національний арбітражний форум (National Arbitration Forum);
- Центр ВОІВ з арбітражу та посередництва (WIPO);
- Чеський арбітражний суд; (The Czech Arbitration Court Arbitration Center of Internet Disputes);
- Арабський центр з вирішення спорів (Arab Center for Domain Name Dispute Resolution).

Основними перевагами вирішення спору з використанням UDRP в порівнянні з іншими методами захисту є наступні:

- **Швидкість.** Як правило, від моменту подання заяви до арбітражного центру до моменту винесення рішення і передачі домену законному власнику проходить не більше 60 днів.
- **Інтернаціональність.** Заявник і відповідач можуть знаходитись в різних частинах світу — це не буде перепоною для подання заяви до ВОІВ і отримати рішення з передачею домену у власність належного правоволодільця.

- **Вартість звернення.** За загальним правилом розгляд справи одним арбітром щодо одного доменного імені буде коштувати близько $ 1500 (в залежності від обраного центру), а розгляд трьома арбітрами — близько 4000 $.

Основним **недоліком використання UDRP є те**, що фактично існує лише 2 варіанти прохальних вимог. Арбітри за результатом розгляду заяви можуть прийняти одне з двох рішень — передати або скасувати домен. Тобто ні про яку втрачену вигоду, стягнення грошей, публічні вибачення та інше не може бути мови. Заявнику або буде передано домен у власність (або ж відмовлено у передачі) або його скасують (тобто він перестане існувати) [28]. Проте, це не позбавляє заявника права ще окремо звернутись до суду з вимогою про відшкодування збитків.

В основі UDRP знаходяться 3 підстави (елементи) доведення, що гарантує передачу оспорюваного домену заявнику.

1. *Доменне ім'я є ідентичним або бентежно схожим з торговою маркою або маркою обслуговування, щодо яких у заявника є права та інтереси* (англ. «your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights»). Відповідно до консенсусного погляду в узагальненій практиці, наявність зареєстрованої торгової марки є достатнім для визнання доменного імені бентежно схожим. Місце, в якому торгова марка зареєстрована, дата реєстрації такої марки, вид діяльності чи продукту, який реалізовується під цією маркою, не є визначальним для знайдення схожості.

Даний пункт UDRP містить порівняння оспорюваного доменного імені з торговою маркою заявника для визначення ступеня схожості та того, як така схожість може заплутати користувача Інтернету.

2. *Відсутність прав або законних інтересів щодо доменного імені* (англ. «you have no rights or legitimate interests in respect of the domain name»). Обов'язок доказування на початку розгляду справи лежить на заявникові. Проте, як неодноразово вказувалося арбітрами, інколи такий тягар доказування просто неможливо здійснити, тому що вся необхідна інформація для такого доведення доступна лише

відповідачу. Таким чином, існує практика доведення prima facie випадку. Тобто випадку, який «на перший погляд» доводить, що у відповідача немає законних інтересів у такому доменному імені. Якщо заявником буде наведено такий приклад, то тягар доказування наявності своїх інтересів у доменному імені переходить на відповідача. Обов'язком відповідача буде надати докази й довести, що законні права та інтереси на доменне ім'я існують. У випадку, якщо відповідач не надасть доказів, то як правило вважається, що другий елемент UDRP задоволено.

3. *Доменне ім'я було зареєстровано та використовується недобросовісно* («domain name has been registered and is being used in bad faith»). **Існує 4 основних види** недобросовісного використання, проте чітко сказано, що перелік не є вичерпним:

- основною метою реєстрації доменного імені є бажання продажу, здачі в оренду або передача домену будь-яким іншим чином особі, яка володіє правами на торгову марку, або конкуренту такої особи за ціною, яка набагато перевищує витрати на реєстрацію домену;

- доменне ім'я було зареєстроване з метою завадити володільцю торгової марки або найменування послуг використовувати відповідне доменне ім'я, за умови, що раніше була помічена така діяльність з боку реєстратора;

- основною метою реєстрації доменного імені є перешкоджання ведення підприємницької діяльності конкурента;

- доменне ім'я використовується для навмисного заманювання з комерційною метою користувачів Інтернету на цей веб-сайт або інший Інтернет-ресурс шляхом створення подібності з торговою маркою заявника, котрий нібито є засновником, спонсором, партнером або підтримує цей веб-сайт або інший ресурс, продукт або послугу, що пропонується на цьому веб-сайті або ресурсі.

У випадку якщо заявник доведе всі 3 елементи, передбачені UDRP, домен буде передано заявникові!

Процедура UDRP включає наступні етапи:

1) подача претензії в організацію, що уповноважена ICANN (один з п'яти вищезазначених центрів);

2) подача відкликання; призначення Адміністративної комісії у складі однієї або трьох осіб (за загальним правилом спір розглядається одним арбітром, але за згодою сторін може бути призначено розгляд трьома – кожна сторона обирає по одному й одного призначає Адміністративна комісія);

3) винесення рішення і повідомлення зацікавлених осіб;

4) виконання рішення реєстратором щодо відмови в задоволенні вимог або скасуванні реєстрації чи передачі доменного імені.

Для успішної скарги треба:

- довести, що товарний знак заявника ідентичний або подібний до ступеня змішання з доменним ім'ям;
- довести, що реєстрант доменного імені не має прав або законних інтересів з приводу цього доменного імені;
- довести, що доменне ім'я зареєстроване або використовується недобросовісно.

Позасудова процедура не перешкоджає переведенню розгляду суперечки в національний суд. У цьому випадку розгляд справи в Центрі арбітражу припиняється до рішення національного суду.

3. **Звернення до суду.** Обираючи цей механізм, необхідно, перш за все, визначитися з підвідомчістю та підсудністю спору. Для цього необхідно визначити коло учасників судового процесу. Фактично в реєстрації доменного імені в домені .UA беруть участь 3 особи: реєстрант, реєстратор і адміністратор. Організацією, уповноваженою на здійснення функцій адміністратора в Україні в домені .UA, є товариство з обмеженою відповідальністю «Хостмайстер», яке діє на підставі договору з корпорацією ICANN (Інтернет-корпорація з присвоєння імен та номерів). Реєстраторами, своєю чергою, виступають суб'єкти господарювання, які діють на підставі договорів з адміністратором та виконують функції посередника між адміністратором та реєстрантом.

Найскладнішим є встановлення саме реєстранта доменного імені. У разі, якщо реєстрантом виступає

юридична особа, відповідні дані можна встановити за допомогою, зокрема, бази who.is. Цей сервіс є джерелом публічної інформації, яка доступна через мережу Інтернет на веб-сайті адміністратора доменної зони com.ua ТОВ «Хостмайстер». Та якщо реєстрантом є фізична особа, зважаючи на вимоги законодавства про захист персональних даних, відомості про неї мають обмежений доступ. Наприклад, у базі who.is відомості про такого реєстранта надаються в знеособленому вигляді. При цьому непоодинокими є випадки, коли доменне ім'я реєструється на осіб, які фактично не існують.

Належним підтвердженням того, що певна особа є власником сайту, можуть бути дані, отримані від адміністратора адресного простору українського сегмента мережі Інтернет у відповідному домені, а також дані, отримані від реєстратора, який на підставі цивільно-правового договору, укладеного з реєстрантом, здійснював реєстрацію відповідного доменного імені (п. 12 постанови Пленуму Верховного Суду України від 27 лютого 2009 р. № 1 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи»).

Однією з проблем розгляду справ даної категорії спорів є те, що сторонами формуються позовні вимоги, які не узгоджуються з переліком способів захисту, наведених в ст. 16 ЦК України та ст. 20 ГК України. За змістом вказаних норм суд може захистити права та законні інтереси й іншим способом, якщо він передбачений договором або законом. Однак, в більшості випадків між сторонами відповідних спорів не має укладених договорів, які б визначали способи захисту порушених прав, як і в інших законодавчих актах не передбачено способів захисту у даній категорії спорів, що відповідно, як і самі відносини, які виникають між учасниками мережі Інтернет, потребує додаткового законодавчого врегулювання [29].

Можливі способи захисту:

1. Припинення користування. Наприклад, зобов'язати видалити з реєстру; скасувати реєстрацію; достроково анулювати; припинити делегування; визнати недійсним

делегування домену. Недоліком цього способу є те, що через декілька годин після виконання рішення відповідач зможе зареєструвати доменне ім'я повторно. В цьому випадку Позивач не може перешкодити повторній реєстрації домену, що призведе до повторного звернення до суду.

2. Делегування – це процес надання можливості правоволоділцю торговельної марки користуватися доменним іменем (тобто передача права користування доменом від реєстранта до власника ТМ).

3. Заборона використання у доменному імені знаку чи комерційного найменування. Але цікавіше його тотальна (або, як пишуть науковців, прогібіторна) версія – **заборона використання доменів або позначення в домені шляхом делегування іншим особам**. Цю вимогу на майбутнє може виконати будь-який реєстратор. Наприклад, в справі 910/32742/15 суд заборонив реєстратору порушувати права інтелектуальної власності позивача на комерційне найменування «БОМОНД» шляхом незаконного делегування на користь інших осіб доменного імені (рішення господарського суду м. Києва від 19.12.2016 р., постанова Київського апеляційного господарського суду від 20.08.2018 р., постанова Верховного Суду від 18.10.2018 р.). Можливо, такий спосіб доречний, якщо позивач не хоче сам використовувати домен, але і не дати іншим це робити.

4. **Антимонопольний комітет України.** Якщо Вашу торговельну марку або схожу до неї використовує суб'єкт господарювання в доменному імені для здійснення своєї господарської діяльності, Ви можете звернутися до цього органу, який своїм рішенням може визнати дії такого суб'єкта недобросовісною конкуренцією, і накласти на нього відповідний штраф.

Запитання для самоконтролю і самостійного опрацювання

1. Доменне ім'я: поняття та ознаки.
2. Інтернет-корпорація з призначення доменних імен та номерів (ICANN): характеристика та функції.

3. Чи є доменне ім'я об'єктом права інтелектуальної власності?

4. Чи можлива реєстрація доменів на кирилиці?

5. В якому домені доменні імена реєструються на підставі свідоцтва на знак для товарів і послуг?

6. Які є способи вирішення конфліктів, пов'язаних з недобросовісним використанням доменних імен?

Рекомендована література:

1. Uniform Domain Name Dispute Resolution Policy. As Approved by ICANN on October 24, 1999. URL: https://www.icann.org/resources/pages/policy-2012-02-25-en

2. Регламент публічного домену, розроблений спільно ТОВ «Хостмайстер», адміністраторами публічних доменів та реєстраторами 24 січня 2020 р. URL: https://hostmaster.ua/registrators/docs/Reglament2ld_3.5_UK.pdf

3. Піхурець О. В. Окремі питання здійснення права на доменне ім'я // Проблеми цивільного права та процесу. Харків, 2018. С. 182-186.

4. Булат Н. М., Доменне ім'я як засіб індивідуалізації Інтернет-ресурсів. *Право і суспільство*. № 2. 2020. – С. 154-160.

5. Іваненко Д. Д., Сітак В. О. Правова природа доменних імен в мережі Інтернет. *Правові горизонти*. 2018. Вип. 8 (21). – С. 21-27.

6. Ходош А. В. Доменні спори, що виникають через порушення прав на торговельну марку: можливі шляхи їх вирішення. *Юридичний науковий електронний журнал*. № 10/2021. – С. 182-186. URL: http://www.lsej.org.ua/10_2021/47.pdf

РОЗДІЛ 4.

ОХОРОНА ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

4.1. Загальна характеристика права інтелектуальної власності

Сучасний стан правового захисту інтелектуальної власності, а також стрімкий розвиток технологій суттєво ускладнюють завдання захисту авторського права. Із розвитком мережі Інтернет та інших засобів комунікацій кожного дня величезний об'єм інформації потрапляє на електронні пристрої, потім на електронні сторінки і миттєво розповсюджується у всесвітній павутинні. Таке швидке розповсюдження даних із доступом до копіювання та наслідування надає не лише величезні можливості для творчого і особистого розвитку людства, але й серйозну загрозу для охорони авторського права. На думку деяких фахівців, наукові досягнення у сфері розробки штучного інтелекту також ускладнюють юридичне регулювання відносин щодо захисту прав на об'єкти інтелектуальної власності. Велика ймовірність того, що штучний інтелект покращить або спростить життя людства в багатьох аспектах, перетинається з непрозорістю розуміння щодо можливостей та правомірності перехресного використання об'єктів інтелектуальної власності між людьми та роботами [30].

Право інтелектуальної власності як право особи на результат творчої інтелектуальної діяльності або інший об'єкт права інтелектуальної власності, визначений законом, пов'язується, перш за все, із розумінням творчості і творчої інтелектуальної діяльності. Творчість людини можна визначити як глибоко усвідомлену нею потребу

самовираження, самоствердження, привнесення в оточуючий світ глибинних душевних переживань задля пошуку гармонії і самовдосконалення. Здатність до творчої та інтелектуальної діяльності вирізняє людину серед інших живих істот і не залежить від віку, стану здоров'я, наявності здібностей чи таланту.

Одне із найбільш вдалих визначень творчої діяльності запропонував видатний український цивіліст і основоположник наукових розробок права інтелектуальної власності в незалежній Україні О. А. Підопригора: «Творча діяльність, або просто творчість, — це цілеспрямована інтелектуальна діяльність людини, результатом якої є щось якісно нове, що відрізняється неповторністю, оригінальністю і суспільно-історичною унікальністю».

Творча діяльність притаманна кожній людині і може проявлятися в усіх сферах її життя, а широке коло видів такої діяльності зумовлює, в свою чергу, і багатоманітність її результатів.

Творчість умовно можна поділити на духовну творчість, тобто творчість переважно гуманітарного спрямування (література, мистецтво, архітектура, фотографія, наукові твори тощо) і науково-технічну творчість (винаходи, корисні моделі, промислові зразки тощо).

Інтелектуальна діяльність — це творча діяльність, а творчість — це цілеспрямована розумова робота людини, результатом якої є щось якісно нове, що відрізняється неповторністю, оригінальністю, унікальністю. Вважається, що чим вищий інтелектуальний потенціал індивідуума, тим цінніші результати його творчої діяльності — інтелектуальна власність.

Держава також визнає за кожним громадянином право на результати своєї інтелектуальної, творчої діяльності, встановлюючи водночас пряму заборону використання або поширення вказаних результатів без згоди автора, за винятками, встановленими законом.

Стаття 54 Конституції України гарантує громадянам свободу літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх

авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності.

Визначення **поняття права інтелектуальної власності** надається у ст. 418 ЦК України як **право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності, визначений законом**.

Крім ЦК України, питанням регулювання інтелектуальної власності присвячені численні закони: «Про авторське право і суміжні права», «Про охорону прав на винаходи і корисні моделі», «Про охорону прав на промислові зразки», «Про охорону прав на знаки для товарів та послуг», «Про охорону прав на зазначення походження товарів», «Про охорону прав на сорти рослин», «Про племінну справу у тваринництві», «Про охорону прав на топографії інтегральних мікросхем», «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних». Крім цього, питання прав інтелектуальної власності почасти віднесені до сфери регулювання й інших законів: «Про наукову та науково-технічну діяльність», «Про видавничу справу», «Про телебачення і радіомовлення», «Про кінематографію», «Про архітектурну діяльність», «Про особливості державного регулювання діяльності суб'єктів господарювання, пов'язаної з виробництвом, експортом, імпортом дисків для лазерних систем зчитування», «Про режим іноземного інвестування», «Про державне регулювання діяльності у сфері трансферу технологій», «Про інноваційну діяльність» тощо.

Для людини характерні два види творчості: художня і технічна. Результатом художньої творчості є, наприклад, літературні і художні твори, результатом технічної творчості — винаходи, торговельні марки, комерційні таємниці тощо.

За сформованою історичною традицією результати художньої творчості людини юридичною наукою віднесені до правового інституту авторського права та суміжних прав, а результати технічної творчості називають

об'єктами інституту права промислової власності. Останні охороняються після спеціального оформлення прав і одержання охоронного документа — патенту або свідоцтва. За назвою документа, що обумовлює охорону більшості об'єктів, — патент — цей інститут також називають патентним правом.

Поняття «інтелектуальна власність» виникло в процесі тривалої практики юридичного закріплення за певними особами їхніх прав на результати інтелектуальної діяльності у сфері науки, виробництва, мистецтва і літератури.

Право інтелектуальної власності слід розглядати у двох значеннях: об'єктивному та суб'єктивному. У *суб'єктивному* значенні право інтелектуальної власності являє собою суб'єктивне право (майнові або немайнові права) на інтелектуальний продукт, тобто певні правомочності творця або іншої особи стосовно інтелектуального продукту. ЦК України визначає, що право інтелектуальної власності становлять особисті немайнові права інтелектуальної власності та (або) майнові права інтелектуальної власності, які поширюються на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності (ст. 418 ЦК України).

В *об'єктивному* значенні право інтелектуальної власності — це система правових норм, які регулюють суспільні відносини у сфері створення та використання інтелектуального продукту. Ця сукупність правових норм становить підгалузь цивільного права і складається з декількох правових інститутів: авторське право та суміжні права, право промислової власності (патентне право), інститут засобів індивідуалізації учасників цивільного обороту, їх продукції і послуг. Кожний із названих інститутів регулює суспільні відносини у певній сфері інтелектуальної діяльності, яка відрізняється як специфікою самого інтелектуального продукту, так і пов'язаними з нею особливостями його використання.

Відповідно до українського законодавства інтелектуальна власність — це підгалузь цивільного права,

яка складається з чотирьох інститутів: Авторське право та суміжні права; Патентне право; Правова охорона засобів індивідуалізації учасників цивільного обороту, Правова охорона нетрадиційних об'єктів інтелектуальної власності.

4.1.1. Суб'єкти та об'єкти права інтелектуальної власності

Суб'єкти права інтелектуальної власності – це особи, яким можуть належати особисті немайнові та майнові права на об'єкти інтелектуальної власності. Суб'єктами права інтелектуальної власності є два види суб'єктів:

1) автор (творець) об'єкта права інтелектуальної власності;

2) інші особи, яким належать особисті немайнові та (або) майнові права інтелектуальної власності.

Таким чином, суб'єкти права інтелектуальної власності поділяються на первинні і похідні. До первинних належать тільки творці – автори творів науки, літератури і мистецтва, виконавці, виробники фонограм і відеограм, автори програм мовлення, винахідники, автори промислових зразків, сортів рослин і порід тварин та інші. До похідних – усі інші особи – правонаступники, до яких право інтелектуальної власності переходить в силу закону чи на підставі договору.

Автор – це особа, в результаті інтелектуальної, творчої діяльності якої створені об'єкти права інтелектуальної власності. Автори не обмежені вимогами до їх віку, стану здоров'я, дієздатності тощо. Творцями будь-яких результатів творчої діяльності можуть бути як повнолітні, так і неповнолітні особи. Слід звернути увагу на те, що «творча правосуб'єктність» не збігається із загальною цивільною дієздатністю, яка за загальним правом настає з досягненням фізичною особою 18 років. Суб'єктом права інтелектуальної власності може бути частково дієздатна, обмежено дієздатна або недієздатна особа. Інша річ, що здійснювати майнові права така особа

може лише за допомогою інших осіб (батьків, усиновлювача, опікуна, піклувальника тощо).

До похідних суб'єктів права інтелектуальної власності можуть належати будь-які особи — як фізичні, так і юридичні, які набувають цих прав за договором чи за законом. Правонаступниками суб'єкта права інтелектуальної власності за законом можуть бути як фізичні, так і юридичні особи — при спадкуванні за законом. Первинний суб'єкт права інтелектуальної власності може передати свої майнові права будь-якій іншій особі за цивільно-правовим договором або заповітом.

Оцінка творчого внеску при створенні об'єкта інтелектуальної власності є важливою у встановленні кола творців (співавторів), оскільки як первинними, так і похідними суб'єктами права інтелектуальної власності можуть бути кілька осіб. За законом, якщо об'єкт створено творчою працею кількох осіб, то кожна з них є суб'єктом права інтелектуальної власності (співавтором). Право інтелектуальної власності може також перейти за спадкуванням до кількох осіб.

Суб'єктом права інтелектуальної власності може бути держава, яка в особі своїх державних органів здійснює такі функції:

- регулює правовідносини в галузі інтелектуальної власності (створення нових нормативних актів);
- охороняє правовідносини інтелектуальної власності (діяльність суду, прокуратури, міліції, створення відповідних нормативних актів і реалізація державної політики);
- здійснює стимулювання творчої, винахідницької діяльності громадян;
- вирішує суперечки в галузі правової охорони інтелектуальної власності і захищає права, інтереси суб'єктів через суди;
- реєструє (веде облік) об'єктів інтелектуальної власності.

Наприклад, в Україні діють такі державні органи: Міжвідомчий комітет з проблем захисту прав на об'єкти інтелектуальної власності, Державна служба

інтелектуальної власності (далі ДСІВ), при якій створено консультативну раду представників усіх творчих спілок України, апеляційну палату для розгляду в адміністративному порядку заперечень проти рішень за заявками на об'єкти інтелектуальної власності.

В Україні функціонують і юридичні особи, створені при державних органах – це підприємства, метою яких є реалізація державних програм: Державне підприємство «Український інститут інтелектуальної власності» (Укрпатент) – інституційна складова державної системи правової охорони інтелектуальної власності в Україні. Згідно з розпорядженням Кабінету Міністрів України від 13 жовтня 2020 року № 1267-р «Про Національний орган інтелектуальної власності» Укрпатент виконує функції Національного органу інтелектуальної власності.

Українське агентство з авторських та суміжних прав – організація колективного управління правами авторів музичних, літературних, драматичних та інших творів мистецтва і науки. УААСП управляє майновими правами українських авторів, а також представляє на території України інтереси закордонних правовласників на підставі договорів про взаємне представництво з іноземними авторсько-правовими організаціями.

Крім державних інституцій, існують недержавні організації: творчі спілки, Всеукраїнська асоціація патентних повірених, Коаліція з питань захисту прав інтелектуальної власності (CIPR).

Кожен автор має право на результати своєї інтелектуальної діяльності. Це право має подвійну природу (таблиця 1). З одного боку, творець (автор) нематеріального об'єкта власності й творець матеріального об'єкта власності мають подібні права власності, тому що право на результат творчої діяльності забезпечує його власнику виняткову можливість розпоряджатися цим результатом на свій розсуд, а також передавати іншим особам, тобто воно подібне до права власності на матеріальні об'єкти (майновим правом). З іншого боку, поряд з майновим правом існує деяке духовне право творця на результат творчої праці, так зване право автора. Тобто **автор має сукупність особистих немайнових**

(моральних) прав, що не можуть відчужуватися від їхнього власника внаслідок їх природи, **та майнових прав**. Іншими словами, якщо майнове (економічне право) на результат творчої праці може бути віддільним від творця (переданим іншій особі в обмежене чи необмежене користування), то моральне (немайнове) право автора невіддільне від творця і не може бути передано іншій особі.

Таблиця 1.

Особисті немайнові права інтелектуальної власності (ст. 423 ЦК України)	**Майнові права інтелектуальної власності (ст. 424 ЦК України)**
1) право на визнання людини творцем (автором, виконавцем, винахідником тощо) об'єкта права інтелектуальної власності	1) право на використання об'єкта права інтелектуальної власності;
2) право перешкоджати будь-якому посяганню на право інтелектуальної власності, здатному завдати шкоди честі чи репутації творця об'єкта права інтелектуальної власності;	2) виключне право дозволяти використання об'єкта права інтелектуальної власності;
3) інші особисті немайнові права інтелектуальної власності, встановлені законом.	3) виключне право перешкоджати неправомірному використанню об'єкта права інтелектуальної власності, в тому числі забороняти таке використання;
	4) інші майнові права інтелектуальної власності, встановлені законом.

Об’єктом права інтелектуальної власності є не кожен результат творчої діяльності, а лише той, який відповідає вимогам закону. Твір літератури, науки і мистецтва, суміжні права підпадають під охорону права, якщо вони відповідають вимогам закону. Науково-технічним результатам правова охорона надається лише на підставі видачі правоохоронного документа. Правова охорона об’єктів права інтелектуальної власності обмежується лише територією України. Охорона прав на зазначені об’єкти на території інших держав здійснюється лише на підставі відповідних міжнародних конвенцій і договорів.

Відповідно до ст. 420 ЦК України до об'єктів права інтелектуальної власності, зокрема, належать: літературні та художні твори; комп'ютерні програми; компіляції даних (бази даних); виконання; фонограми, відеограми, передачі (програми) організацій мовлення; наукові відкриття; винаходи, корисні моделі, промислові зразки; компонування напівпровідникових виробів; раціоналізаторські пропозиції; сорти рослин, породи тварин; комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення; комерційні таємниці. Ці об’єкти можна розподілити за інститутами Права інтелектуальної власності (рис. 2).

Кожен об’єкт права інтелектуальної власності має правовий механізм захисту, визначений законодавством (Додаток 1). Специфікою вирізняється використання об'єкта інтелектуальної власності, який створено у зв'язку з виконанням трудового обов'язку чи на замовлення: особисті немайнові права залишаються у творця, а майнові права на об'єкт інтелектуальної власності належать творцеві та особі, з якою він перебуває у трудових відносинах, спільно, або замовнику, якщо інше не встановлено законом або договором.

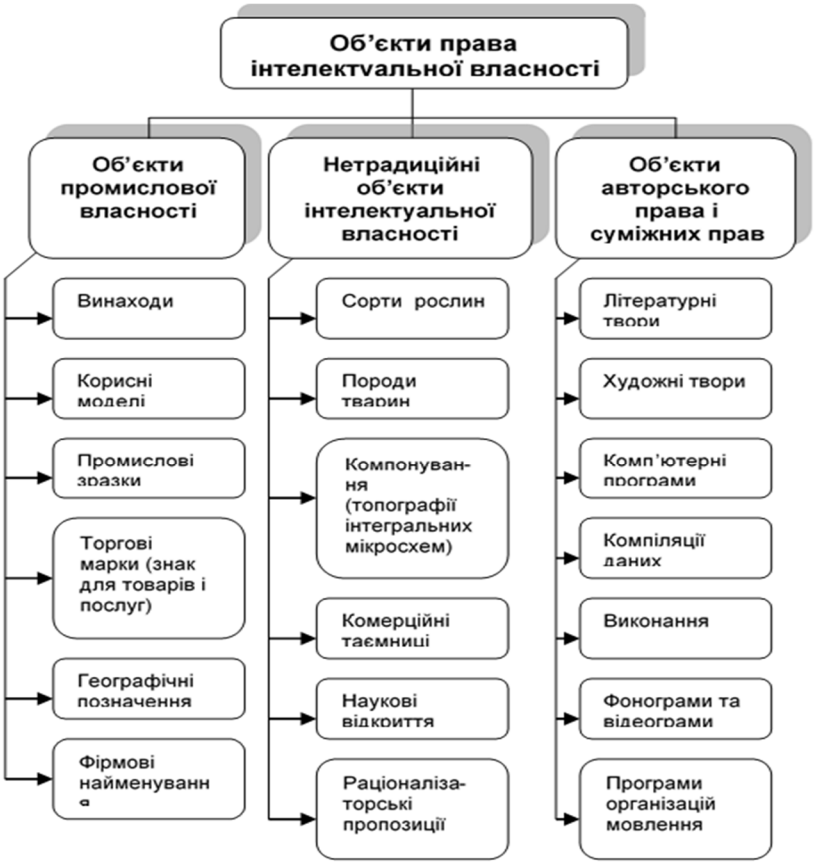

Рисунок 2 — Класифікація об'єктів права ІВ

4.1.2. Міжнародна та європейська нормативно-правова база у сфері захисту права інтелектуальної власності

МІЖНАРОДНІ ДОГОВОРИ:

1. Договір Всесвітньої Організації Інтелектуальної Власності (ВОІВ) про виконання і фонограми (WPPT) від 20 грудня 1996 р.;

2. Договір ВОІВ про авторське право (WCT) від 20 грудня 1996 р. Україна приєдналася 29 листопада 2001 р. Договір набув чинності 6 березня 2002 р. Охорона творів та авторського права у цифровому середовищі. Договором визнаються додаткові права автора, не передбачені Бернською конвенцією, а саме: — право на розповсюдження; — право на оренду; — більш широке право на публічне сповіщення ;

3. Договір ВОІВ про виконання і фонограми від 20 грудня 1996 р. (WPPT) Україна приєдналася 29 листопада 2001 р. Договір набув чинності в Україні 20 травня 2002 р. Охорона, зокрема у цифровому середовищі, прав інтелектуальної власності для виконавців та виробників фонограм;

ДИРЕКТИВИ ЄС:

1. Директива 2000/31/ЄЕК Європейського парламенту та Ради, від 8 червня 2000 року, про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку. Встановлює режим вільного надання послуг в інформаційному суспільстві ЄС; регулює та сприяє використання електронних договорів; визначає режим відповідальності постачальників послуг в інформаційному суспільстві (статті 12–15). Поміж іншого, включає:

- Електронну комерцію (укладення договорів онлайн)
- Пропонування контенту онлайн (YouTube)
- Інструменти пошуку, доступу та зберігання даних (пошукові системи, Google)
- Послуги із передачі інформації через комунікаційну мережу (електронна пошта)
- Послуги зі зберігання інформації, наданої одержувачем послуг (хмарний сервіс)

2. Директива 2001/29/ЄС Європейського парламенту та Ради, від 22 травня 2001 р., про гармонізацію певних аспектів авторського права та суміжних прав в інформаційному суспільстві. Дана Директива покликана відповісти на вплив, який має технологічний розвиток (цифрове середовище тощо) на права інтелектуальної

власності (створення, виробництво, використання; але також і необхідність посилити захист прав, враховуючи підвищену легкість їх порушення). Визнає за авторами право дозволяти публічне сповіщення та на розповсюдження у всіх їх різновидах. Визнає за власниками авторських та суміжних прав право на відтворення та на надання доступу (надання публіці доступу до об'єкта дротовими чи бездротовими засобами таким чином, що будь-яка особа могла мати доступ до них із місця та в момент, обраний нею, наприклад, через мережу Інтернет) як підвид права на публічне сповіщення (ст. 3). Систематизує можливі винятки з авторського права та суміжних прав, залишає за державами-членами рішення про встановлення (чи не встановлення) певних винятків із прав на відтворення та (у певних випадках) на розповсюдження. Документ також встановлює обов'язок передбачити захист від обходу технологічних засобів, призначених для запобігання або протидії діям стосовно об'єктів, використання яких не дозволено суб'єктом авторського або суміжних прав.

3. Директива ЄС 2019/790 про авторське право в єдиному цифровому ринку та яка доповнює директиви 96/9/ЄС та 2001/29/ЄС, прийнята 17 квітня 2019 р. (7 червня 2019 р. набула чинності). Її прийняття безпосередньо стосується України з врахуванням процесу наближення законодавства України до законодавства ЄС відповідно до Угоди про асоціацію між Україною та ЄС. Також у Директиві ряд положень належать науковому середовищу, що включає права наукових установ зі здійснення аналізу тексту (text and data mining), права бібліотек стосовно збереження примірників видань у цифровій формі; використання видань, що знаходяться поза комерційного обігу; використання творів у навчальній діяльності, визначення прав організацій, що здійснюють анотований огляд новин та публікацій тощо. Директива містить визначення трьох випадків винятків та обмежень стосовно використання творів та інших об’єктів (випадки вільного використання), а саме: що стосується аналізування даних та тексту в цілях наукових досліджень (ст. 3), використання

творів та інших об’єктів у цифровій та транскордонній навчальній діяльності (ст. 5) та збереження культурної спадщини (ст. 6).

4.2. Охорона авторських і суміжних прав в мережі Інтернет

Сфера захисту авторського права в мережі Інтернет є доволі специфічною, через те, що використання стороннього контенту відбувається практично кожним, хто має доступ до мережі Інтернет. Інтернет-технології дозволяють завантажувати, зберігати, поширювати різні види інформації, в тому числі об'єкти, які охороняються авторським правом. Проблема захисту авторських та/або суміжних прав у сфері Інтернет зумовлена, перш за все, у простоті та швидкості розміщення інформації у всесвітній мережі, у відсутності необхідності обов’язкової авторизації при вчиненні таких дій, відкритості та доступності користування електронними ресурсами необмеженим фактично колом осіб. Такі переваги інформаційних технологій мають водночас відповідно до принципу діалектичного розвитку й зворотній бік, – у відкритому стані інформація та об’єкти права інтелектуальної власності потрапляють до мережі Інтернет без згоди й навіть поза межами обізнаності автора, чим порушуються не тільки права автора на отримання винагороди за свій інтелектуальний труд, а і його особисті немайнові права, перш за все, право вимагати визнання свого авторства шляхом зазначення належним чином власного імені на творі і його примірниках і за будь-якого публічного використання твору. Отже, при однозначній привабливості саме Інтернет-мережа стає віртуальним ринком обороту і збуту продукції із порушенням виключних прав авторів та інших правоволодільців [31].

4.2.1. Комп’ютерна програма як об’єкт правової охорони

Комп’ютерна програма в еру інформаційних технологій є одним із головних стратегічних ресурсів як

держави в цілому, так і приватних осіб, це визначає її особливе місце серед інших об'єктів права інтелектуальної власності. Аналіз судової практики показує, що вона зазнає найбільшого впливу від правопорушень, що обумовлено суттєвою різницею між витратами ресурсів на створення комп'ютерних програм та витратами на їх незаконне копіювання та розповсюдження.

Інтеграція комп'ютерних програм та програмного забезпечення в повсякденне життя, а також стрімке оновлення технологій їх створення, збільшили не тільки сферу застосування цього об'єкта права інтелектуальної власності, але і надали йому нових особливих ознак.

Вперше комп'ютерна програма почала охоронятися як об'єкт авторського права у 1964 році в США. Сьогодні практично в усіх країнах світу комп'ютерна програма охороняється авторським правом.

Статтею 1 Закону України «Про авторське право і суміжні права» закріплено **визначення комп'ютерної програми**, відповідно до якого остання — **це набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату.**

Постає цікаве питання: чому законодавець поєднав охорону літературних творів та комп'ютерних програм? Існує кілька неофіційних пояснень із цього приводу, одне з яких свідчить про те, що відповідно до норм авторського права захищається форма, в якій втілені ідеї автора [32].

У науковій літературі називаються такі фактори, що свідчать про належність комп'ютерних програм до об'єктів авторського права:

- вихідний текст комп'ютерної програми має риси письмового літературного твору (подібність з літературним твором доповнює й те, що текст комп'ютерної програми може бути написаний різними мовами програмування — Асемблері, Сі, Яві, Паскалі, Бейсику тощо, як і будь-який літературний твір — українською, російською, англійською чи іншою мовами);

- алгоритми, методи, ідеї, теорії, формули, використані при розробці комп'ютерної програми, додають їй риси наукового твору, тобто галузеву належність до об'єктів авторського права;

- аудіовізуальні зображення, анімація і графіка, створювані комп'ютерною програмою, мають риси музичного (з текстом і без тексту), аудіовізуального, твору образотворчого мистецтва, твору, виконаного способами, подібними до фотографії, художнього твору, що також дає підстави віднести їх до творів у галузі мистецтва [33].

Ця тотожність творчого процесу щодо створення літературних творів і комп'ютерних програм стали підставою для вибору форми захисту для комп'ютерних програм.

Однак, в літературі існує багато аргументів і проти того, щоб ототожнювати комп'ютерну програму з художніми творами. Наприклад, Д. Жуванов розглядаючи комп'ютерну програму як твір літератури, відзначає цікаві особливості:

- будь-який фрагмент будь-якої програми можна використовувати як цитату в іншій програмі. Це дає можливість безоплатно і безкарно тиражувати чужі ідеї і отримувати за це прибуток. Таке тиражування приводить до перенасичення ринку програмного забезпечення однотипними програмами.

- основою авторського права є унікальність об'єкта, що захищається ним, тобто неможливість незалежного створення ідентичного твору. Саме тому для визнання прав автора на твір не потрібно обов'язкова реєстрація. Відсутність унікальності, а серед комп'ютерних програм існує велика кількість аналогів, які однаково виконують ті самі функції, також суперечить основам авторського права і може розглядатися як підстава для порушення питання щодо правомірності віднесення програм до об'єктів авторського права

- на відміну від літературних творів, текст комп'ютерної програми (вихідний чи об'єктний код) не мають самостійної цінності без можливості їх застосування в комп'ютері. Отже, сприйняття комп'ютерної програми,

тобто, власне кажучи її тексту, відбувається не безпосередньо людиною, а опосередковано, за допомогою комп'ютера.

- ще один недолік авторського механізму охорони випливає зі способу написання більшості сучасних програм. Як відомо, програми не пишуться «з чистого листа», а створюються в середовищі розробки при використанні певної мови програмування. При цьому, програмісти в більшій чи меншій мірі використовують вже готові шаблонні конструкції, які є в середовищі розробки. З огляду авторського механізму охорони, будь-яка програма, створена в середовищі розробки (а це 80–90% від загальної кількості програм у світі), може вважатися складеним твором, з чим важко погодитися [34].

Авторське право розповсюджується на всі види комп'ютерних програм. Це можуть бути корпоративні інформаційні системи, Інтернет-клієнти, системи управління базами даних, засоби захисту, текстові й графічні редактори, відеоігри, драйвери різноманітних пристроїв тощо. Це можуть бути як прикладні програми, так і операційні системи, а також програмні комплекси. Програма може бути вбудована в сам процесор будь-якого технічного пристрою. Розмір програми, кількість використаних мов програмування, файлів чи рядків коду не має значення для охорони авторським правом.

Функціонально завершені елементи програми, наприклад, підпрограми, бібліотеки, модулі, об'єкти створені та використані для розробки програмного забезпечення також являються об'єктами авторського права.

Таким чином, авторським правом, як єдиний об'єкт, захищається комп'ютерна програма, яка складається з: вихідного кода, об'єктного кода, супровідних матеріалів та документації, отриманих в ході розробки програми, аудіовізуальні відображення програм.

Така позиція вітчизняного законодавця має свої як позитивні, так і негативні риси. Основною позитивною рисою такого виду захисту є те, що — права автора виникають з моменту створення комп'ютерної програми

(бази даних), реєстрація прав, яка має формальний характер, здійснюється за бажанням автора. Крім того, права автора будуть діяти протягом усього життя автора, та 70 років після його смерті, хоча, з іншого боку, користь від такого тривалого терміну дії незначна, тому що ринок програмного забезпечення стрімко розвивається, і на ринок швидко виходять нові версії програм. Основним недоліком подібного роду захисту є те, що авторське право захищає саму програму у формі вихідного тексту або об'єктного коду, а зміст (як процес, засіб) – авторським правом не охороняється. Отже, охороняється авторське вираження ідеї в конкретній матеріальній формі, це означає, що при захисті комп'ютерної програми має значення код, а не ідея, концепція, принципи, алгоритми [32]. На сьогодні вже непоодинокими є пропозиції про встановлення поряд з авторським правом патентної системи охорони для комп'ютерних програм. Так, у багатьох країнах комп'ютерні програми також визнаються й об'єктами патентної охорони (йдеться про випадки, коли комп'ютерна програма є частиною технологічного процесу, технічного пристрою тощо й сумісно з ними може бути визнана об'єктом патентної охорони). Так, наприклад, у Сполучених Штатах Америки, зважаючи на високий рівень розробки численних програмних продуктів, поряд з авторсько-правовою охороною комп'ютерних програм, також існує і патентно-правова охорона. Аналогічного підходу дотримується також і Японія. У численних країнах, таких як Бразилія, Угорщина, Ізраїль, Китай та інших, охорона комп'ютерних програм патентним правом стала можливою на базі наявних судових прецедентів [35].

Українське ж законодавство на сучасному етапі визначає комп'ютерні програми виключно як об'єкти авторського права. При цьому авторське право на комп'ютерну програму виникає в момент його створення і не потребує обов'язкової реєстрації.

Але зараз однієї «презумпції авторства» на комп'ютерну програму недостатньо, а тому враховуючи можливі порушення авторських прав в майбутньому, творці комп'ютерних програм вважають за краще

реєструвати свої права в Реєстрі й отримувати Свідоцтва про реєстрацію авторського права, оскільки це має ряд переваг.

По-перше, автори комп'ютерних програм, які зареєстрували об'єкт перебувають у виграшному становищі у разі виникнення непередбачуваних ситуацій. Офіційна реєстрація насамперед дає суттєву перевагу у випадках порушень, суперечок або розбіжностей. Закон установлює презумпцію належності авторського права на комп'ютерну програму тій особі, яка офіційно зареєструвала комп'ютерну програму як об'єкт авторського права. Це звільняє від необхідності спеціально доводити належність авторських прав. І навпаки, якщо хто-небудь буде заперечувати авторське право на комп'ютерну програму, то саме ця особа повинна буде доводити, в тому числі в суді, цей факт. А проблема доведення авторства є досить непростою при захисті авторських прав без свідоцтва.

По-друге, наявність свідоцтва дозволяє вільно розпоряджатися своїми правами на програму та делегувати їх третім особам.

По-третє, на сьогодні реєстрація авторських прав в нашій державі є одним з найдешевших і водночас швидких способів захистити свої права.

Разом з тим велика кількість авторів комп'ютерних програм не звертаються до Державної служби інтелектуальної власності України із заявою про отримання свідоцтва. З однієї сторони це є абсолютно вірним з огляду на наявність «презумпції авторства», проте з огляду на велику кількість порушень авторських прав на комп'ютерні програми ця практика повинна зазнати змін.

Комп'ютерна програма має свою специфіку як об'єкт авторського права, оскільки це не літературний твір, а набір інструкцій у вигляді слів, цифр, кодів, схем, символів тощо, що зчитуються комп'ютером. Комп'ютерну програму неможливо прочитати як певний письмовий твір. Тому фахівці пропонують показувати ім'я автора комп'ютерної програми у вихідному коді, в аудіовізуальних зображеннях, породжуваних комп'ютерною програмою, у супровідній

документації та на пакуванні носіїв екземпляра програми. Відтак при відкритті файлу з вихідним кодом можна побачити ім'я автора, за умови його розміщення.

Водночас суди не завжди вдаються до таких дій при розгляді спору. Автори не у всіх випадках вказують своє ім'я самим таким способом. Крім того, як слушно вказує О. С. Яворська, комп'ютерна програма нерідко створюється колективом авторів, і цей колектив може бути досить численним, зважаючи на складність комп'ютерного продукту, а відтак виникає питання щодо технічної можливості зазначення імен всіх авторів у примірнику комп'ютерної програми [36].

У випадку комп'ютерної програми норми авторського права можуть бути застосовані тільки для охорони від загального відтворення програми, а також від копіювання комп'ютерного коду (такі порушення входять до поняття «літературних»). Авторське право також забезпечує охорону комп'ютерних програм від деяких «нелітературних» порушень, таких яких відтворення екранних заставок (screen displays). Суттєвий недолік авторської охорони полягає в неможливості запобігти створенню конкуруючої комп'ютерної програми з використанням ідеї наявної програми.

Відповідно, на думку фахівців слід реєструвати окремі елементи комп'ютерних програм:

- реєстрація самого коду програми; як об'єкта авторського права;

- реєстрація алгоритму роботи комп'ютерної програми шляхом отримання патенту України на корисну модель або патенту на винахід як на спосіб (процес);

- реєстрація назви комп'ютерної програми — як торговельної марки.

З метою усунення цього недоліку авторського права останнім часом усе частіше й частіше в Україну подаються заявки на отримання патенту на винахід (корисну модель) для охорони та захисту алгоритму (способу) роботи комп'ютерної програми для розв'язання конкретної задачі.

Патент на винахід дає змогу захистити змістовий бік програмного забезпечення, патентна охорона

поширюється на сутність, що є основною ідеєю програми, втіленою в алгоритмі. Крім того, патент дає виключне право власності на саму ідею (якщо вона показана в істотних ознаках формули винаходу) і запобігає її несанкціонованому використанню. Перевага патентної охорони для комп'ютерних програм полягає у можливості захистити певний алгоритм, втілений у комп'ютерній програмі, від використання його іншими особами без дозволу.

Нині виключається віднесення програмних продуктів до винаходів, і як наслідок можливість їх патентування, проте для того, щоб все ж таки отримати патент, варто подати заявку на реєстрацію алгоритму програми в якості вирішення конкретного завдання. Алгоритм, його суть і етапи записуються у зрозумілій словесній формі, після чого підкріплюються діаграмами та блок-схемами. Після проходження алгоритму на патентоспроможність подається заявка на отримання патенту на винахід. Для проходження експертизи в патентному відомстві потрібна ретельна підготовка заявочної документації. З моменту подання документації до видачі патенту в середньому проходить два-три роки. Але, на думку фахівців, віднесення комп'ютерних програм до об'єктів промислової власності буде сприяти розвитку IT-індустрії і поширенню програмного забезпечення. Так, обов'язковою умовою патентування технічних рішень є те, що охоронний документ (патент на винахід або корисну модель) видається за умови розкриття суспільству його сутності (алгоритм у вигляді вихідного коду комп'ютерної програми повинен подаватися в патентне відомство в описі до патенту). Разом з тим обмежений термін охорони програмного продукту як об'єкта промислової власності забезпечував би перехід комп'ютерних програм у загальне користування через 5–7 років, що, безумовно, сприяло б вирівнюванню технологічного рівня розвитку комп'ютерних технологій в різних країнах і прискоренню його розвитку в більш розвинених країнах [35].

Реєстрація назв програм і сайтів, як торговельних марок у Державному департаменті інтелектуальної

власності може стати дієвим механізмом уникнення повного або ж часткового копіювання вже наявного якісного продукту у вигляді комп'ютерної програми. Така реєстрація дозволяє надійно захистити назви програм, баз даних і сайтів від крадіжки, а також отримувати прибуток від використання третіми особами, а власник зареєстрованої торговельної марки може вимагати відшкодування збитку від незаконного використання його торговельної марки, а також забороняти використання своєї торгової марки.

4.2.2. Веб-сайт як складний об'єкт права Інтелектуальної власності

Веб-сайт (Інтернет-сайт) є одиницею віртуального простору, за допомогою якої можна зберігати різноманітну інформацію, маючи доступ для ознайомлення та обміну з будь-якої точки планети.

На законодавчому рівні вперше було визначено поняття «веб-сайт» у спільному Наказі Державного комітету інформаційної політики, телебачення та радіомовлення України та Державного комітету зв'язку та інформатизації України «Про затвердження Порядку інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади та Порядку функціонування веб-сайтів органів виконавчої влади» від 25 листопада 2002 р. № 327/225, де зазначається, що веб-сайт – це сукупність програмних та апаратних засобів з унікальною адресою у мережі Інтернет разом з інформаційними ресурсами, що перебувають у розпорядженні певного суб'єкта й забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів, а також інші інформаційні послуги через мережу Інтернет. У цьому нормативно-правовому акті було надано визначення веб-сайту як певного поєднання технічної та інформаційної складових частин.

На рівні закону відповідне поняття законодавці затвердили лише 26 квітня 2017 р. у новій редакції Закону

України «Про авторське право і суміжні права» (Закон № 3792-XII), де зазначається, що **веб-сайт — це сукупність даних, електронної (цифрової) інформації, інших об'єктів авторського права і (або) суміжних прав, пов'язаних між собою і структурованих у межах адреси веб-сайту та (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики й (або) числової адреси за Інтернет-протоколом** [37]. З аналізу цього визначення стає зрозумілим, що законодавець у новій редакції Закону розширив поняття веб-сайту, зазначивши його як складний структурний об'єкт, що містить невизначену кількість елементів (причому не простих за своєю природою елементів, а окремих об'єктів права інтелектуальної власності), поєднаних між собою в особливому порядку. Отже, Закон визначає такі ознаки веб-сайту:

- за змістом веб-сайт є сукупністю даних, електронної (цифрової) інформації та інших об'єктів авторського права і (або) суміжних прав;
- всі інформаційні матеріали пов'язані між собою і структуровані у межах адреси веб-сайту та (або) облікового запису власника цього веб-сайту;
- доступ до веб-сайту здійснюється через адресу мережі Інтернет (доменне ім'я, запис про каталоги чи виклики і (або) числової адреси за Інтернет-протоколом).

У науковій літературі вчені (зокрема, Ю. Атаманова), розвиваючи цю тезу, наголошують, що: «Досягнення формальної та змістовної єдності веб-сайтом здійснюється завдяки трьом основним його складовим, а саме: 1) програмним та апаратним засобам (серверним програмним засобам; програмним засобам сайту); 2) адресі у мережі Інтернет або доменному імені; 3) інформаційному наповненню, яке охоплює текстову інформацію, графічну інформацію, аудіовізуальну інформацію» [38].

Проаналізувавши нормативну базу, розуміємо, що в неї відсутня пряма вказівка на приналежність веб-сайту до об'єктів права інтелектуальної власності, як і в інших нормативно-правових актах, а саме у ст. 8 Закону України

«Про авторське право і суміжні права» та ст. 420 ЦКУ веб-сайт до переліку об'єктів авторського права та переліку об'єктів права інтелектуальної власності не включений. При цьому до переліку об'єктів авторського права у ст. 8 Закону України «Про авторське право і суміжні права» включено «інші твори», тому виникає спір між науковцями щодо того, чи є веб-сайт окремим об'єктом права інтелектуальної власності або він є просто носієм інформації, яка належить до об'єктів права інтелектуальної власності [39].

Більшість фахівців з інтелектуальної власності згодна з тим, що веб-сайт це об'єкт права інтелектуальної власності. Однак питання, до якого інституту цього права зазначений об'єкт належить, залишається відкритим. У науковій та практичній літературі зустрічаються позиції, за якими науковці відносять веб-сайт до: різновиду комп'ютерної програми; сукупності графічних, візуальних, літературних та інших творів, кожен з яких є самостійним об'єктом авторського права; складеного твору; бази даних; окремого файлу, який зчитує комп'ютерна програма.

На наш погляд, Інтернет-сайт як об'єкт ІТ-права та права інтелектуальної власності — складне явище, яке містить елементи різних правових понять. Окрім поняття «Інтернет-сайт» в якості його синоніму у науковій літературі та в чинному законодавстві вживається також поняття «веб-сайт». Веб-сайт як об'єкт ІТ-права потребує інтелектуальної творчої праці для створення та належного функціонування. Інтернет-сайт не існує поза межами Інтернету.

Інтернет-сайт — це складний об'єкт ІТ-права та права інтелектуальної власності, оскільки:

- містить програмні засоби (відповідні комп'ютерні програми, завдяки яким веб-сайт функціонує);
- має інформаційне наповнення (тексти, зображення тощо);
- має унікальне ім'я (доменне ім'я);
- інформація, що міститься на веб-сайті, зберігається на віддаленому комп'ютері (цей процес характеризується як хостинг);

- доступ до Інтернет-сайту можливий із будь-якого комп'ютера (чи іншого пристрою), підключеного до мережі Інтернет, завдяки використанню відповідного програмного забезпечення (публічний доступ будь-якої особи). З наведених ознак убачається, що без відповідного програмного забезпечення функціонування Інтернет-сайту з технічної точки зору неможливе. Йдеться, зокрема, про комп'ютерні програми, які працюють «всередині» веб-сайту. Відповідно до загального правила правова охорона комп'ютерної програми здійснюється авторським правом. Водночас комп'ютерна програма може бути складовою винаходу (корисної моделі), що виконує певну функцію в межах винайденого технічного рішення [40].

Інформаційне наповнення Інтернет-сайту – це, як правило, інтелектуальна власність певної особи. На веб-сайті можуть бути розміщені об'єкти авторського права (тексти, малюнки, музичні твори тощо), суміжних прав (приміром, фонограми, відеограми), об'єкти патентного права (наприклад, зображення промислового зразка), засоби індивідуалізації (зокрема, комерційне найменування, зображення знака для товарів і послуг) тощо. У більшості випадків на веб-сайтах розміщують саме об'єкти авторського права, зважаючи на те, що в основному веб-сторінки – це текстова інформація. Інтернет-сайт має доменне ім'я, яке є унікальним. Зазвичай доменне ім'я показує або знак для товарів і послуг, або комерційне найменування, або ім'я фізичної особи. Відтак, у багатьох випадках використання домену (як назви Інтернет-сайту) – спосіб використання таких об'єктів права інтелектуальної власності, як торговельна марка чи комерційне найменування. Відповідно до ст. 20 Закону України «Про охорону прав на знаки для товарів і послуг» порушенням прав власника свідоцтва на знак для товарів і послуг вважається використання знака без його згоди в доменних іменах. Доменне ім'я становить частину системи доменних імен та функціонально забезпечує адресацію в мережі Інтернет.

Отже, можна погодитися з позицією науковців, що **веб-сайт** виступає **комплексним** за структурою, **окремим і**

самостійним об'єктом права інтелектуальної власності у сфері авторського права, оскільки під час створення потребує використання творчих здібностей людини та не має чітко визначеної структури, а саме може складатися з різних об'єктів права інтелектуальної власності, в різних комбінаціях та з особливим їх впорядкуванням, що, як наслідок, породжує оригінальність та унікальність кожного веб-сайту, тобто, поєднуючи різнорідні за своїм характером об'єкти, веб-сайт має ознаки, що не є сукупністю ознак його складових частин. При цьому додатковими ознаками приналежності до авторського права для веб-сайту є те, що останній належить до творів мистецтва, науки, літератури, має об'єктивну форму вираження через своє програмне забезпечення й поширення в мережі Інтернет, а також є відтворюваним [39]. За змістом веб-сайт є сукупністю даних, електронної (цифрової) інформації та інших об'єктів авторського права і (або) суміжних прав, а всі інформаційні матеріали Інтернет-сайту пов'язані між собою та структуровані у межах адреси веб-сайту і (або) облікового запису власника цього веб-сайту.

4.2.3. Авторські права на службовий твір

Питання визначення виключних майнових авторських прав (ВМАП) на службовий твір є дуже актуальним, оскільки багато творів, зокрема в сфері ІТ-технологій, створюються як службові твори. Важливість цієї теми полягає також в тому, що в цій ситуації є два суб'єкти правовідносин, які мають правові підстави бути авторами — працівник та роботодавець, а також різні підходи в законодавстві Україні щодо регулювання цього питання.

У зв'язку з тим, що роботодавець не завжди добросовісно підходить до питання належності ВМАП на службовий твір, це породжує багато проблем в майбутньому щодо розпорядження цими правами.

Окрім того, набрання чинності положеннями Угоди про асоціацію України з ЄС, яка вносить певні

нововведення до питання про правове регулювання ВМАП, підкреслює потребу аналізу вищевказаних питань.

Нормативна база: Бернської конвенції про охорону літературних і художніх творів, Паризький Акт від 24 липня 1971 року, змінений 2 жовтня 1979 року (далі – Бернська конвенція), Цивільного кодексу України, Кодексу законів про працю України, Закону України «Про авторське право і суміжні права» та інших нормативно-правових актів.

На сучасному етапі існує термінологічна неузгодженість щодо терміну «службовий твір» загального закону (Цивільного кодексу України зі спеціальним законом (Законом України «Про авторське право і суміжні права». Так, у ст. 429 ЦК України, на відміну від ст. 16 Закону України «Про авторське право і суміжні права», законодавець не оперує поняттям «службовий твір», а використовує словосполучення «об'єкт, створений у зв'язку із виконанням трудового договору». У наведених вище статтях законів існує ще одна парадоксальна ситуація. Так, у ст. 16 Закону закріплено, що службовий твір створює автор за трудовим або цивільно-правовим договорами. У той час, як у ст. 429 ЦК України з'являється працівник, у якого відсутні будь-які авторські права на службовий твір, оскільки законодавством України про авторське право цього не передбачено. Положення ст. 429 ЦК України вступає у розбіжність з ч. 1 ст. 435 ЦК України, якою закріплено, що первинним суб'єктом авторського права є саме автор твору, а не працівник.

Виходячи із вищевикладеного, на практиці, говорячи про службові твори поняття «автор» і «працівник», застосовують в однаковому значенні.

Службовий твір є об'єктом авторського права. У чинному законодавстві немає визначення поняттю «твір», але вказується на його ознаки. Перш за все, твір є результатом творчої діяльності. Показником творчого характеру, на думку багатьох вчених, є його оригінальність, що виражається у новому змісті, новій формі, ідеї, концепції та ін. У цьому сенсі кожний твір є новим, оригінальним, неповторним. Це означає, що два

різних автори ніколи не напишуть два однакові твори. Якщо це відбувається, то говорять про плагіат. Якщо якесь творення не є результатом творчої праці, то така робота не може бути визнана твором і, отже, об'єктом авторського права. Не вважається об'єктом авторського права суто технічна робота (наприклад, передрук на друкарській машинці чи набір на комп'ютері чужого твору або навіть його літературна обробка – редагування, коректура тощо).

Другою ознакою твору є наявність об'єктивної форми (ч. 3 ст. 8 Закону), що робить його доступним для сприйняття, допускає можливість відтворення. Форма вираження твору може бути усна, письмова, звуко- чи відеозапис, зображення, об'ємно-просторова тощо. Розвиток науки і техніки породжує все нові форми вираження твору.

Визначення поняття «Службовий твір»

Службовий твір – це твір, створений автором у порядку виконання службових обов'язків відповідно до службових завдань або трудового договору (контракту) між ним і роботодавцем (ст. 1 Закону України «Про авторське право і суміжні права»).

Службовим вважається твір:

- створений за трудовим договором або за цивільно-правовою угодою і в порядку їх виконання;
- пов’язаний із трудовими обов’язками працівника, визначеними в трудовому договорі, посадових інструкціях чи інших документах роботодавця і працівник із ними ознайомлений;
- створений за окремим дорученням роботодавця

Закон не дає визначень понять службових обов'язків і службового завдання. Коло службових обов'язків працівника визначається посадовими інструкціями, положеннями про структурні підрозділи, статутами організацій і підприємств. Службовим зазвичай є конкретне завдання працівникові, що виходить від роботодавця в особі її органів і зафіксоване в документації, з якої працівник був ознайомлений до створення твору.

Виконання роботи може бути здійснено як протягом робочого часу, так й у позаробочий час, незалежно від місця створення службового твору; як із застосуванням засобів і матеріалів, що належать роботодавцю, так і без застосування таких засобів та матеріалів.

Суб'єкти права інтелектуальної власності на службові твори

У випадку авторсько-трудових відносин **суб'єктами** права інтелектуальної власності на службові твори є **роботодавець** (юридична або фізична особа, де або в якої працює автор) і **найманий працівник** (автор).

Роботодавець — особа, яка найняла працівника за трудовим договором (контрактом) (ст. 1 Кодексу законів про працю України). *Автор* — фізична особа, яка своєю творчою працею створила твір (ст. 1 Закону). Автор може бути штатним або позаштатним працівником.

У ст. 429 ЦК України замість терміну «роботодавець» використовується термін «юридична або фізична особи, де або у якої працює працівник». Під «фізичною особою, де або у якої працює працівник» необхідно розуміти фізичну особу, зареєстровану як суб'єкт підприємницької діяльності, оскільки фізична особа — не підприємець не може виконувати функції роботодавця у відносинах з автором.

Службові твори можуть бути створені спільною творчою працею авторів (колективом авторів). У такому випадку виникає співавторство. Твір, створений у співавторстві, належить всім співавторам незалежно від того, чи утворює такий твір одне нерозривне ціле або складається із частин, кожна з яких має самостійне значення. Відносини між співавторами можуть бути визначені договором. У разі відсутності такого договору авторське право на твір здійснюється всіма співавторами спільно. Винагорода за використання твору належить співавторам у рівних частках, якщо в договорі між ними не передбачається інше (ст. 436 ЦК України, ст. 13 Закону). У разі створення службового твору співавторами, слід враховувати, що стороною договору, укладеного з

роботодавцем, може бути не окремий автор, а співавтори (колектив авторів).

Особливості трудових прав та обов'язків працівників щодо створення певних творів у галузі науки, літератури і мистецтва визначені спеціальними законами, зокрема:

- ст. 30 Закону України «Про архітектурну діяльність» (щодо прав та обов'язків творчих працівників у сфері архітектурної діяльності);
- ст. 60 Закону України «Про телебачення і радіомовлення» (щодо прав та обов'язків творчих працівників телерадіоорганізацій);
- ст. 49, 50 Закону України «Про вищу освіту» (щодо прав та обов'язків педагогічних та науково-педагогічних працівників);
- ст. 11, 16 Закону України «Про кінематографію» (щодо прав та обов'язків авторів, виконавців та виробників фільму);
- ст. 6, 32 Закону України «Про інформаційні агентства» (щодо прав та обов'язків творчих працівників інформаційних агентств).

Особисті немайнові права на службові твори

Відповідно до статті 6 bis Бернської конвенції про охорону літературних і художніх творів передбачено, що незалежно від майнових прав автора і навіть після поступки прав він має право вимагати визнання свого авторства на твір і протидіяти будь-якому перекрученню, спотворенню чи іншій зміні цього твору, а також будь-якому іншому посяганню на твір, здатному завдати шкоди честі або репутації автора. Зазначені права, визнані за автором, зберігають силу після його смерті принаймні до припинення майнових прав і здійснюються особами або установами, уповноваженими на це законодавством країни, в якій вимагається охорона.

За чинним українським законодавством особисті немайнові права інтелектуальної власності на об'єкт, створений у зв'язку з виконанням трудового договору, належать працівникові, який створив цей об'єкт (ч. 1 ст. 429 ЦК України, ст. 16 Закону України «Про авторське право і

суміжні права»). До особистих немайнових прав, зокрема, належать: право вимагати визнання свого авторства шляхом зазначення імені автора на творі та його примірниках; право вибирати псевдонім, зазначати й вимагати зазначення псевдоніма замість справжнього імені автора на творі та його примірниках; право вимагати збереження цілісності твору й протидіяти будь-якому перекрученню, спотворенню чи іншій зміні твору або будь-якому іншому посяганню на твір, що може зашкодити честі й репутації автора, а також супроводженню твору без його згоди ілюстраціями, передмовами, післямовами, коментарями тощо. Особисті немайнові права автора не можуть бути передані (відчужені) іншим особам.

У разі смерті автора недоторканність твору охороняється особою, уповноваженою на це автором. За відсутності такого уповноваження недоторканність твору охороняється спадкоємцями автора, а також іншими зацікавленими особами (ст. 439 ЦК України).

Частиною першою статті 429 ЦК України встановлено, що у випадках, передбачених законом, окремі особисті немайнові права інтелектуальної власності на об'єкт, створений у зв'язку з виконанням трудового договору, можуть належати юридичній або фізичній особі, де або у якої працює працівник. Однак, норми спеціального закону (Закону України «Про авторське право і суміжні права») не встановлюють таких випадків належності особистих немайнових прав іншим особам, у тому числі роботодавцю.

Майнові права інтелектуальної власності на службові твори

Майновими правами інтелектуальної власності на твір є:

- право на використання твору;
- виключне право дозволяти використання твору;
- право перешкоджати неправомірному використанню твору, в тому числі забороняти таке використання;
- інші майнові права інтелектуальної власності, встановлені законом.

Нині діють два законодавчі акти у сфері авторського права: ЦК України та Закон України «Про авторське право і суміжні права». Між цими законами є протиріччя (колізія) в частині належності майнових прав на службові твори.

Так, відповідно **до ЦК України** (частина 2 ст. 429) **майнові права на твір**, створений у зв'язку з виконанням трудового договору, **належать працівникові і роботодавцю спільно**, якщо інше не встановлено у трудовому договорі. Відповідно до **Закону України** «**Про авторське право і суміжні права**» (частина 2 ст. 16) **майнові права** на службовий твір **належать роботодавцю**, якщо в трудовому договорі не встановлено інше.

Необхідно зазначити, що Закон України «Про авторське право і суміжні права» є спеціальним законом у сфері авторського права. У зв'язку з цим деякі роботодавці дотримуються тієї точки зору, що при розв'язанні питання належності майнових прав на службовий твір слід застосовувати норму саме цього Закону. Тому, що є загальноприйняте правило про те, що якщо виявлено протиріччя між загальним і спеціальним нормативно-правовим актом, то перевага віддається спеціальним актом. З метою врегулювання цієї колізії законодавчих актів, Пленум Верховного Суду України в Постанові «Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав» від 4 червня 2010 року № 5 в пункті 24 дав роз'яснення щодо цього питання, і визначив, що працівник та роботодавець мають спільні ВМАП. У даній ситуації Верховний Суд України керувався, тим, що норма Цивільного кодексу України є новішою у порівнянні з нормою Закону і застосував саме її.

Однак треба зазначити, що 01.09.2017 року набрала чинності Угода про асоціацію з Європейським Союзом від 16.09.2014 року. Ця Угода є важливою не лише в ракурсі європейської інтеграції України, але містить важливі питання правового регулювання різних правовідносин. Угода про асоціацію включає також цілий розділ щодо правового регулювання інтелектуальної власності. Зокрема, містить окремі положення щодо регулювання

комп'ютерної програми, як об'єкта права інтелектуальної власності (об'єкт ІВ), правове регулювання декомпіляції, суб'єктів, які можуть претендувати на авторство тощо.

У ч. 4 ст. 181 розділу 9 Угоди є положення щодо належності виключних майнових прав працівників, а саме чітко вказано, що *права на комп'ютерну програму, створену найманим працівником належать роботодавцю.* Згідно ст. 9 Конституції України, міжнародні договори, які ратифіковані Верховною Радою України, є складовою українського законодавства. А відтак, оскільки Угода про асоціацію України з Європейським Союзом, містить інші правила щодо правового регулювання сфери належності виключних майнових прав працівників, то слід застосовувати саме правила, визначені Угодою. Нагадаємо, що вищевказана Угода встановлює належність виключних майнових прав працівників на твір, створений працівником, роботодавцю. Зважаючи на вищевказану правову колізію з питань регулювання належності виключних майнових прав працівників на службові твори, наразі не відомо яку саме норму законодавства будуть застосовувати українські суди. Враховуючи те, що кожен ІТ-продукт створюється найманим працівником відповідно до певних технічних завдань, визначених роботодавцем і його кінцевою метою є продаж клієнту, питання належності виключних майнових прав працівників роботодавцеві є дуже важливим. Більша частина ІТ-сфери в Україні орієнтована все ж таки на іноземного клієнта, відтак простота передачі виключних майнових прав працівників має надважливе значення. Враховуючи швидкий розвиток сфери ІТ-технологій в Україні та вихід з відповідними продуктами на міжнародний рівень, є нагальна потреба у розв'язанні цієї проблеми [41].

Відтак для виключення конфліктних ситуацій з приводу використання службового твору, сторони правовідносин (роботодавець і працівник) мають укласти письмовий трудовий договір, який повинен містити положення щодо обов'язку працівника створювати відповідні службові твори, як об'єкт інтелектуальної

власності, розмір та порядок виплати авторської винагороди та положення про закріплення майнових прав на створені працівником службові твори за роботодавцем.

Запитання для самоконтролю і самостійного опрацювання

1. Розкрийте зміст Договору ВОІВ з авторського права
2. У чому полягає основний зміст Договору ВОІВ про виконання і фонограми?
3. У чому полягає суть понять «творча діяльність» і «інтелектуальна діяльність»?
4. Визначте основний статус Інтернет-договорів ВОІВ.
5. Чи може штучний інтелект набувати прав автора об'єкта інтелектуальної власності?
6. Які правові наслідки слід очікувати після надання штучному інтелекту правосуб'єктності?
7. Як здійснюється охорона авторського права в цифровому середовищі?
8. Якими документами здійснюється правове регулювання відносин щодо використання прав інтелектуальної власності в мережі Інтернет в країнах ЄС?

Рекомендована література:

1. Рекомендації для Інтернет-провайдерів, контент-провайдерів та користувачів файлообмінних мереж та інших веб-сервісів щодо правомірного використання об'єктів авторського права і суміжних прав у мережі Інтернет, затв. Державною службою інтелектуальної власності України. URL: http://sips.gov.ua/ua/ip.html?s=print
2. Авторське право та авторознавча лінгвістична експертиза у цифрову добу : монографія / О. І. Харитонова, Н. І. Клименко, Є. О. Харитонов, Г. О. Ульянова, Г. І. Григорянц; за ред. О. І. Харитонової, Н. І. Клименко. — Одеса : Фенікс, 2017. — 270 с.
3. Тарасенко Л. Л. Об'єкти авторського права у цифровому середовищі. *Вісник Львівського університету. Серія юридична*. 2019. Випуск 68. — С. 231–239.
4. Тарасенко Л. Л. Інтернет-сайт як об'єкт ІТ-права. *Право України*. — 2018. №3. — С. 103-113.
5. Тарасенко Л. Л. Комп'ютерна програма як об'єкт інтелектуального права // ІТ-право: проблеми і перспективи

розвитку в Україні: збірник матеріалів науково-практичної конференції. — Львів : НУ «Львівська політехніка», 2016. — С. 251.

6. Венедіктова І. Авторське право на елементи літературного твору у комп'ютерній відеогрі. *Право України.* . — 2018. №3. — С. 91-102.

7. Жилінкова О. Договірне регулювання відносин щодо інтелектуальної власності у сфері інформаційних технологій. *Право України.* — 2018. №3. — С.137-145.

8. Резворович К. (2021). Право інтелектуальної власності у мережі Інтернет: недоліки вітчизняного нормативно-правового регулювання та шляхи його вдосконалення. *Interconf.* (78). — С. 255-261. https://doi.org/10.51582/interconf.7-8.10.2021.028

9. Позиція Інституту Медіа-Права щодо законопроекту про захист авторських прав в Інтернеті. Центр демократії та верховенства права. URL: http://www.medialaw. kiev.ua/news/ organization/2454

10. Державні реєстри // Офіційний веб-портал Державної служби інтелектуальної власності. URL: http://sips.gov.ua/ua/registers.html

11. Зазначення походження товару // Офіційний веб-портал Державної служби інтелектуальної власності. URL: http://sips.gov.ua/ua/origin_commodity.html

12. Знаки для товарів та послуг // Офіційний веб-портал Державної служби інтелектуальної власності. URL: http://sips.gov.ua/ua/signs.html

13. Зразки примірних договорів у сфері авторського права і суміжних прав // Офіційний веб-портал Державної служби інтелектуальної власності. URL: http://sips.gov.ua/ua/zrazkydogap.html

РОЗДІЛ 5.

ДОГОВІРНІ ВІДНОСИНИ В ЦИФРОВОМУ СЕРЕДОВИЩІ

5.1. Загальна характеристика договорів у цифровій сфері

З розвитком цифрового середовища виникає необхідність у правовому обґрунтуванні та закріпленні правових норм, що встановлюватиме та регулюватиме можливість укладання договорів на використання цифрового середовища. Важливим є адаптування іноземних нормативних положень та положень договорів для українського споживача та створення відповідного підґрунтя на вітчизняному законодавчому рівні, враховуючи, що на сьогодні відсуне нормативно-правове регулювання даної сфери.

У науковій і практичній літературі доволі часто вживаються такі поняття «цифрове середовище», «мережа Інтернет», «сфера ІТ» Тому важливо з'ясувати співвідношення між ними. Визначення поняття «цифрове середовище» у законодавстві України не наводиться. Однак, в науковій літературі це словосполучення використовується в юридичній лексиці. Цифрове середовище показує як цифрову форму об'єкта інтелектуальної власності, так і надає новий зміст правам інтелектуальної власності.

Поняття цифрове середовище ширше, ніж поняття мережа Інтернет. Цифрове середовище охоплює не лише веб-сайти, веб-сторінки, а й електронні документи, файли, в тому числі цифрові об'єкти інтелектуальної власності, які використовуються на відповідних пристроях, що не передбачають паперову форму документообігу (комп'ютери, ноутбуки, планшети, телефони та інше).

У сфері цифрового середовища діють загальні норми цивільного права, але дуже часто правовідносини регулюються непойменованими договорами або договорами, що мають комплексний характер, тобто містять положення, характерні для різних видів цивільно-правових угод. Крім того, велике значення має питання, яке право застосовується до договору, що укладається у цифровому середовищі, оскільки їх більшість укладається між представниками різних країн, які ніколи не бачили один одного.

Сфера цифрового середовища (IT) — одна з найбільш специфічних в частині договорів. Це пов'язано, перш за все, з транснаціональністю бізнесу та його динамічністю.

Зважаючи на те, що вітчизняне законодавство на сьогодні не встигає за динамікою розвитку сфери IT, відносини між учасниками цифрового середовища регулюються переважно на договірних засадах. Разом з тим, зростає і кількість договорів спрямованих на використання безпосередньо цифрового середовища. Проте єдиного розуміння серед науковців та в законодавстві різних країн правової природи договорів у даній сфері не існує. У зв'язку, з чим ні в судовій практиці, ні в доктрині не вироблено єдиного підходу щодо даного питання.

Серед можливих варіантів кваліфікації договорів в даній сфері, можна виділити договір на розробку, модернізацію, дебаг, тестування програмного забезпечення, договір на розробку веб-сайту, договір на розробку мобільного застосунку, договір на розробку з застосуванням VR/AR, договір на пошукову оптимізацію, договір про надання послуг в сфері інформатизації, договір на технічну підтримку, договір на хмарні послуги, договір найму (оренди), ліцензійний договір, договір надання послуг, змішаний договір, непоіменований договір тощо.

Як наслідок, законодавча невизначеність щодо врегулювання зазначених відносин призвели до паралельного існування декількох видів договорів між учасниками відносин в IT-сфері.

Велика кількість учасників договірних відносин у сфері ІТ є іноземними компаніями, які з'являються на українському ринку з усталеними підходами у сфері надання доступу до цифрового середовища. Однак, зазвичай такі підходи складно адаптувати до українських правових реалій. У результаті в цивільному обороті виникають договірні конструкції, що опосередковують використання інформаційних цифрових технологій користувачами, юридична природа яких потребує ретельного правового аналізу.

Вважаємо що у даній сфері є доцільним запозичувати іноземний досвід регулювання даних відносин. Якщо регулювання питань, що стосуються загальних положень договорів в Україні й інших країнах більш-менш схожі, то в інших питаннях (наприклад, щодо відповідальності сторін, предмету договору, визначення термінології), відмінності можуть бути істотними. Використовувати іноземний досвід у регулюванні договірних відносин у цифровому середовищі не тільки можна, але й потрібно.

Розвиток цифрового середовища та ІТ-сфери в цілому значно випереджає їх нормативно-правове забезпечення. На сьогодні Україна прагне залишатись активним учасником відносин у цій сфері, та вносити у національне законодавство зміни з обов'язковим врахуванням подальшого розвитку цифрового середовища.

У цифровому середовищі предмет договору – це програмна розробка, верстка, тестування, просування і т.д. Договори у сфері інформаційних технологій, заведено називати кастомними або вузькоспеціалізованими, через специфіку предмета договору, системи оплати, гнучкості термінів. Договір виконує функції захисту інтересів замовника і розробника при реалізації технічного завдання. У разі виникнення суперечок між сторонами з приводу виправлення багів, змін технічного завдання протягом спринту, помилки при роботі інтегрованих систем – договір допомагає розв'язувати проблемні питання шляхом переговорів. Використовуючи договірні конструкції впорядковуються терміни, умови оплати та відповідальність за порушення домовленостей.

У цифровому середовищі договори бувають ***односторонні –*** публічна оферта, в якій однією стороною виступає компанія-розробник з іншого боку необмежену кількість фізичних і юридичних осіб; ***двосторонні*** – договори на розробку веб-сайту, що укладаються між замовником і розробником; ***багатосторонні*** – договори на розробку софтверних рішень, укладаються між генеральним підрядником і замовником.

Договірні відносини у сфері ІТ мають строковий характер, тому договори поділяються на ***безстрокові***, які укладаються по системі Time&Material[1] виходячи з кількості спринтів; ***строкові***, що укладаються на умовах Fixed Price[2], терміном на 3, 6 або 12 місяців; ***проєктні***, які укладаються на умовах змішаної системи оплати та терміни виконання договору залежать від результатів розробки.

Враховуючи вищенаведене за системою оплати ІТ-договори класифікуються на:

- Time&Material – продаж людино-годин;
- Fixed Price – фіксована оплата за кількістю та найменування послуг.

За характеристикою предмета договори у сфері ІТ можуть поділятись на наступні:

- договір на розробку сайту
- договір на розробку програмного забезпечення чи додатку;
- договір на розробку програмного рішення для бізнесу;
- договір на технічне обслуговування;
- договір на SEO, PPC;
- договір на впровадження програмних систем;

---

[1] T&M це модель роботи, коли оплачується не результат, а час виконавця. Наприклад, оплата за договором здійснюється не за розробку та впровадження програми управління підприємством, а за людино-години, що витрачені виконавцем на розробку програми.

[2] Fixed price (з фіксованою ціною) договір – це проєктний договір на розробку програмного забезпечення, в якому сторони домовилися про результати роботи в Технічному завданні (Statement of Work) ще на початку своїх договірних відносин.

- договір на верстку, тестування, копірайт на графічний дизайн;

- договір про відчуження авторських прав і т.д.

5.2. Ліцензійний договір

Ліцензійний договір є ключовим договором у сфері ІТ, та широко використовується з метою розповсюдження та дистрибуції програмного забезпечення.

Цивільний кодекс України визначає, що *ліцензійний договір* — це договір, за яким одна сторона (ліцензіар) надає другій стороні (ліцензіату) дозвіл на використання об'єкта права інтелектуальної власності (ліцензію) на умовах, визначених за взаємною згодою сторін з урахуванням вимог законодавства (ч. 1 ст. 1109 ЦК України).

У випадку укладення ліцензійного договору відбувається добровільне звуження прав володільця виключних майнових прав інтелектуальної власності, оскільки розширюється коло осіб, які можуть використовувати належний йому результат творчої діяльності. Інакше кажучи, укладаючи ліцензійний договір, правовласник ніби знімає з контрагента встановлену законодавством заборону на використання зазначеного об'єкта інтелектуальної власності.

З огляду на правові підходи в ЦК України ліцензійний договір набув значення універсального договору, який може слугувати правовою підставою використання будь-якого об'єкта інтелектуального права.

Ліцензійний договір, судячи з його визначення у ч. 1 ст. 109 ЦК України, моделюється як договір ***реальний*** — одна сторона *надає* іншій стороні дозвіл (ліцензію) на використання об'єкта інтелектуального права.

Тобто, договір мав би вважатися укладеним з моменту досягнення домовленості сторін з усіх його істотних умов та видачі дозволу (ліцензії) на використання відповідним об'єктом. Сама ліцензія може бути оформлена як окремий документ, або бути складовою ліцензійного договору. У ліцензійному договорі, відповідно до ч. 3 ст. 1109 ЦК України, визначаються усі умови, які сторони

вважають доцільним включити у договір. З факту досягнення відповідних домовленостей виникають взаємні зобов'язання для сторін договору. Реальна конструкція договору не знаходить свого підкріплення в інших правових нормах. Тому немає підстав, опираючись лише на дефініцію договору, стверджувати про його реальний характер. Таким чином, ***ліцензійний договір є консенсуальним***.

Укладений договір породжує взаємні права та обов'язки для його сторін, тому це договір є ***взаємозобов'язуючим.***

У ліцензіата (сторони, яка отримує ліцензію на використання певного об'єкта) виникає обов'язок використовувати цей об'єкт відповідно до погоджених у договорі умов та виду ліцензії на користування об'єктом, якому кореспондує право ліцензіара вимагати дотримання відповідних умов користування. Ліцензіат має право вимагати забезпечення нормального використання погодженого об'єкта з кореспондуючим йому обов'язком ліцензіара тощо.

У законодавчій дефініції договору нічого не зазначено про грошовий еквівалент надання дозволу на використання. Своєю чергою, презумпція відплатності договору, виходячи з положень частини 5 ст. 626 ЦК України не спростована, а у частині 3 ст. 1109 ЦК України йдеться про те, що у ліцензійному договорі визначаються розмір, порядок і строки виплати плати за використання об'єкта права інтелектуальної власності. Тому ***ліцензійний договір є оплатним,*** але така характеристика не виключає можливості його сторін домовитися про безоплатне використання об'єкта.

Ліцензійний договір завжди ***має строковий характер***. Строк є істотною умовою договору, виходячи з положень ст. 1110 ЦК України. Оскільки за ліцензійним договором передаються майнові права інтелектуальної власності, які мають часові межі чинності, які встановлені законом, а саме для майнових авторських прав або визначені патентами чи свідоцтвами, то у будь-якому разі строк

договору не може перевищувати граничних строків чинності цих прав.

Сторонами ліцензійного договору є ліцензіар і ліцензіат, якими можуть бути як фізичні, так і юридичні особи.

Ліцензіар – це особа, яка надає дозвіл (ліцензію) на використання об'єкта інтелектуального права. Тому ліцензіар – це фізична або юридична особа, яким належать виключні права надавати дозвіл на використання відповідного об'єкта. Такою особою не завжди є творець об'єкта. Окрім автора, ліцензіарами можуть бути: правонаступники або роботодавець, якщо їм належать майнові права, та інші особи, які на законних підставах набули виключних прав на розпорядження відповідним об'єктом.

До того ж такі права можуть належати кільком особам спільно. У такому разі слід ураховувати правила ст. 428 ЦК України. Права інтелектуальної власності, які належить кільком особам спільно, можуть здійснюватися за договором між ними. У разі відсутності такого договору, такі права здійснюються спільно. Тобто, у разі укладення ліцензійного договору та видачі ліцензії на використання об'єкта, права на який належать спільно кільком особам, усі вони повинні виявити спільну волю щодо укладення договору та видачі ліцензії на його підставі. Відповідно, у такому разі сторона ліцензіара буде представлена множинністю осіб, які є однією стороною договору.

Ліцензіар може укласти декілька договорів щодо одного і того ж об'єкта інтелектуального права на різних умовах. Законом не передбачено необхідності одержання згоди ліцензіата за раніше укладеними ліцензійними договорами на передання виключних майнових прав інтелектуальної власності іншій особі. В силу ч. 2 ст. 1113 ЦК України перехід виключного майнового права інтелектуальної власності до іншої особи не є підставою для зміни або розірвання раніше укладеного ліцензійного договору.

Ліцензіар як сторона договору має відповідати загальним правовим вимогам щодо суб'єктного складу

договору. Статус особи як суб'єкта підприємництва, його громадянство, інші соціальні характеристики не мають правового значення.

Ліцензіат – фізична чи юридична особа, яка на підставі договору отримує дозвіл на використання об'єкта інтелектуальних прав у визначених межах та на певний строк. Ця сторона договору може бути представлена як однією, так і більшою кількістю осіб. Ліцензіат має відповідати загальним правовим вимогам щодо суб'єктного складу договору. Жодних спеціальних вимог щодо нього не встановлено.

Сторони можуть діяти як особисто, так і через представника. Представником може бути будь-яка особа, що діє відповідно до правил глави 17 ЦК України про представництво.

Укладення та форма ліцензійного договору. У ЦК України, та у спеціальних актах не встановлені особливі правила щодо укладення ліцензійного договору. Тому цей договір укладається відповідно до загальних правил укладення цивільних договорів відповідно до глави 53 ЦК України. Тобто, ліцензійний договір може укладатися вільно шляхом досягнення взаємних домовленостей за результатами усних переговорів між сторонами, та з використанням електронних засобів тощо.

Права та обов'язки сторін ліцензійного договору. З факту укладення ліцензійного договору у письмовій формі у його сторін виникають взаємні права та обов'язки.

Основними обов'язками ліцензіара є:

1) передати ліцензіату об'єкт інтелектуального права, включаючи передання всієї необхідної інформації та технічної документації, що забезпечує його використання відповідно до погоджених умов;

2) забезпечити ліцензіату безперешкодне використання цього об'єкта в обумовлених межах;

3) не розголошувати змісту предмета ліцензії;

4) не передавати об'єкт інтелектуального права третім особам, якщо інше не передбачено договором тощо.

Цим обов'язкам кореспондують відповідні **права ліцензіата:**

1) вимагати передання об'єкта інтелектуального права разом з усією документацією, що забезпечує його використання на погоджених умовах;

2) на використання об'єкта інтелектуального права в межах, обумовлених ліцензійним договором;

3) вимагати від ліцензіара забезпечення належних умов використання об'єкта інтелектуального права;

4) на негайне та безоплатне передання ліцензіаром усіх подальших удосконалень предмета ліцензії, якщо це передбачено договором тощо.

Основними обов'язками ліцензіата є:

1) сплачувати винагороду за використання об'єкта інтелектуального права, якщо така встановлена умовами договору;

2) використовувати об'єкт інтелектуального права у межах наданої ліцензії;

3) надавати інформацію про межі використання об'єкта інтелектуального права, отримані прибутки, а також зроблені удосконалення тощо.

Цим обов'язкам кореспондують **права ліцензіара:**

1) на отримання винагороди за ліцензійним договором, якщо така встановлена умовами договору;

2) вимагати від ліцензіата використовувати об'єкт інтелектуального права відповідно до умов договору;

3) на інформацію про межі й обсяг використання об'єкта інтелектуального права ліцензіатом, про одержані у результаті такого використання прибутки, про подальше удосконалення ліцензіатом предмета договору та їх безоплатне використання тощо.

У ЦК України безпосередньо не передбачена можливість укладення субліцензійного договору. У ч. 4 ст. 1108 ЦК України йдеться про можливість видачі субліцензії. Принцип договірної свободи надає сторонам можливість передбачити укладення субліцензійних договорів. Таке право належить ліцензіату лише зі згоди ліцензіара. За відсутності будь-яких спеціальних правил, опираючись на загальні норми договірного права, ураховуючи принцип свободи договору, допускаємо, що умова щодо можливості укладення субліцензійного

договору може бути зафіксована у самому ліцензійному договорі або ж може бути погоджена згодом у разі виникнення такої потреби.

Якщо ж така умова відсутня, а ліцензіат виявляє бажання з будь-яких мотивів укласти субліцензійний договір, то згода ліцензіара має бути надана у письмовій формі. Прямого зазначення у законодавстві про таке немає. Але, оскільки субліцензійний договір є похідним від основного, то основний (ліцензійний договір) укладається у письмовій формі, то й умова про субліцензійний договір теж має мати письмову форму. Зрештою наявність письмової форми спрощує процедуру доказування у разі виникнення спору.

Зміст даного договору має важливе значення для врегулювання відносин між сторонами, забезпечення належного виконання його умов.

При визначенні змісту договору сторони керуються принципом свободи договору. Однак умови ліцензійного договору, які суперечать положенням чинного законодавства України, є нікчемними (ч. 9 ст. 1109 ЦК України).

Законодавством України передбачається можливість затвердження уповноваженими відомствами або творчими спілками типового ліцензійного договору. У цьому випадку, звичайно, сторони також зможуть на свій розсуд включати в ліцензійний договір бажані для них умови, які не передбачені типовим договором. Однак умови ліцензійного договору, укладеного з автором об'єкта права інтелектуальної власності, що погіршують його становище у порівнянні зі становищем, передбаченим законом або типовим договором, є нікчемними та замінюються умовами, встановленими типовим договором або законом (ст. 1111 ЦК України).

З урахуванням природи ліцензійного договору законодавство передбачає, що в ліцензійному договорі визначаються:

- вид ліцензії;
- сфера використання об'єкта права інтелектуальної власності (конкретні права, що надаються

за договором, способи використання зазначеного об'єкта, територія та строк, на які надаються права тощо);

- розмір, порядок і строки виплати винагороди за використання об'єкта права інтелектуальної власності;
- якщо в ліцензійному договорі про видання або інше відтворення твору винагорода визначається у вигляді фіксованої грошової суми, то в договорі має бути встановлений максимальний тираж твору (ч. 3, 8 ст. 1109 ЦК України).

Однак деякі із вищезазначених умов ліцензійного договору, закріплених у ч. 3 ст. 1109 ЦК України (такі як вид ліцензії, територія та строк), можуть бути відсутніми, оскільки діятиме загальне правило, передбачене ЦК України. Ця обставина перетворює зазначені умови з істотних у звичайні, а тому навіть при відсутності цих умов у договорі договір вважається укладеним.

Зокрема, якщо у договорі не зазначено вид ліцензії, то вважається, що за ліцензійним договором надається *невиключна ліцензія* (ч. 4 ст. 1109 ЦК України). Що стосується сфери використання об'єкта права інтелектуальної власності, то у разі відсутності в договорі умови про територію, на яку поширюються надані права на використання об'єкта права інтелектуальної власності, дія ліцензії поширюється на територію України (ч. 7 ст. 1109 ЦК України).

Ліцензійний договір укладається на строк, встановлений договором, який повинен спливати не пізніше спливу строку чинності виключного майнового права на визначений у договорі об'єкт права інтелектуальної власності. У разі відсутності у договорі умови про строк договору він вважається укладеним на строк, що залишився до спливу строку чинності виключного майнового права на визначений у договорі об'єкт права інтелектуальної власності, але не більше ніж на п'ять років. Якщо за шість місяців до спливу зазначеного п'ятирічного строку жодна зі сторін не повідомить письмово іншу сторону про відмову від договору, договір вважається продовженим на невизначений строк. У цьому випадку кожна зі сторін

може в будь-який час відмовитися від договору, письмово повідомивши про це другу сторону за шість місяців до розірвання договору, якщо більший строк для повідомлення не встановлений за домовленістю сторін (ч. 1, 3 ст. 1110 ЦК України).

Положення ЦК України закріплюють, що ліцензіар може відмовитися від ліцензійного договору у разі порушення ліцензіатом встановленого договором терміну початку використання об'єкта права інтелектуальної власності (ч. 2 ст. 1110 ЦК України).

Умовами ліцензійного договору може бути надано право ліцензіату укладати субліцензійний договір. За цим договором ліцензіат надає іншій особі (субліцензіату) субліцензію на використання об'єкта права інтелектуальної власності. У цьому разі відповідальність перед ліцензіаром за дії субліцензіата несе ліцензіат, якщо інше не встановлено ліцензійним договором (п. 2 ст. 1109 ЦК України). Винагорода за наданий дозвіл може бути встановлена у вигляді фіксованої грошової суми (паушальний платіж) [42], періодичних платежів (роялті) чи їх поєднання (комбінованих платежів).

Слід враховувати, що права на використання об'єкта права інтелектуальної власності та способи його використання, які не визначені у договорі, вважаються такими, що не надані ліцензіату.

Права на використання комп'ютерної програми як об'єкта права інтелектуальної власності можуть передаватися за ліцензією або ліцензійним договором. Ліцензія на використання об'єкта права інтелектуальної власності може бути виключною, одиничною, невиключною, а також іншого виду, що не суперечить закону (п. 3 ст. 1108 ЦК України).

Отже, предметом ліцензійного договору у цифровому середовищі є *ліцензія* (дозвіл на використання об'єкта права інтелектуальної власності), а об'єктом — комп'ютерна програма, база даних тощо.

Стрімкий етап розвитку інформаційних технологій породжує низку проблем щодо ефективного захисту та охорони прав інтелектуальної власності на такі об'єкти, як

програмне забезпечення, комп'ютерні програми та інші об'єкти цифрового середовища.

Програмне забезпечення (software) — сукупність програм системи обробки інформації та програмних документів, необхідних для експлуатації цих програм.

Розрізняють *системне програмне забезпечення* (зокрема, операційна система, транслятори, редактори, графічний інтерфейс користувача) і *прикладне програмне забезпечення*, що використовується для виконання конкретних завдань, наприклад, статистичне програмне забезпечення.

Так, виконання програмного забезпечення комп'ютером полягає у маніпулюванні інформацією та керуванні апаратними компонентами комп'ютера. Наприклад, типовим для персональних комп'ютерів є відтворення інформації на екран та отримання її з клавіатури.

Програмне забезпечення (software) та апаратне забезпечення (hardware) — це два комплементарні компоненти комп'ютера, причому межа між ними нечітка: деякі фрагменти програмного забезпечення на практиці реалізуються суто апаратурою мікросхем комп'ютера, а програмне забезпечення, своєю чергою, здатне виконувати функції електронної апаратури.

На відміну від прикладного програмного забезпечення, системне не розв'язує прикладні задачі, а лише забезпечує роботу інших програм, управляє апаратними ресурсами обчислювальної системи й т. д.

Системне програмне забезпечення призначене для: створення операційного середовища функціонування інших програм (інакше кажучи, для організації виконання програм); автоматизації розробки (створення) нових програм; забезпечення надійної та ефективної роботи самого комп'ютера й обчислювальної мережі; проведення діагностики та профілактики апаратури комп'ютера та обчислювальних мереж; виконання допоміжних технологічних процесів (копіювання, архівування, відновлення файлів програм і баз даних і т. д.) [43].

Згідно з типовим положенням з охорони програмного забезпечення (ПЗ), розробленим Всесвітньої організації інтелектуальної власності (ВОІВ) ще у 1977 р., програмне забезпечення містить кілька компонентів: програма для ЕОМ – сукупність команд, які, якщо їх записати на машинозчитуваному носієві, можуть забезпечувати виконання машиною, що здатна оброблювати інформацію, певних функцій; опис програми – повне викладення алгоритму у словесній, схемній або іншій формі, настільки детально, що дозволяє з'ясувати команди, які створюють зміст програми; допоміжний матеріал – будь-який матеріал, створений із метою полегшення розуміння чи застосування програмного забезпечення (наприклад, інструкція для користування).

Будь-який із цих компонентів можна позначити як «програмне забезпечення», але жоден із них не має статусу самостійного об'єкта правового регулювання. Таким об'єктом є лише програмний засіб – тобто матеріальний об'єкт у вигляді машинозчитуваного носія інформації із записаною у нього програмою.

Сам об'єкт охорони має подвійну природу: матеріальний об'єкт (диски, магнітна стрічка тощо) та нематеріальний комплекс операцій, що втілені в алгоритмі та програмі і являють собою результат творчої діяльності, тобто об'єкт інтелектуальної власності [44]. Комп'ютерні програми є об'єктом інтелектуальної власності (ч. 1 ст. 420 ЦК України) та об'єктом авторського права (п. 2 ч. 1 ст. 433 ЦК України, п. 3 ч. 1 ст. 8 Закону України «Про авторське право і суміжні права») [36].

Комп'ютерні програми, безумовно, є об'єктом права інтелектуальної власності – як результат творчої діяльності, але мають низку специфічних відмінностей від об'єктів авторського права: вони призначені для управління роботою технічного пристрою – комп'ютера, але при цьому є рішенням не технічного завдання, а логіко-математичного. Об'єктивна форма вираження комп'ютерної програми дозволяє швидко і дешево виготовляти якісні копії, тому в охороні комп'ютерних програм принципове значення має захист від копіювання [44].

Авторське право поширюється тільки на *форму вираження комп'ютерної програми як твору*. Відповідно, автору твору належать особисті немайнові права та майнові права інтелектуальної власності.

У статті 1107 ЦК України зазначені види договорів щодо розпорядження майновими правами інтелектуальної власності, які передбачають використання об'єкта права інтелектуальної власності, до яких належать у тому числі *ліцензія* або *ліцензійний договір*.

Враховуючи особливості програмного забезпечення пропонується виокремити *чотири групи цивільно-правових договорів* (*ліцензійних договорів*): спрямовані на *створення програми або про механічне відтворення* (виникнення прав); спрямовані на *розпорядження майновими правами виробників програмного забезпечення*; ті, які *регулюють розповсюдження комп'ютерних програм*; ті, які *регулюють ліцензування програмного забезпечення*.

На сучасному етапі розвитку цифрового середовища є декілька форм *ліцензування програмного забезпечення та розподілу програм*.

Головними критеріями поділу ліцензійних договорів є: доступність вихідного коду програми й ціна програмного забезпечення.

Відповідно до критеріїв поділу розрізняють: *пропрієтарне програмне забезпечення* (від англ. *proprietary software*. Це програмне забезпечення, на яке зберігаються як немайнові, так і майнові авторські права. Отримавши або придбавши таке програмне забезпечення, користувач отримує обмежені права користування ним: може бути заборонено або закрито доступ до коду (вивчення), внесення змін, тиражування, розповсюдження та перепродаж), *програмне забезпечення загального використання*, *програмне забезпечення, яке вільно розповсюджується*, і *програмне забезпечення з відкритим вихідним кодом*, яке розповсюджується на умовах ліцензування, що не обмежує право використання такого програмного забезпечення, зокрема його копіювання та модифікацію.

Специфіка здійснення права на відтворення пропрієтарного комп'ютерного програмного забезпечення надає можливість власникові ліцензійного примірника комп'ютерної програми копіювати один примірник безпосередньо на комп'ютер – для надання комп'ютеру працездатності та один примірник – для архівних цілей. Таким чином, одночасно у нього може бути два примірники однієї комп'ютерної програми. У випадках втрати, пошкодження чи непридатності придбаного примірника власник має право замінити його архівним примірником.

Ні у ЦК України, ні у спеціальних нормативних актах не встановлені особливі правила щодо правових підстав та наслідків зміни та припинення ліцензійного договору. Тому такі питання, як і питання відповідальності у разі невиконання чи неналежного виконання ліцензійного договору, слід вирішувати, виходячи із загальних положень договірного права.

5.3. Договір на розробку програмного забезпечення

Зазвичай з договору на розробку програмного забезпечення (надалі – ПЗ) розпочинається співпраця розробника та власника, і саме цей перший договір в історії окремого програмного продукту підтвердить його подальшу життєздатність на ринку.

Відповідно до українського законодавства програмне забезпечення є твором. Зокрема, положення ЦК України і Закону України «Про авторське право та суміжні права» містять визначення *«комп'ютерні програми»* як об'єкта авторського права. Це є початком, з якого мають виходити сторони, укладаючи договір на розробку програмного забезпечення.

Договір на розробку не може бути універсальним. Його модель залежить від того, яку модель розробки ПЗ договір повинен показувати.

Договір **Time & Materials (оплата за фактом).** Зазвичай такі договори використовують у разі, коли обсяг виконаних робіт важко спрогнозувати, а тому розробник отримує оплату за роботи, які він фактично виконав.

Такий вид договору є доволі гнучким, оскільки розробники виконують роботи з урахуванням короткострокових завдань замовника, а тому вимоги до кінцевого продукту можуть змінюватися у процесі. Проте, укладаючи такий договір, замовнику варто пам'ятати, що вартість робіт може бути вищою за очікувану. Також, оскільки такий вид договору передбачає виконання короткострокових завдань, вони не завжди можуть бути прописані в технічному завданні.

Договір **Fixed Price (фіксована ціна).** Укладаючи такий договір, сторони визначають усі вимоги до ПЗ в технічному завданні та прописують строк виконання робіт і їхню вартість. Проте за таким договором важко вносити зміни до вимог кінцевого продукту, а тому його краще не використовувати для розроблення «складного» ПЗ (ризик для замовника). Виконавець також ризикує не отримати відшкодування фактичних затрат, якщо вони перевищили зафіксовану ціну.

Договір **Fixed Budget.** У разі укладання цього типу договору замовник установлює фіксований бюджет, на підставі якого формують технічні завдання до ПЗ та строк виконання робіт. Такий договір найкраще підходить у випадках, коли витрати на розробку програмного забезпечення обмежені.

Договір **Out Staff**. За таким договором замовник отримує в розпорядження на певний час фахівців із конкретно визначеними навичками, повністю регулюючи процес виконання завдань розробниками. Такий варіант договору більше сприятливий для замовників із досвідом у розробленні програмного забезпечення.

Waterfall договір (з англ. Waterfall іноді перекладають як модель «Водоспад» або «Каскадна модель») — договір на розробку програмного забезпечення, в якому істотні умови послідовно врегульовують проходження фази аналізу вимог, проєктування, реалізації, тестування, передання замовнику, інтеграції та підтримки. Як джерело, часто вказують статтю, опубліковану У. У. Ройсом у 1970 році; при тому, що сам автор використовував договір ітеративної моделі розробки [45].

Дотримуючись каскадної моделі, розробник за waterfall-договором переходить від однієї стадії до іншої строго послідовно. Спочатку повністю завершується етап «визначення вимог», у результаті чого виходить список вимог до програмного забезпечення. Після того як вимоги повністю визначені, відбувається перехід до проєктування, у ході якого створюються документи, що детально описують для програмістів спосіб і план реалізації зазначених вимог. Після того, як проєктування повністю виконане, програмістами за договором виконується реалізація отриманого проєкт. На наступній стадії процесу відбувається інтеграція окремих компонентів, що розробляються різними командами програмістів. Після того, як реалізація та інтеграція завершені, проводиться тестування і налагодження продукту; на цій стадії усуваються всі недоліки, що з'явилися на попередніх стадіях розробки. Після цього програмний продукт передається замовнику, впроваджується і забезпечується його підтримка — внесення нової функціональності та усунення помилок.

Перехід від однієї фази до іншої відбувається тільки після повного та успішного завершення попередньої. Таким чином, каскадна модель має на увазі, що перехід від однієї фази розробки до іншої відбувається тільки після повного та успішного завершення попередньої фази, і що переходів назад, вперед або перекриття фаз — не відбувається. У таких waterfall-договорах чітко вказується технічне завдання, яке, зазвичай, узгоджується сторонами у додатках та відразу підписується. Бувають кейси, коли замовник підписує таке технічне завдання, при цьому не читаючи його, а потім, коли результат не відповідає очікуванням, виявляється, що в самому технічному завданні також вказано зовсім не те, що хотів би бачити замовник. У таких випадках замовнику, який не розуміється у технічних нюансах і для якого технічне завдання виглядає наче ієрогліфи, перед укладенням договору, краще проконсультуватись з іншим незалежним розробником перш ніж затверджувати технічне завдання на предмет того, чи відповідає воно його очікуванням.

Якраз відповідність технічному завданню в судовій практиці часто стає предметом експертизи й вирішальних спорах про неякісне надання послуг стосовно розробки програмного забезпечення [46].

Наступним договором на розробку програмного забезпечення є ***agile-договір.*** В agile-договорі закріплюються основні лейтмотиви, ідеї та концепції гнучкої розробки — а саме, постійна співпраця між замовником та підрядником (розробником).

Сторони agile-договору скоріше добрі партнери, ніж замовник та підрядник (розробник). В agile-договорі у будь-якому випадку мають бути істотні умови, характерні для договорів розробки софту і т.п.

Всі детальні умови комунікації між сторонами можна розмістити у відповідному розділі — «Взаємодія Сторін». Калькуляцію вартості конкретних User Story можна також виокремити, так само як і спринти — етапи в рамках загального строку надання послуг. Такі види договорів набирають все більшої популярності серед підрядників (розробників) та замовників, оскільки досить часто процес розробки є довготривалим і умови ринку, під який створюється продукт змінюються. Саме адаптивність до можливих змін, постійна співпраця і націленість обох сторін на успішний реліз продукту є основною перевагою agile-договорів.

Ще одним варіантом урегулювання ІТ-відносин може бути **out staff-договір.** У цьому випадку замовник отримує у своє розпорядження певні години конкретних спеціалістів з професійними навичками, які описані в договорі. Такі спеціалісти надають послуги в межах заявлених навичок. При цьому, роботу таких спеціалістів може координувати менеджер, години якого також продаються в рамках out staff-договору. Такий варіант підходить для досвідчених замовників, або тих, хто має розуміння у сфері розробки софту, і відповідно, зможе отримати користь саме від такого алгоритму роботи.

У таких ІТ-договорах фіксуються кількість годин конкретних спеціалістів, вартість таких годин, у залежності від спеціалізації та навичок осіб, що залучені.

Пояснюючи складне простими словами, можна сказати, що це один з численних видів управління персоналом. Суть out staff в тому, що спеціалісти виводяться за штат компанії або організації, офіційно числяться в іншій юридичній особі або в стартапі, але продовжують працювати на колишньому робочому місці. Фактично ці співробітники беруться в оренду на термін, визначений у договорі. Інколи це кілька місяців, а іноді кілька років — все залежить від компанії-наймача.

Вперше подібна практика була застосована ще в Сполучених Штатах Америки в 70-х роках минулого століття, у період одного з серйозних економічних криз. До України така форма кадрового менеджменту прийшла в 1998 році, коли багато компаній розорювалися, а решта намагалися всіляко мінімізувати штат співробітників. Нині послуги out staff-персоналу надають практично всі великі кадрові агентства, і з кожним роком популярність цієї форми найму тільки зростає.

Дуже часто out staff за співзвучністю плутають з outsourcing, проте це абсолютно різні поняття. Outsourcing являє собою передачу компанією тих чи інших непрофільних для неї функцій стороннім організаціям за договором (наприклад, IT-обслуговування).

Як приклад, наведемо тактику Apple Inc TM, однією з найпопулярніших і найбагатших компаній в світі. Ця компанія — лідер в частині грамотного використання персоналу та передачі функцій стороннім організаціям. Як відомо, Apple не виготовляє телефони та планшети самостійно. Всі компоненти і фінальна збірка виробляються в Китаї та Південній Кореї, що становить собою типовий outsourcing. Для розробки передових моделей або нових пристроїв беруться в найм дизайнери й вузькі фахівці в тій чи іншій області. Зокрема, до роботи над iWatch (годинник від «яблучної» компанії) було залучено близько сотні тимчасових фахівців з провідних годинникових фірм Швейцарії [47].

Наведений поділ доволі умовний, а тому в кожному індивідуальному випадку сторонам слід поєднувати потрібні для них аспекти та компоненти.

Предметом договору на розробку програмного забезпечення є комплекс послуг, який за договором виконавець надаватиме замовнику.

Деталізацію послуг можливо конкретизувати у специфікації ПЗ в тексті самого договору, або в додатку до нього. У специфікації визначаємо всі вимоги й технічні характеристики до програмного забезпечення. У процесі розроблення програмного забезпечення замовник може забажати внести зміни до його специфікації, що своєю чергою може позначитися на строках та оплаті (зміни можуть потребувати додаткових витрат на реалізацію, а також розробник може не вкластися у визначений договором строк). Тому для уникнення неприємних ситуацій у майбутньому краще передбачити можливість вносити зміни за угодою сторін до попередньо оговореної специфікації.

Окрему у вагу необхідно приділити питанню оплати послуг та передання прав інтелектуальної власності за даним договором.

Відповідно до ст. 8 Закону України «Про авторське право та суміжні права» об'єктами авторського права є твори в галузі науки, літератури та мистецтва (зокрема, комп'ютерні програми та бази даних). Схожі за змістом положення містяться в ЦК щодо об'єктів права інтелектуальної власності (ст. 420 ЦК України).

Стаття 11 Закону передбачає виникнення авторського права на твір внаслідок факту його створення. У даному конкретному випадку автором є розробник, у якого виникає авторське право на відповідне програмне забезпечення з моменту його створення.

Українським законодавством передбачено **наявність у автора особистих немайнових і майнових прав** (статті 14 та 15 Закону), які дають йому можливість:

- вимагати визнання свого авторства через зазначення належним чином імені автора на творі та його примірниках і за будь-якого публічного використання твору, якщо це практично можливо;

- забороняти під час публічного використання твору згадувати його ім'я, якщо він як автор твору бажає залишитись анонімом;

- обирати псевдонім, зазначати й вимагати зазначення псевдоніма замість справжнього імені автора на творі та його примірниках і під час будь-якого його публічного використання;

- вимагати збереження цілісності твору та протидіяти будь-якому перекрученню, спотворенню чи іншій зміні твору або будь-якому іншому посяганню на твір, що може зашкодити честі й репутації автора.

Під майновими правами автора потрібно розуміти **виключне право на використання твору** (дозволяє автору використовувати твір у будь-якій формі і будь-яким способом) та **виключне право на дозвіл або заборону використання твору іншими особами.**

На відміну від особистих немайнових прав, майнові права автора можна передавати (відчужувати) іншій особі, після чого ця особа стає суб'єктом авторського права.

У контексті договору на розробку ПЗ нас цікавить саме передання майнових прав на об'єкт авторського права, а тому в договорі обов'язково має бути прописано момент, спосіб та умови їх передання від розробника замовнику (наприклад, через акт прийому-передавання). На вибір сторін, права на розроблене ПЗ може бути передано або з моменту оплати замовником послуг розробника, або з моменту створення розробником відповідного ПЗ.

На жаль, інколи розроблене програмне забезпечення може мати дефекти чи будь-яким іншим чином суперечити специфікації, а тому варто внести до договору право замовника вимагати від розробника привести ПЗ у відповідність до специфікації (наприклад, прописати положення в договорі, згідно з яким замовник повідомляє розробника про дефекти або/та будь-які невідповідності вимогам договору впродовж певного часового проміжку з моменту отримання акту прийому-передавання).

5.4. Договір про нерозголошення

Оскільки комерційна таємниця може містити технічну, організаційну та іншу схожу інформацію, яка використовується в діяльності господарюючого суб'єкта і володіє перерахованими характеристиками, вона стає одним зі способів отримання прибутку. Зважаючи на це IT-сфера зацікавлена зберегти її в секреті: IT-продукти часто схожі між собою або ж є прямими конкурентами. І тільки комерційна таємниця, бренд і реєстрація прав інтелектуальної власності утримує такі продуктові компанії на ринку.

Національне законодавство виокремлює характеристики, якими повинна володіти інформація, щоб підлягати захисту як комерційна таємниця:

- вона є секретною (в цілому, частково або в сукупності її складових залишається невідома)
- не є легкодоступною для осіб, які працюють зі схожою інформацією;
- володіє комерційною цінністю з огляду на її важкодоступність;
- особа, яка контролює доступ до цієї інформації й розпоряджається нею, прийняло запобіжні заходи для збереження її секретності.

Разом з тим, деяка інформація не може бути віднесена за грифом «Комерційна таємниця», оскільки її розкриття є обов'язковим згідно із законодавством. Наприклад, державні органи будуть вимагати розкриття інформації стосовно охорони праці, травматизму працівників і частоти професійних захворювань, кінцевих бенефіціарів або розподілу статутного капіталу тощо.

Відомо, що серед компаній в IT-сфері існує досить велика конкуренція. Це пов'язано з тим, що деякі з них можуть розробляти суміжні або навіть аналогічні продукти. Кожна компанія прагне бути першою, продати свій продукт якнайкраще та зайняти передові позиції на ринку. Кожен власник IT-компанії в таких умовах має розуміти, що інформаційна безпека виходить на перше місце. З метою захисту своїх ідей та програмних продуктів,

задля убезпечення їх від крадіжок конкурентів виникає необхідність у створенні та застосуванні всіх можливих засобів та методів, серед яких укладення ***договору про конфіденційність (NDA)*** та договору про неконкуренцію – ***заборону конкурувати (NCA)*** [48].

Договір NDA в IT-бізнесі. Угода про нерозголошення інформації – це гарантія для бізнесу від недобросовісної поведінки співробітника, підрядника та клієнта.

У процесі співпраці часом виникають конфлікти. Що заважає співробітникові піти до конкурента, забравши результати своєї роботи? Щоб уникнути конфліктів, а також заздалегідь встановити відповідальність за недобросовісні дії співробітників, підрядників і клієнтів підписується договір про нерозголошення інформації. Він може бути частиною контракту на розробку програмного забезпечення, а може виступати окремою угодою. Є можливість передбачити в основному договорі окремий пункт, а докладні аспекти викласти в окремій угоді, яка буде присвячена питанням роботи з конфіденційною інформацією.

Договір NDA має передбачати наступні пункти: поняття конфіденційної інформації, яка інформація не вважається конфіденційною, правомірне розголошення конфіденційної інформації, способи передачі інформації, штраф за порушення договору та обов'язок відшкодувати шкоду, місце розгляду спору.

Договір про нерозголошення інформації має бути викладений у такій формі, щоб у разі його порушення співробітником, клієнтом чи розробником цей факт можна було довести у суді. Для того, щоб довести, що розголошена інформація дійсно була конфіденційною, в угоді має бути визначено, яка саме інформація є конфіденційною. Аналізуючи судову практику в Україні, можна помітити, що є дуже багато відмов з боку суду з посиланням на те, що у документах не було чітко зазначено, яка саме інформація є конфіденційною. Були відсутні будь-які внутрішні документи, які визначали б, яка інформація є конфіденційною, а також режим поводження з конфіденційною інформацією.

Як приклад, можна навести Постанову Верховного Суду від 28.02.2019 р. у справі №752/5775/16-ц [49], в якій, відмовляючи в задоволенні позову, суд посилався на наступні обставини: «Факт розголошення конфіденційної інформації та комерційної таємниці було визнано недоведеним у зв'язку з відсутністю його документального підтвердження, а також вказівки на конкретну інформацію, яка була розголошена. За матеріалами справи працівниця під час перебування у відпустці по догляду за дитиною здійснила доступ до корпоративної системи Redmine, що містить комерційну таємницю».

Отже, необхідно не тільки підписувати договір про нерозголошення конфіденційної інформації, а й мати затверджену повноцінну внутрішню політику, де визначено, що таке конфіденційна інформація та як з нею поводитися.

Договір NCA в IT-бізнесі. Договір про уникнення конкуренції укладається між роботодавцем і працівником, та обмежує останнього у праві роботи в будь-якому подібному бізнесі на певний проміжок часу після припинення трудових відносин. Зазвичай NCA підписують разом з NDA.

Договір про неконкуренцію виконує наступні функції: захищає замовника або роботодавця від можливої конкуренції з боку підрядника або працівника, який після закінчення співпраці вирішить створити бізнес у тій самій сфері або на тій самій території чи працювати на прямого конкурента; запобігає витоку унікальних знань, навичок, ідей, технологій замовника або роботодавця, контактів клієнтів, бізнес-практики; допомагає замовнику або роботодавцю утримати кваліфікованих спеціалістів; здійснює психологічний вплив на працівника/підрядника.

В Україні застосування договорів NCA не має достатнього правового регулювання, тому, на відміну від європейських країн, не знайшло широкого застосування. Багато питань виникає у разі укладення договору про неконкуренцію між працівником та роботодавцем. Суди у разі виникнення спорів, як правило, визнають такі договори недійсними, розглядаючи їх як обмеження права

на вільний вибір праці, гарантованого статтею 43 Конституції України. Те ж стосується і врегулювання відносин між замовником та виконавцем.

Укладення договору про неконкуренцію є однією з обов'язкових умов співпраці замовників-нерезидентів з українськими ІТ-компаніями чи окремими розробниками та є нормальною практикою для багатьох країн Європи і США (в деяких штатах). У такому разі вирішення спорів про неконкуренцію підпорядковується праву іноземної держави та захищає, в першу чергу, інтереси замовника.

Підсумовуючи, можемо з повною впевненістю рекомендувати ІТ-бізнесу не нехтувати укладенням договорів NDA та NCA, адже такі договори спрямовані на збереження інформації, ідей, продуктів, створених розробником, клієнтської бази компанії, що, безумовно, є одними з основних найбільш цінних активів будь-якої ІТ-компанії.

Запитання для самоконтролю і самостійного опрацювання

1. Назвіть поняття, ознаки та характеристика вільних публічних ліцензій.
2. Схарактеризуйте Ліцензійний договір як договір щодо передання прав інтелектуальної власності у цифровому середовищі.
3. Сторонами якого договору завжди виступають суб'єкти підприємницької діяльності?
4. Які договори у сфері інтелектуальної власності підлягають державній реєстрації?
5. Чи можуть договори щодо розпоряджання майновими правами інтелектуальної власності укладатись в усній формі?
6. Які договори, на Вашу думку, можна віднести до згаданих у ст. 1107 Цивільного кодексу України інших договорів щодо розпоряджання майновими правами інтелектуальної власності?

Рекомендована література:

1. Рзаєв Д. О., Шарапов О. Д., Ігнатенко В. М., Дибкова Л. М. Інформатика та комп'ютерна техніка : навч.-метод. посібник для самост. вивч. дисц. — Київ : КНЕУ, 2002. — 486 с. URL: https://nmetau.edu.ua/file/130.pdf

2. Верба І. І. Основи інтелектуальної власності : навч. посіб. / За ред. С. В. Чікін. 2-ге вид., перероб. і доп. — Київ : НТУУ «КПІ», 2013.

3. Фасій Б. В. Agile waterfall та out staff-договір або договори на розробку програмного забезпечення. *Часопис цивілістики*. 26 (2017) . — С. 98-102.

4. Ткачук А. Договори NDA та NCA в IT-бізнесі. URL:https://yur-gazeta.com/dumka-eksperta/navishcho-potribno-ukladati-dogovori-nda-ta-nca-v-itbiznesi.html

5. Коросташова І. М. Щодо розпорядження майновими правами інтелектуальної власності: питання класифікації. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. Збірник наукових праць. — Дніпропетровськ. Вип. №4 (40). 2008. — С.70-79.

6. Жилінкова О. В. Договірне регулювання відносин щодо інтелектуальної власності в Україні та закордоном : монографія. — Київ : Юрінком Інтер, 2015. — 280 с.

РОЗДІЛ 6.

ГОСПОДАРСЬКА ДІЯЛЬНІСТЬ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

6.1. Електронна комерція

Комунікації та обмін інформацією у XXI столітті стають дуже важливими елементами як особистого, так і професійного життя. На даному етапі розвитку українського суспільства відбуваються кардинальні зміни підходів як до життя нації у цілому, так і до окремих сфер. Зокрема, сьогодні серйозний вплив здійснюється на провадження господарської діяльності за допомогою застосування інформаційних технологій.

Одним з найважливіших елементів сучасних інноваційних перетворень є інформаційні системи та технології, здатні виробляти великі обсяги інформації та знань, передавати їх на значні відстані, накопичувати, зберігати та формувати нові інтелектуальні продукти як у національних, так і в міжнародних економічних системах [50]. Динамічний розвиток світового ринку інформаційних технологій здійснює значний вплив на розвиток світового господарства, розробка та втілення нових інформаційних технологій оптимізує процеси виробництва, дозволяє більш ефективно використовувати ресурси, сприяє прискоренню обміну інформацією.

Сучасні інтеграційні процеси бізнесових структур у світовий інформаційний простір виступають одним із пріоритетних чинників їх ефективної діяльності у майбутньому та підтримання конкурентоспроможності в ринкових умовах. Бурхливий розвиток інформаційних комп'ютерних технологій, вдосконалення технічної платформи і поява принципово нових класів програмних

продуктів привів у наші дні до зміни підходів до автоматизації управління виробництвом [51].

Сучасні компанії та установи використовують інформацію та комунікаційні технології для оптимізації ефективності своєї діяльності та збільшення власного прибутку. Завдяки мережі Інтернет, будь-яке підприємство здатне охопити клієнтів з усієї країни і навіть знайти нових замовників з-за кордону.

Для кожного виду бізнесу сьогодні найважливішими завданнями є своєчасне інформування цільової аудиторії та можливість максимально швидко реалізувати продукт (товар чи послугу), саме тому такого поширення набула система електронної комерції (e-commerce), адже такий підхід дозволяє одночасно виконувати ці та інші завдання, здійснювати контроль за реалізацією маркетингових завдань і зробити купівлю-продаж максимально ефективною. Засобом реалізації та втілення засад електронної торгівлі є всесвітня мережа Інтернет, котра дає можливість заощадити велику кількість часу і коштів на проведенні взаєморозрахунків.

Зручною є система e-commerce і під час корпоративних закупівель, адже жодна інша модель бізнесу так не наголошує на необхідності тісної інтеграції між виробниками, постачальниками та дистриб'юторами, в процесі якої встановлюється ринкова ціна. Збільшення швидкості проходження цього ланцюжка за допомогою можливостей, які відкриває Інтернет, значно підвищує ефективність.

Отож, зручність використання системи електронної комерції зумовлює її беззаперечну актуальність та популярність, а, отже, і значний науковий інтерес до неї.

У відносно великих обсягах українські споживачі придбавають через Інтернет одяг, косметику та парфумерію, подарункову продукцію, книжки, товари для дітей, приладдя для спорту й відпочинку. «Ринок Інтернет-торгівлі зростає настільки швидко, що у деяких сегментах роздрібної мережі частка такої торгівлі є набагато вищою за середню та істотно збільшиться упродовж кількох наступних років, — стверджує економіст Міжнародного

центру перспективних досліджень Ганна Чередниченко. – Приміром, за даними тогорічних досліджень, у продажах техніки вона сягнула 17%. До речі, саме на цьому ринку Інтернет-магазини істотно впливають на ціни, змущуючи традиційні торговельні точки стримувати їхнє зростання» [52].

У цілому перспективи ринку е-комерції, переважну частину якого займають туристична галузь, онлайн-продаж квитків, купівля одягу та побутової техніки в Інтернеті, очевидні. Вітчизняні споживачі оцінили також зручність поповнення рахунку мобільного телефону або оплати послуг Інтернет-провайдера через Інтернет.

А от електронним платежам (зокрема, за комунальні послуги), як свідчать соціологічні опитування, почали довіряти порівняно недавно. За даними експертів ринку, за рік онлайн-платежі збільшилися майже втричі. Справжній бум відбувся щодо такого сервісу, як переказ коштів з картки на картку. На думку експертів, це пов'язано передусім з військовими діями в Україні, коли на окупованих територіях припинили діяльність чимало банківських установ, обмеживши платоспроможність громадян. Цей напрям, за спостереженнями фахівців, продемонстрував зростання понад 5000% за рік. І це не межа, переконують експерти.

Концепція е-бізнесу виникла у США у 80-х роках XX ст. і стала результатом розвитку ідеї глобальної інформаційної економіки, яка була теоретичною основою створення локальних і корпоративних інформаційних мереж з поєднанням застосування інформаційних технологій в компаніях.

Зараз бізнес стає електронним, тобто комерційні дії між партнерами (покупка/продаж товарів або послуг, операції на фондовому ринку з цінними паперами, укладання і виконання договорів і тому подібне) відбуваються за допомогою обміну електронними документами в інформаційному просторі – тій частині реальності, яка викликає у людини спеціальний інтерес і виділяється із загальної картини навколишньої об'єктивної дійсності. У ролі ПО можуть виступати компанія, корпорація, держава і тому подібне. Інформаційний сектор

економіки є основою для зазначеної трансформації традиційних форм господарювання в економічну систему постіндустріального типу.

Серед ***характерних особливостей інформаційного суспільства виділяють***:

- пріоритет інформаційних ресурсів у порівнянні з іншими ресурсами;

- автоматизовану генерацію, збереження, оброблення і використання знань та інформації на основі інформаційних комунікаційних технологій і технологій е-бізнесу;

- глобальний характер застосування мережних технологій;

- вільний доступ кожної людини до інформаційних ресурсів.

Електронний бізнес — це вид економічної діяльності компаній через комп'ютерні мережі, зокрема, Internet, з метою отримання прибутку. Електронна комерція є такою, що становить е-бізнес, це один зі способів його здійснення.

Електронна комерція (e-commerce) — вид електронної комерційної діяльності з використанням інформаційних комунікаційних технологій. Поняття «електронна комерція» ширша, ніж Інтернет-комерція, оскільки до нього входять усі види комерційної діяльності, здійснюваної електронним шляхом.

Інтернет-комерція — електронна комерція, обмежена використанням тільки комп'ютерної мережі Інтернет. До Інтернет-комерції не входять: здійснення банківського обслуговування через системи «Клієнт-Банк», комерційна діяльність з використанням мереж VAN, мобільна комерція, системи управління ресурсами підприємства (MPR, ERP, CSRP).

Електронний бізнес — це більш ніж проста електронна покупка або продаж товарів, він потребує використання мережних комунікаційних технологій для проведення дій з метою отримання прибутків усередині й поза підприємством. Розвиток електронного бізнесу означає перехід до інформаційного простору основних бізнес-процесів і каналів зв’язку, а це рано чи пізно

відіб'ється на діяльності всіх підприємств. Електронний бізнес складається з чотирьох стадій: маркетингу, виробництва, продажу і платежів. Якщо дві або більше стадій бізнесу здійснюються із застосуванням електронних систем, тоді бізнес вважається електронним.

У вужчому розумінні е-бізнес – перетворення бізнес-процесів із застосуванням Інтернет-технологій, що дозволяє досягти вищої продуктивності.

Бізнес-процес – це сукупність операцій, що взаємопов'язуються між собою, процедур, за допомогою яких реалізується конкретна комерційна (підприємницька) мета діяльності компанії в рамках організаційної структури, при цьому функції структурних підрозділів та їх відношення між собою заздалегідь чітко визначені і зафіксовані.

Електронний бізнес – дуже динамічна галузь. Зараз технології е-бізнесу – один із важливих інструментів сучасної конкурентної боротьби. Вплив електронного бізнесу змінює всі форми діяльності великих і малих підприємств – від розробки продуктів до продажу товарів на ринку. Головним джерелом ринкової сили стає інтелект, втілений в організаційні структури дослідницьких і ринкових корпорацій, які створюють нові ІТ й утримують контроль над ними.

У цілому електронне ведення бізнесу охоплює три складові:

1. Електронний документообіг;
2. Електронну систему платежів;
3. Електронну торгівлю.

Можна розглянути такі основні види електронної економічної діяльності:

- віртуальні компанії;
- електронну гуртову і роздрібну торгівлю, електронний маркетинг, післяпродажну підтримку споживачів, електронні гуртові й роздрібні фінансові послуги, зокрема кредитування і страхування;
- комерційні дослідження маркетингового типу;
- електронна реклама;

- комерційні операції (інтерактивне електронне замовлення, доставляння, оплата);
- загальне розроблення продукту (товарів, послуг);
- розподілене спільне виробництво електронних товарів;
- електронне адміністрування бізнесу зокрема сферу податкового адміністрування);
- електронну торгівлю товарами/послугами;
- електронний бухгалтерський облік;
- укладення угод в електронній формі;
- електронне арбітражне адміністрування (тобто розв'язання суперечок) і тому подібне.

Глобалізація ринків, виникнення регіональних економічних з'єднань (великі електронні торгові мережі), інтеграційні процеси відкривають нові можливості для підприємств. Сьогодні відсутність певної діяльності підприємства у всесвітній мережі Інтернет розцінюють як недолік. Брак часу змушує споживачів все частіше купувати товари та послуг через Інтернет, а це, своєю чергою, зумовлює ще більший розвиток електронної торгівлі та появу нових її різновидів.

У переважній більшості закордонні автори, пояснюючи поняття електронної комерції, узагальнюють її — як таку діяльність, що охоплює всі типи електронних транзакцій між організаціями та зацікавленими особами [53]. Американський дослідник В. Звасс дає такі характеристики електронній комерції: обмін бізнес-інформацією, налагодження бізнес-відносин, здійснення бізнес-транзакцій через телекомунікаційні мережі, а також торгові відносини. Тобто він акцентує саме на бізнесовому аспекті поняття [54]. Такої ж думки дотримуються й А. Саммер та Г. Дункан, які визначають електронну комерцію як будь-яку форму бізнес-процесу, в якому взаємодія між суб'єктами відбувається засобами електронної комунікації [55]. Бізнесовий і торговий аспекти е-комерції описують вчені В. Тріз та Л. Стюарт. На їхню думку, вона включає застосування технологій у фінансовому бізнесі, електронному резервуванні квитків, постачанні, замовленнях, а також використання Інтернету

для покупок і продажів товарів та послуг, зокрема післяпродажні послуги й підтримку [56]. Схоже визначення знаходимо і в працях таких вітчизняних науковців, як В. Л. Плескач та Т. Г. Затонацька [57].

Аналіз вищезазначених визначень дає підстави стверджувати, що існує єдність підходів щодо визначення поняття електронної комерції, трактуванні її призначення та форм реалізації. Проте думки щодо цього виду ділової активності змінюються пропорційно до росту популярності електронної торгівлі, оскільки маємо можливість спостерігати все нові та нові сфери діяльності, у яких застосування електронної комерції є виправданим та ефективним, а, отже, і нові ознаки цього економічного явища, які можуть стати предметом наукового дослідження.

Електронна комерція (e-commerce, Інтернет-торгівля, електронна торгівля) — це широкий набір інтерактивних методів ведення діяльності з надання споживачам товарів та послуг. Також під електронною комерцією розуміють будь-які форми ділових операцій, де сторони взаємодіють через електронні технології, а не в процесі фізичного обміну чи контакту [58].

Ведення бізнесу засобами електронної торгівлі ґрунтується на використанні електронних комунікацій та технологій обробки цифрової інформації для встановлення та зміни відносин із створення вартості між організаціями та організаціями й індивідами. Загалом електронний бізнес об'єднує якісно нові підходи та методи роботи компаній, надаючи у такий спосіб можливість забезпечити конкурентні переваги шляхом зменшення витрат на взаємодію, розширення ринків і сфери діяльності, проникнення на вже наявні ринки та виявлення нових каналів збуту, залучення нових та поліпшення обслуговування старих клієнтів, більшої мобільності та оперативності під час прийняття управлінських рішень.

Щодо певного історичного поступу, електронна комерція поступово пройшла етапи уніфікації та стандартизації різних систем електронного обміну. У 80-х роках XX ст. на базі англійських та американських

стандартів міжнародна організація із стандартизації ISO розробила новий стандарт Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT, ISO 9735).

Одночасно динамічно зростали обсяги електронної торгівлі, а також кількість компаній, які її здійснювали. Так, у 1996 р., коли торгівля за допомогою Інтернету лише формувалася, обсяг EDI-трансакцій становив 300 млрд дол. США, а в 1999 р. – 1,1 трлн дол. США. Галузь електронної комерції й надалі зберігала надзвичайно динамічні темпи розвитку – на початку століття вона подвоюється щорічно, а наприкінці 2003 р. обсяг світової торгівлі через мережу Інтернет досяг майже 1,25 млрд дол. США [59].

Україна також має чималий досвід зі становлення системи електронної комерції. Так, за останні роки ріст українського сегмента Інтернету (UAnet) спостерігається у всіх напрямках. Аудиторія UAnet подвоювалася щорічно за останні три роки, за різними оцінками, становить від 2 до 4 % населення. UAnet містить понад 12 тис. українських сайтів. Очікується щомісячний ріст відвідувачів UAnet на 15 %, 56 % аудиторії UAnet представлена мешканцями України, 19 % – Росії, 12 % – США, 8 % – Західної Європи, 5 % – інші. Регулярна аудиторія користувачів UAnet, що проживають в Україні, – 450 тис., а користувачів Інтернету – від 750 тис. до 2 млн осіб. Швидке збільшення користувачів Інтернет стане рушієм Інтернет-сектора в Україні. Інтернет-економіка нашої країни представлена галузями комп'ютерної техніки і комунікаціями, рекламою і медіаіндустрією, Інтернет-послугами, електронною комерцією [58].

На сьогодні для опису економічних відносин через мережу Інтернет використовується поняття «електронна комерція», яке і є частиною Інтернет економіки. Так, Організація економічного співробітництва та розвитку надає два визначення даного терміну [60]:

1) у вузькому сенсі, електронна комерція – це продаж чи покупка товарів та послуг між бізнесом, домашніми господарствами, фізичними особами, урядами та іншими державними чи приватними організаціями, що

проводяться через мережу Інтернет. Товари та послуги замовляються через Інтернет, але платіж та остаточне доставляння товару або послуги можуть здійснюватися як в онлайн, так і в офлайн режимі.

2) у широкому сенсі, електронна комерція — це будь-яка форма бізнес-відносин, де взаємодія між суб'єктами відбувається шляхом використання Інтернет-технологій.

Зважаючи на те, що електронна комерція на сьогодні стала окремою галуззю економіки, велика увага приділяється і законодавчому врегулюванню даного поняття.

Так, у 1997 році згідно з резолюцією Генеральної Асамблеї ООН було введено в дію Типовий закон «Про електронну торгівлю». Цей законодавчий акт має рекомендаційний характер і, перш за все, повинен бути використаний державами як основа для розробки національного законодавства.

Не виключенням є й Україна. Правове регулювання діяльності в сфері Інтернет економіки започатковано ухваленням Закону України «Про Національну програму інформатизації» у 1998 році [62]. Фінальним етапом законодавчого визначення організаційно-правових засад діяльності у сфері електронної комерції в Україні, на сьогодні, став Закон України «Про електронну комерцію», прийнятий у 2015 році [63]. Даний закон, крім надання тлумачення основних дефініцій, встановлює порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та визначає права і обов'язки учасників відносин у сфері електронної комерції.

Так, згідно з Законом України «Про електронну комерцію», електронна торгівля визначається як частина електронної комерції, а саме — господарська діяльність у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом покупцю шляхом вчинення електронних правочинів із використанням інформаційно-телекомунікаційних систем.

Електронний бізнес має низку переваг:

1. Пропонує глобальний доступ на глобальні ринки (компанія може розширити свою базу клієнтів, а також асортимент товарів).

2. Дозволяє поліпшити бізнес-контакти (продавці товарів промислового призначення можуть налагодити більш тісні зв'язки з покупцями (наприклад, ринки «бізнес-бізнес» – B2B)).

3. Дозволяє покупцям швидко, просто і безплатно отримати зразки товарів (доступність інформації про товари і послуги в Інтернет-магазинах у режимі реального часу).

4. Дозволяє знизити витрати (укладання оборудки електронним шляхом на порядок зменшує витрати на обслуговування операції, а це, і собі, тягне за собою зниження цін для споживачів; відсутність митних податків, пов'язаних з електронним продажем).

5. Дозволяє отримувати високоякісні послуги (електронна комерція дозволяє постачальникам підвищувати конкурентоспроможність, стаючи ближчим до замовника).

6. Зменшує кількість носіїв інформації, які потрібні для збереження даних.

7. Скорочує час виходу товару на ринок і процесу адаптації компанії до змін ринку.

8. Сприяє появі нових бізнес-моделей. Нові бізнес-моделі – віртуальні підприємства, віртуальні агенти, технологи аутсорсингу і телероботи значно підвищують ефективність комерційної діяльності. Окрім перетворення ринку наявних товарів і послуг, електронна комерція відкриває можливість появи абсолютно нових продуктів і послуг. Наприклад: страхові, брокерські послуги служби електронного постачання і підтримки.

10. Підвищує рівень прихильності споживачів до торгової марки (якість обслуговування в Інтернет постійно поліпшується: споживач може отримати нову інформацію про компанію і товари в будь-який зручний для себе час) [64].

Недоліки розвитку електронного бізнесу:

Перш за все, мова йде про особливості самого Інтернету як майданчика для торгівлі: Інтернет може знищити інститут торгових посередників; конкуренція переходить з локального рівня на глобальний; проблеми захисту авторських прав; недостатня правова визначеність

операцій в Інтернеті, наслідків укладених договорів, умови їх чинності тощо. Крім того, для мережі Інтернет не розроблено правову базу, яка б діяла у планетарному масштабі. Визначають такі основні недоліки ведення бізнесу у цифровій сфері:

1. Зниження прихильності споживачів. Оскільки в мережі Інтернет відсутній персональний контакт, рівень прихильності клієнтів не є стабільним.

2. Проблеми ціноутворення. В Інтернеті дуже легко порівнювати ціни, тому вони знижуватимуться, проте зросте роль додаткових послуг.

3. Питання інформаційної безпеки при роботі в Інтернеті.

4. Питання прозорості. Через засоби ідентифікації особи користувача можна здійснювати контроль за людьми, перевіряти їх діяльність (унікальний ідентифікаційний код особи може стати об'єктом загрози для людини).

5. Життєздатність. Багато підприємств не мають упевненості в тому, що їх е-бізнес виявиться життєздатним.

6. Неохопленим залишається деякий сегмент населення, що не має доступу до Інтернету [64].

Щодо перспектив розвитку електронної комерції в Україні, то її стан можна назвати лише початковим, але вона набуває все більшої популярності. На це впливає ціла низка факторів:

1) недостатній рівень розвитку ринкових відносин у більшості секторів економіки, що не стимулює впровадження прогресивних високоефективних інформаційних технологій;

2) відсутність достатнього обсягу вільних фінансових засобів у вітчизняних підприємств та фінансових установ, що не дозволяє інтенсивно розвиватись ринку Інтернет-послуг;

3) низька платіжна спроможність населення, що не сприяє збільшенню користувачів мережі. Для того, щоб щось купувати в Інтернеті, треба мати якісь кошти. З огляду на те, що більш ніж половина українців знаходяться

за межею бідності, важко розраховувати на реально широку аудиторію. Інтернет-технології найбільш ефективні, коли ними користується не менше 5% населення. В Україні, за різними оцінками, можливості глобальної інформаційної мережі Інтернет активно використовують від 1,2 до 2 млн користувачів;

4) недостатній рівень розвитку телекомунікаційної інфраструктури, що не дозволяє надавати споживачеві сучасні види послуг. Доступ до Інтернету в Україні ще досить дорогий;

5) низький рівень використання інформаційних технологій на підприємствах, в організаціях та органах державної влади, що не сприяє усвідомленню місця і ролі мережі Інтернет у сучасній економіці;

6) значна різниця у рівні інформатизації великих міст та регіонів країни, що зменшує потенційну аудиторію користувачів мережі;

7) повна відсутність у нашій країні (і в СНД) надійної системи оперативного доставляння матеріальних цінностей гальмує розвиток нашої онлайнової торгівлі навіть більше, ніж мала кількість користувачів Інтернету;

8) нерозвиненість надійних і легітимних засобів автентифікації, цифрових підписів, сертифікатів і шифрування. Виникають проблеми конфіденційності та цілісності даних, дотримання прав інтелектуальної власності. Стандарти і законодавча база недостатньо розроблені, недостатня нормативно-правова база в питаннях розвитку Інтернет, інформаційних ресурсів та інтелектуальної власності, що не сприяє розвитку ринку Інтернет-послуг;

9) недосконалі механізми оплати. Попри розвинуту культуру використання магнітних карток, їхні власники утримуються від їхнього активного застосування, побоюючись шахрайства;

10) низький рівень безпеки при здійсненні оплати кредитною карткою. Обдурити при проведенні платежу по пластиковій карті через Інтернет легше, ніж при платежі в звичайному магазині. У США близько 1% платежів по пластикових картах виявляються шахрайськими.

Половина цих шахрайських платежів приходиться на Інтернет (при тому, що обсяг платежів через Інтернет складає менш як 10%);

11) за допомогою багатьох кредитних карт можна платити суми не менше якогось певного ліміту, у той час, як чимала частина обороту в інформаційному бізнесі буде забезпечена платежами в «нижньому ціновому діапазоні» (менш як 1 долар);

12) недостатньо широкий спектр товарів і послуг, доступний через мережу. Безумовно, ключовим моментом для залучення споживчих грошей в електронні ринки, як і у звичайному бізнесі, є формування достатнього обсягу пропозиції за привабливими цінами. Фактично ця складова поки тільки починає розвиватися, особливо у сфері продукції щоденного використання;

13) висока вартість володіння електронним магазином. Сьогодні створити повноцінний магазин, прив'язаний до системи обліку реальної фірми, можуть великі компанії, тому що комплекс послуг по його «розгортанню» коливається від 2 до 50 тисяч доларів США;

14) трудомісткість пошуку необхідного товару чи інформації. Обсяг ресурсів мережі Інтернет практично подвоюється щороку, пошукові машини дають багатотисячні відгуки на прості запити, мови запиту ще дуже далекі від природних;

15) менталітет українського народу. 70-літнє загартування радянського (тепер українського) народу виробило звичку добувати необхідні товари з боєм, у чергах, з номерками на руках. Тепер це виражається в іншій формі. Більшість людей перш ніж щось купити — телевізор чи холодильник — самі об'їдуть магазини, помацають, поспілкуються із продавцями й т. ін;

16) довіра до продавця. Покупець має довіряти магазину. Багато хто вже «наївся» пірамідами та іншими видами афер [65, 66].

Крім всього вищезазначеного, окремо хотілося б виділити таку проблему, як повна відсутність державної статистичної інформації, що стосується електронної комерції в Україні. Це значно звужує можливості аналізу

та прогнозування тенденцій розвитку електронної комерції в нашій країні.

Запитання для самоконтролю і самостійного опрацювання:

1. У чому різниця між «електронною комерцією» та «електронним бізнесом»?
2. Назвіть суб'єктів електронної комерції.
3. Назвіть сфери, у яких на сьогодні використовується електронна комерція.
4. На яких рівнях може здійснюватися електронна комерція?
5. Схарактеризуйте сучасний стан ринку електронної комерції у світі та в Україні.
6. Яке правове підґрунтя для здійснення електронної комерції існує в Україні?

Рекомендована література:

1. Asaul A., Voynarenko M., Dzhulii L., Yemchuk L., Skorobohata L. and Mykoliuk O. The Latest Information Systems in the Enterprise Management and Trends in their Development // 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019. — P. 409-412, doi: 10.1109/ACITT.2019.8779874
2. Клепікова О. А. Сучасний стан і місце інформаційних технологій в управлінні підприємством. *Науковий вісник міжнародного гуманітарного університету. Серія: Економіка і менеджмент.* — 2013. № 5. — С. 74-77.
3. Головко І. Електронна комерція: визнання де-юре. URL: http://www.visnuk.com.ua/ua/pubs/id/8946
4. Chaffey D. E-business and E-commerce Management. Strategy, Implementation and Practice. — Prentice Hall, 2009. — 800 p.
5. Zwass V. Electronic Commerce: Structures and Issues. I*nternational Journal of Electronic Commerce*. — V.1, №1, Fall, 1996. — P. 3–23.
6. Саммер А., Дункан Гр. Маркетинг. Пятая волна. E-commerce. — М. : 1999. — 152 с.
7. Treese C. Winfield, Stewart Lawrence C. Designing Systems for Internet Commerce. — AddisonWesley, 1998. — 375 p.
8. Плескач В. Л., Затонацька Т. Г. Електронна комерція : підручник. — Київ : Знання, 2007. — 535 с.

9. Маєвська А. А. Електронна комерція і право : навч.-метод. посібник. — Харків, 2010. — 256 с.

10. Маловичко С. В. Тенденції та перспективи розвитку електронної торгівлі в Україні. *Економіка і регіон.* — 2015. № 4. — С. 67-73.

11. Про електронну комерцію : Закон України. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

12. Тардаскіна Т. М., Стрельчук Є. М., Терешко Ю. В. Електронна комерція : навч. посіб. — Одеса : ОНАЗ ім. О. С. Попова, 2011. — 244 с.

13. Самойленко Л. Переваги застосування електронного бізнесу. *Економіка АПК.* — 2003. № 8. — С. 141–146.

14. Гресь А. М. Удосконалення організації систем доставки товарів у електронній торгівлі в Україні. *Науковий вісник Українського державного лісотехнічного університету*. — 2004. Вип.14.4. — С. 288–294.

РОЗДІЛ 7.

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ. ЦИФРОВИЙ ПІДПИС

Актуальність електронних документів для використання у господарській діяльності, взаємодії з державними органами та суді збільшується щодня. Останній етап відбувся 01.12.2021р. коли Верховна Рада України прийняла Закон «Про особливості надання публічних (електронних публічних) послуг» (про режим paperless), який передбачає відмову від паперового документообігу в Україні. Основна мета paperless – держоргани в Україні не зможуть вимагати паперові документи, довідки та посвідчення, якщо інформація є в державних реєстрах. А прийняті дещо раніше – 2003-го, 2015-го, 2018-го та 2019-го – закони регулюють різні типи відносин у роботі з електронним документообігом. Електронну форму документа передбачають Закони України «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», «Про захист прав споживачів», «Про зовнішньоекономічну діяльність», «Про електронну комерцію», Цивільний кодекс України та інші нормативно-правові акти.

Так, Закон України «Про електронні документи та електронний документообіг» регламентує легальні визначення понять і встановлює правовий статус електронного документа та його копії. Відповідно до ст. 5 зазначеного Закону **Електронний документ** – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму [67]. Візуальною формою подання електронного документа є відображення даних, які він

містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною. *Прикладом візуальної форми є pdf-формат документа згідно з Переліком форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання, затвердженого наказом Мін'юсту від 11.11.2014 р. № 1886/5.*

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги». У разі надсилання електронного документа кількох адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу. Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії (ст. 7 Закону України «Про електронні документи та електронний документообіг»).

Електронний цифровий підпис (ЕЦП) – вид підпису, що надає можливість здійснювати підпис документів в електронній формі. Фактично це електронний файл з набором зашифрованих даних для ідентифікації підписанта.

Закон України «Про електронні довірчі послуги» [68] визначає електронний підпис як електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис : Закон України «Про електронні документи та електронний документообіг», визначає правову природу електронного документа та закріплює, що юридична сила електронного документа не може бути заперечена

виключно через те, що він має електронну форму. Верховний Суд України у постанові по справі № 922/788/19 від 28.12.2019 р. остаточно визначився: *без електронного підпису електронний документ не вважається створеним, а, отже не може розглядатися судом як доказ.* Скриншоти, роздруківки з електронної пошти без електронного підпису не вважатимуться доказами здійснення господарських операцій.

Дуже часто разом з електронним підписом на документі ставиться «позначка часу». **Електронна позначка часу** – електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу;

Електронний цифровий підпис отримується в акредитованих центрах сертифікації ключів (АЦСК), перелік яких можна знайти на сайті Міністерства цифрової трансформації України. Підписання документів ЕЦП є найнадійнішим способом ідентифікації підписувача та фіксації волевиявлення. Окрім підписання документів ЕЦП, на практиці можуть використовувати скановані документи зі зразками підписів та печаток; простий текстовий підпис в електронному листі; погодження з договором (офертою) може відбуватися шляхом проставлення відповідного «прапорця», «галочки» на веб-сайті. Таким чином існують різні рівні захисту електронного документа і, відповідно, різні рівні електронної ідентифікації автора електронного документа.

Електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи. Електронна ідентифікація здійснюється за допомогою засобів електронної ідентифікації.

Засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг. Міжнародні договори України щодо електронних довірчих послуг

повинні передбачати порядок подання повідомлень та визнання схем електронної ідентифікації. Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Схема електронної ідентифікації визначається Кабінетом Міністрів України (ст.15 Закону України «Про електронні довірчі послуги»). Використання кваліфікованих електронних підписів та печаток забезпечує високий рівень довіри до схем електронної ідентифікації. Використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації.

Електронний документ повинен мати реквізити, установлені для аналогічного паперового документа (п. 2 розд. ІІ наказу Мін'юсту від 11.11.14 р. № 1886/5, далі – Наказ № 1886/5). Згідно зі ст. 9 Закону «Про бухгалтерський облік та фінансову звітність в Україні» усі первинні та зведені облікові документи повинні містити такі обов'язкові реквізити: назву документа (форми); дату складання; назву підприємства, від імені якого складено документ; зміст, обсяг та одиницю виміру господарської операції; посади осіб, відповідальних за провадження госпоперації та правильність її оформлення; особистий підпис або інші дані, які дозволяють ідентифікувати особу, яка взяла участь у госпоперації. Усі ці реквізити необхідно вказувати і в електронному первинному документі. Передача електронного документа може здійснюватися в електронній формі за допомогою засобів інформаційних або телекомунікаційних систем, а також шляхом передачі електронного носія (диска, флешки і т. д.), на якому записано цей документ.

Запитання для самоконтролю і самостійного опрацювання:

1. Визначте поняття, ознаки та характеристика електронного документа.
2. Що є оригіналом електронного документа?

3. Електронний документообіг: поняття, ознаки, суб'єкти, сфера застосування, умови функціонування.

4. Порядок відправлення, передавання та одержання електронних документів.

5. Що таке електронний цифровий підпис?

6. Чим відрізняються кваліфікований електронний підпис, електронний підпис і удосконалений електронний підпис?

Рекомендована література:

1. Про особливості надання публічних (електронних публічних) послуг : Закон України. *Відомості Верховної Ради України.* 2021, № 47. Ст. 383.

2. Про електронні документи та електронний документообіг : Закон України. *Відомості Верховної Ради України.* 2003, № 36. Ст. 275.

3. Про електронні довірчі послуги : Закон України. *Відомості Верховної Ради України.* 2017, № 45. Ст. 400.

4. Про бухгалтерський облік та фінансову звітність в Україні : Закон України. *Відомості Верховної Ради України.* 1999, № 40. Ст. 365.

РОЗДІЛ 8.

ЕЛЕКТРОННІ ГРОШІ: ПОНЯТТЯ, ЗМІСТ ТА ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ В УКРАЇНІ

Стрімкий розвиток електронної комерції та технологій зіграли свою роль у проникненні електронних грошей в українську економіку. Сьогодні чимало Інтернет-магазинів та інших суб'єктів господарювання, які так чи інакше пов'язані з технологіями та комунікаціями, крім готівкового й безготівкового розрахунків приймають оплату за товари та послуги в електронних грошах [69]. Розвиток систем електронних грошей на сучасному етапі еволюції суспільства характеризується поступовим звуженням сфери використання готівки та паперових платіжних документів, переходом до нових платіжних інструментів і сучасних технологій платежів. Електронні гроші широко залучаються до обігу і стають важливим інструментом фінансової інфраструктури економічно розвинутих країн.

Термін «електронні гроші» часто застосовується для позначення широкого спектра платіжних інструментів (цифрові гроші, цифрова готівка, електронна готівка, Інтернет-гроші, кібергроші тощо), заснованих на інноваційних технологічних рішеннях.

Відповідно до Директиви Європейського парламенту і ради від 16 вересня 2009 року **електронні гроші** означають грошову вартість, що зберігається в електронній, у тому числі магнітній, формі як вимога до емітента, що випускається після отримання коштів для здійснення платіжних транзакцій, і що її приймає фізична чи юридична особа, крім емітента електронних грошей» [70].

У вітчизняному законодавстві застосування і використання електронних грошей регламентується окремим законодавчим нормативним актом – Законом України «Про платіжні послуги» [71]. А також Положенням про електронні гроші в Україні, затверджене постановою Національного банку України від 04.11.2010 р. № 481.

Стаття 15 зазначеного Закону надає таке визначення **терміну** «**електронні гроші**» – одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими особами, ніж особа, яка їх випускає, і є грошовим зобов'язанням цієї особи, що виконується в готівковій або безготівковій формі.

Таким чином, електронні гроші – грошове зобов'язання особи, яка їх випустила. Вони не мають власної внутрішньої вартості (на відміну від, наприклад, монет, вироблених із дорогоцінних металів). Цим вони відрізняються від грошей, які випускає Нацбанк України, і які є національною валютою. Випущені емітентом електронні гроші на 100% забезпечуються традиційними формами грошей та інколи – іншими високоліквідними активами, причому в більшості випадків емітент зобов'язується на вимогу власника грошей обміняти їх на звичайні гроші і навпаки. Також хибним є ототожнення електронних грошей із безготівковими грішми [72].

У 2020 році Нацбанк України оновив регулювання ринку електронних грошей і гармонізував його із законодавством України та Європейського Союзу у сфері здійснення фінансового моніторингу. Відповідна постанова Правління НБУ від 11 вересня 2020 р. № 133 «Про затвердження Змін до Положення про електронні гроші в Україні» набрала чинності 15.09.2020 р. Цим документом, зокрема, було встановлено вимоги Центрального банку до господарюючих суб'єктів, що займаються випуском, обігом та погашенням електронних грошей, зобов'язання здійснювати заходи з належної перевірки користувачів електронних грошей, у тому числі їх ідентифікацію та верифікацію, як і під час відкриття рахунків. Йдеться про клієнтів, які відкривають електронні гаманці, щоб здійснювати різні операції: купувати товари, платити за

послуги тощо. Крім того, перекази з використанням електронних грошей мають супроводжуватися інформацією про платника та отримувача. Також у законодавство офіційно введено поняття «електронний гаманець».

Щоб підвищити захист прав користувачів електронних грошей, регулятор також встановив низку вимог до банків-емітентів електронних грошей. Зокрема, банк-емітент:

- зобов'язаний перед укладенням договору з користувачем інформувати його про створення електронного гаманця та отримати його згоду;
- не може надавати кредит із коштів, отриманих як передоплата за випущені електронні гроші;
- повинен надати користувачу інформацію про найменування і місцезнаходження емітента та оператора; умови та порядок створення/використання електронного гаманця; порядок, способи здійснення переказів між користувачами — фізичними особами та оплати за товари електронними грошима; суму та порядок сплати комісійної винагороди користувачем, а також іншу інформацію;
- не може залучати комерційних агентів для випуску електронних грошей.

Вважається, що **використання електронних грошей** — це сукупність відносин між емітентом, оператором, агентами, торговцями та користувачами щодо здійснення випуску, розповсюдження, розрахунків за товари, переказів між користувачами — фізичними особами, обмінних операцій, приймання агентом з розрахунків електронних грошей в обмін на готівкові/безготівкові кошти, погашення емітентом електронних грошей та поповнення електронних гаманців.

Таким чином, законодавець виділяє таких ***учасників*** відносин з електронними грошима:

емітент — банк-резидент, що здійснює випуск електронних грошей і бере на себе зобов'язання з їх погашення;

емітент-нерезидент — особа, яка здійснює випуск електронних грошей за межами України для їх

використання в міжнародній системі Інтернет-розрахунків, відомості щодо якої внесено до Реєстру платіжних систем, систем розрахунків, учасників цих систем та операторів послуг платіжної інфраструктури;

оператор електронних грошей (далі — оператор) — юридична особа, інша, ніж емітент, яка на підставі договору, укладеного з емітентом, виконує операційні, інформаційні та інші технологічні функції, що забезпечують використання електронних грошей;

комерційний агент — юридична особа-резидент, представництво установи міжнародної організації, членом якої є Україна або яка здійснює в Україні діяльність з надання гуманітарної допомоги на підставі міжнародних угод з Україною (представництво міжнародної організації), — особа, яка на підставі договору, укладеного з емітентом, здійснює:

- розповсюдження електронних грошей (далі — агент з розповсюдження);
- надання засобів поповнення електронними грошима електронних гаманців (агент з поповнення);
- обмінні операції з електронними грошима (агент з обмінних операцій);
- приймання електронних грошей в обмін на готівкові/безготівкові кошти (агент з розрахунків);

користувач — фізична особа або суб'єкт господарювання, який є власником електронних грошей і має право використовувати їх для придбання товарів і здійснення переказів з урахуванням обмежень, установлених законодавством.

Отже, випуск електронних грошей в Україні мають право здійснювати лише банки і лише в гривнях. Перелік банків-емітентів визначає Національний банк України. Перелік можна подивитись на офіційній веб-сторінці Нацбанку [73]. Випуск електронних грошей здійснюється шляхом їх надання користувачам або комерційним агентам в обмін на готівкові або безготівкові кошти. Банк, що здійснює випуск електронних грошей, зобов'язаний погашати випущені ним електронні гроші на вимогу користувача. При цьому емітент зобов'язаний забезпечити, щоб сума випущених ним

електронних грошей не перевищувала: суми отриманих ним від користувачів та агентів (крім агента з поповнення/агента з розповсюдження) готівкових або безготівкових коштів та суми отриманих агентом з поповнення/агентом з розповсюдження готівкових коштів, які мають бути перераховані емітенту.

Емітент зобов'язаний протягом 10 календарних днів з початку здійснення випуску електронних грошей повідомити про це Національний банк.

Електронні гроші є випущеними з часу їх завантаження емітентом або оператором на електронний гаманець, що перебуває в розпорядженні користувача або агента.

Емітент зобов'язаний щокварталу до 10 числа місяця, наступного за звітним періодом, надавати Національному банку інформацію про діяльність, пов'язану з випуском та використанням електронних грошей.

Сьогодні не існує єдиної класифікації електронних грошей. У науковій літературі фахівці пропонують систематизувати електронні гроші за наступними критеріями:

За типом носія*:*

1. *На базі фізичного пристрою* (англ. hardware-based): електронні гроші зберігаються на спеціальному пристрої (наприклад, на чіпі, вбудованому в смарт-карту), що одночасно використовується для здійснення платежів. При використанні такого типу платіжних інструментів транзакція між платником та отримувачем платежу іноді може бути виконана без додаткового під'єднання смарт-карт до мережі (третьої особи).

2. *На базі програмного забезпечення* (англ. network-based чи software -based), або їх ще називають онлайн-грошима: електронні гроші зберігаються на накопичувачах інформації у формі файлів бази даних/масиву інформації. У цьому випадку, при здійсненні транзакції запит до оператора електронних грошей є обов'язковим для завершення операції.

Типом технології зберігання*:*

1. Із централізованим веденням рахунків (англ. accoun-based): всі транзакції записуються та

авторизуються через централізовану систему рахунків, управління якою здійснює система електронних грошей.

2. Із використанням електронних записів/символів (англ. token-based): транзакція не потребує авторизації і електронні гроші існують у формі електронних символів, які обертаються всередині комп'ютерної чи телекомунікаційної мережі, або шляхом прямого під'єднання до такої мережі електронних пристроїв (наприклад, електронних чіпів у смарт-картах чи RFID-модулів у смартфонах).

Ступенем анонімності:

1. *Повністю анонімні системи* електронних грошей: ідентифікація користувача не вимагається ані при придбанні ним електронних грошей, ні при здійсненні ним транзакцій, а отже, ідентифікація та відстеження здійснених операцій між платником та отримувачем платежу є неможливою.

2. *Системи, що вимагають ідентифікації*: платник та отримувач платежу, здійсненого за допомогою електронних грошей, мають ідентифікувати себе, надаючи, таким чином, можливість системі електронних грошей відстежувати транзакції.

3. *Системи*, що вимагають *часткової ідентифікації*: як правило, вимоги щодо часткової ідентифікації клієнтів можуть бути встановлені на законодавчому рівні та передбачати мінімальну ідентифікацію клієнта (наприклад, за паспортними даними). Проте, доступ до інформації щодо ідентифікації клієнтів та здійснені ними угоди можуть мати лише чітко визначені державні інституції.

Розміром платежу:

1. *Системи пікоплатежів* (англ. picopayments): можуть здійснюватись платежі розміром від менш ніж 1 євроценту до 1 євро.

2. *Системи мікроплатежів*: можуть здійснюватись платежі розміром від 1 євро до 10 євро. Здійснення платежів такого розміру із використанням чеків чи платіжних карт часто не є економічно вигідним.

3. *Системи макроплатежів*: можуть здійснюватись транзакції більшого розміру [72].

Запитання для самоконтролю і самостійного опрацювання:

1. Що таке Інтернет-платіжна система?
2. Що таке електронні гроші?
3. Назвіть платіжні системи на основі електронних грошей, які використовуються в Україні?
4. Які ви знаєте українські платіжні системи на основі кредитних карток? На основі смарт-карток?

Рекомендована література:

1. Про затвердження Змін до Положення про електронні гроші в Україні : Постанова Правління НБУ від 11 вересня 2020 року № 133.
2. Про платіжні послуги : Закон України від 30.06.2021. № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#n1249
3. Положенням про електронні гроші в Україні : Постанова Національного банку України від 04.11.2010 № 481.
4. Про здійснення операцій з використанням електронних платіжних засобів : Постанова Національного банку України від 05.11.2014 № 705. URL: http://zakon4.rada.gov.ua/laws/show/v0705500-14
5. Про електронну комерцію : Закон України. URL: http://zakon4.rada.gov.ua /laws/show/675-viii
6. Дучак Б. Електронні гроші в (У)країні третього світу. URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ000975
7. Директива європейського парламенту і ради 2009/110/ЄС від 16 вересня 2009 року про започаткування та здійснення діяльності установами-емітентами електронних грошей і пруденційний нагляд за нею, про внесення змін до директив 2005/60/ЄС і 2006/48/ЄС та про скасування Директиви 2000/46/ЄС.
8. Кравчук В., Науменко Д., Глибовець А. Електронні гроші в Україні / Аналітичний звіт. — Київ : Альфа-ПІК, 2012. — 64 с.

РОЗДІЛ 9.

ПРАВОВИЙ РЕЖИМ ВІРТУАЛЬНОЇ ВАЛЮТИ (КРИПТОВАЛЮТИ)

9.1. Зміст та юридична природа криптовалюти

В Україні активно продовжується інформатизація економіки, важливим елементом якої є використання цифрових валют. Україна входить у першу десятку країн світу за кількістю користувачів криптовалютою. За даними аналітичної компанії Chainalysis «Глобальний індекс прийняття криптовалют у 2020 році: криптовалюта – глобальне явище» – українці є найактивнішими користувачами криптовалюти в світі. Країна тоді зайняла першу сходинку. У 2021 році Україна має 4-е місце, пропустивши вперед В'єтнам, Індію і Пакистан [74]. За останній рік ринок криптовалют виріс і досяг загальної ринкової вартості, яку оцінюють приблизно у 2 трильйони доларів США. І він продовжує розширятися попри всі обмеження. Сьогодні добова сума угод на ринку криптовалют коливається в межах 50–60 млрд дол. США. Тому вироблення єдиних правових стандартів, юридичних механізмів регулювання відносини за участю криптовалют є актуальним питанням як для України, так і для світової спільноти. Фінрегулятори різних країн не можуть прийти до спільної думки щодо того, чим саме є криптовалюта. Сьогодні у світі та в Україні не вироблено єдиного підходу до встановлення юридичної природи віртуальної валюти, відсутнє бачення того, яким чином слід трансформувати віртуальну валюту в фіатну валюту і чи потрібно це робити взагалі. Аналіз практики тих держав, які лише впроваджують правове регулювання обігу криптовалюти та криптовалютного бізнесу, свідчить, що більшість із них для надання віртуальній валюті правового статусу

прирівнюють її до вже наявної в їхньому законодавстві категорії. Таким чином, в Австрії криптовалюта вважається нематеріальним активом, у Німеччині — фінансовим інструментом, в Ісландії — цифровою валютою, у Фінляндії — програмним забезпеченням, який є «сировинним товаром».

Спочатку звернемось до історії. Концепція біткоїн була вперше описана в офіційному документі, опублікованому 31 жовтня 2008 року людиною або групою людей під псевдонімом Сатоші Накамото [75]. Сатоші Накамото вперше описав принцип роботи платіжної системи у вигляді однорангової мережі, який в 2009 році був представлений ним же у вигляді відкритого коду програми клієнта — Bitcoin в Інтернеті. Крім того, ним було створено спеціальний додаток — гаманець для комп'ютерів, що містив криптовалюту Bitcoin (далі — «біткоїн»). За подальшу розробку і координацію функціонування мережі тепер відповідає спільнота розробників. Однак це не означає, що лише розробники приймають рішення про те, в якому напрямку буде рухатися біткоїн. Будь-які значні зміни в протоколі можливі тільки після того, як з ними погодиться більшість майнінгових пулів — об'єднань власників комп'ютерних потужностей, внаслідок яких і «народжуються» нові біткоїни.

На офіційному сайті біткоїн має назву «open source P2P digital currency» — «вільна пірінгова цифрова валюта». Монети в системі біткоїн (BTC) є криптографічними (математичними) хеш-кодами, кожен з яких є унікальним і не може використовуватися двічі. Bitcoin — це платіжна система, заснована на P2P-технологіях (англ. Peer-to-peer — рівний до рівного). Принцип її роботи побудований на відкритому протоколі передачі даних. Система використовує єдину розрахункову одиницю «біткоїн» — перша і найвідоміша криптовалюта [76].

В сучасних вітчизняних та міжнародних дослідженнях представлені різновекторні позиції стосовно сутності «віртуальної валюти». Наприклад, у країнах ЄС загальновизнаним є наступне визначення «**віртуальної**

валюти»: *це цифрове представлення вартості, яке не видається або не гарантується центральним банком або державним органом, не обов'язково приєднується до законодавчо встановленої валюти і не має юридичного статусу валюти чи грошей, але приймається фізичними та юридичними особами як засіб обміну і може передаватися, зберігатися та торгуватися в електронному вигляді.* Дане визначення було закріплено в Директиві ЄС № 2018/843 від 30.05.2018 р.

На міжнародному рівні одне з офіційних визначень віртуальної валюти було запропоновано Міжнародним валютним фондом, що визначив **віртуальну** *валюту як цифровий вираз вартості, випущений (issued) приватними розробниками (developers) та вираженій у їх власній розрахунковій одиниці.*

Вперше в Україні рекомендаційні роз'яснювальні документи, якими намагались врегулювати сферу криптовалюти, з'явились ще в 2014 році. НБУ опублікував Роз'яснення «Щодо правомірності використання в Україні «віртуальної валюти/криптовалюти Bitcoin». В даному документі НБУ розглядав криптовалюту «Bitcoin» як грошовий сурогат. Через місяць після цього, НБУ доповнює свою позицію щодо криптовалют, та відносить операції з «віртуальною валютою/криптовалютою «Bitcoin»» до операцій з торгівлі іноземною валютою. Також визначається, що «Bitcoin» є грошовим сурогатом, який не має забезпечення реальної вартості, а діяльність з купівлі-продажу «Bitcoin» за долари США або іншу іноземну валюту має ознаки функціонування так званих «фінансових пірамід». Пізніше, у 2017 році, відбувається спільна заява НБУ та Нацкомфінпослуг щодо статусу криптовалют в Україні, згідно з якою: «криптовалюта не може бути визнана грошима, валютою або законним платіжним засобом, не є валютною цінністю, електронними грошима, цінним папером. Таким чином, криптовалюта не може бути визнана грошовим сурогатом».

Національне агентство з попередження корупції та Держфінмоніторинг (Україна) опублікувало інструкцію з правилами декларування, де віртуальним активам

присвячена окрема глава «Особливості відображення відомостей про нематеріальні активи». У правилах є визначення поняття «**криптовалюта**» — **це цифрові (віртуальні) кошти в формі токенів, створені і враховуються в розподіленому реєстрі.**

Вже в 2020 році були внесені зміни в Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдженню зброї масового знищення», де дали визначення поняттю **криптовалюти як віртуальному активу**, а саме: «**цифровий вираз вартості, яким можна торгувати в цифровому форматі або переводити, і який може використовуватися для платіжних або інвестиційних цілей».** Це дійсно важливий крок для нашої держави, бо після легалізації криптовалюти, з'явилась можливість подальшого законодавчого регулювання відносин щодо неї.

8 вересня 2021 року Верховна Рада України у другому читанні прийняла Закон України «Про віртуальні активи» [77], який встановлює правове регулювання обігу віртуальних активів в Україні. «Законом передбачено комплексне врегулювання правовідносин, що виникають у зв'язку з обігом віртуальних активів в Україні, визначено права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обігу віртуальних активів», — повідомляється на сайті парламенту. Законом також встановлено загальні принципи державного регулювання обороту віртуальних активів та органи, що здійснюють державне регулювання у сфері обороту віртуальних активів. Зокрема, повноваженнями щодо ринку віртуальних активів наділені Національний банк України, Національна комісія з цінних паперів та фондового ринку, Державний реєстр постачальників послуг.

Цей закон визначає віртуальний актив наступним чином:

- це нематеріальне благо;
- віртуальний актив є об'єктом цивільних прав;
- віртуальний актив має вартість;

- існує віртуальний актив лише в електронній формі у вигляді сукупності даних;
- існування віртуального активу забезпечується певним програмним комплексом обміну даних.

На думку фахівців, зміст зазначеного закону містить ряд недоліків. По-перше, якщо віртуальний актив це нематеріальне благо, виходить «віртуальні активи» не дорівнює «криптовалюта»: наприклад, NFT також мають вартість, існують лише в електронній формі та є нематеріальним благом у розумінні законодавства. По-друге, в Законі України про запобігання та протидію легалізації (відмиванню) доходів вже міститься визначення віртуального активу – і воно є іншим: віртуальний актив визначається як цифрове вираження вартості, яке можна торгувати у цифровому форматі, переказувати й використовувати для платіжних/інвестиційних цілей. Постає питання – так що ж в результаті є віртуальним активом: лише криптовалюта чи ні? Виходячи з визначення віртуального активу, будь-який цифровий токен, NFT та навіть ігрові скіни та сети – все це підходить під визначення віртуальних активів: вони нематеріальні, існують лише у цифровій формі, однозначно мають вартість і функціонують лише у межах певної цифрової системи – екосистеми певної гри, блокчейн-платформи тощо.

Таким чином, залишається відкритим питання щодо того, вважати віртуальним активом лише цифрові платіжні засоби чи будь-які цифрові активи та, відповідно, яке із визначень віртуальних активів є правильним [78]. У науковій літературі зустрічаємо такі характеристики електронної валюти, як: «цифрова валюта», «електронні платіжні засоби», «цифрові активи», «засіб обміну» тощо. Загалом усі теперішні підходи можна звести до наступних, де віртуальна валюта визнається: 1) грошовими коштами; 2) грошовим сурогатом; 3) товаром (майно, актив); 4) майновим правом і 5) формою платіжної послуги [79].

Науковці виділяють такі основні ознаки віртуальної валюти:

1) криптовалюта має вигляд цифрового коду, який генерується відповідно до складних математичних алгоритмів;

2) криптовалюта може виконувати функції фіатних грошей, наприклад виступати мірою вартості, засобом платежу, засобом обміну;

3) криптовалюті притаманна анонімність учасників операцій – у мережі використовуються криптографічні методи асиметричного шифрування даних із застосуванням публічного та приватного ключів;

4) облік операцій з криптовалютами здійснюється за допомогою технології блокчейн;

5) криптовалютна система – замкнута децентралізована система, правила функціонування якої встановлюються її учасниками; криптовалюти не випускаються центральним банком, тому їх емісія не контролюється з боку державної влади; курс криптовалют формується ринковим шляхом і безпосередньо ніяк не пов'язується з економікою будь-якої країни;

6) відсутність реальної їх забезпеченості (вартість криптовалют є результатом співвідношення попиту та пропозиції на них серед користувачів) [80]. Але багато компаній декларують, що їхня криптовалюта чимось підкріплена і забезпечена [81] (рис. 3).

Незвичайне забезпечення криптовалют

№	Криптовалюта	Країна	Забезпечення
1	Royal Mint Gold-Stablecoin	Велика Британія	Золото
2	Carat	Ізраїль	Діаманти
3	Farad	Малайзія, ОАЕ	Технологія та виробництво суперконденсатора
4	Tether	Гонконг	Долари США
5	Petro	Венесуела	Нафта
6	Tcoin	Швейцарія	Метали
7	Watercoin	США	Технології очищення води
8	Coinloan	Естонія	Позика у криптовалюті
9	Amar Hidroponia	Мексика	Урожай перцю

Рис. 3.

В навчальній і науковій літературі є чимало спроб визначити відмінності між електронними грошима і віртуальною валютою. Спробуємо систематизувати ці напрацювання.

Форма вираження. Відмінність криптовалют від електронних грошей полягає в тому, що вона не має якоїсь особливої матеріальної чи електронної форми. Це число, яке записується у відповідній позиції інформаційного пакета протоколу передачі даних, і не несе ніякої інформації про транзакції між адресами системи. Криптовалюта функціонує завдяки механізму асиметричного шифрування. Одиниця криптовалюти — це код, який народжується в результаті складних комп'ютерних математичних обчислень

Емітент. Емітентом електронних грошей в Україні може бути банк, який повинен отримати дозвіл на це Нацбанку. В інших країнах це право надається і іншим установам, але це завжди визначені суб'єкти права (як правило юридичні особи). У створенні віртуальної валюти державні структури участі не приймають — криптовалюту виробляють самі користувачі. Цей процес називається «Майнінг». Він побудований на рішенні комп'ютерами складних математичних задач. Комп'ютери при цьому знаходяться в самих різних точках планети, а майнери для більшої ефективності роботи об'єднуються в пули. За свою роботу вони отримують певну нагороду. Наприклад, нові біткоїни генеруються кожен раз, коли знайдений новий блок транзакцій. Частота створення таких блоків постійна: 6 одиниць / годину. Кількість біткоїнів в блоці періодично зменшується — кожні чотири роки відбувається так званий «халвінг», тобто зниження вдвічі нагороди майнерам. Таким чином, є точно розписаний графік емісії біткоїна, також відома і загальна сума монет, які будуть коли-небудь випущені: 21 мільйон. Остання емісія повинна відбутися приблизно у 2140 році [76].

Державний нагляд. При випуску і обігу криптовалют відсутній централізований контроль або нагляд у вигляді центрального банку або іншого державного регулятора, який повинен здійснювати роль центрального

адміністратора [79]. Емісія монет і обробка транзакцій здійснюються колективно учасниками мережі. Таким чином, ніхто не може контролювати криптовалюту, заблокувати або скасувати транзакцію. Однак приєднатися до мережі може будь-хто.

Ідентифікація користувача. Вважається, що операції з криптовалютою є анонімними і це головний чинник їх великої популярності. Але швидше, можна говорити про відносну анонімність. Іншими словами, рух коштів і поточний баланс адреси може побачити будь-яка людина, але сказати, кому саме вони належать, досить складно. Однак при достатньому бажанні можна відстежити IP-адреса відправника, навіть якщо він і не зберігається в блокчейні. Наприклад, такою інформацією володіють власники серверів деяких провайдерів гаманців. До теперішнього часу вже розроблені досить ефективні інструменти для аналізу транзакцій. Їх функціонал дозволяє криптовалютним компаніям миттєво з'ясувати наскільки надійний їхній контрагент і чи оперує він коштами, які раніше використовувалися в незаконних фінансових операціях.

Крім того, необхідно зазначити, що при спробах законодавчо врегулювати обіг криптовалюти, більшість країн (у т.ч. і Україна) покладають на суб'єкта первинного фінансового моніторингу, що надає послуги переказу коштів обов'язок ідентифікувати й перевірити платника (ініціатора переказу).

Розподілена база «blockchain» демонструє усі проведені транзакції. В такому реєстрі будь-який користувач може відстежити територію, де була проведена така транзакція.

Щодо правозахисної практики віртуальних активів, то тут також спостерігаємо наслідки законодавчої невизначеності і недосконалості в регулюванні. Різні інстанції по-різному трактують зміст і визначення криптовалюти і по-різному вирішують спори щодо її обігу:

- **Суд** визнав криптовалюту віртуальною річчю і відмовив на основі цієї причини в судовому захисті: *Рішенням Дарницького районного суду від 24.03.2016 року*

у справі 753/599/16-ц [82], підтриманим Апеляційним судом міста Києва, позивачу було відмовлено в задоволенні позову про витребування від відповідача Bitcoin у якості оплати за виконану роботу. Суд мотивував своє рішення тим, що криптовалюта належить до віртуально-цифрової продукції й не є предметом матеріального світу, не має індивідуальних ознак, її порядок обігу нормативно не врегульовано, а тому вона не може бути об'єктом судового захисту.

- Банк затримав переказ коштів із рахунку позивача, відкритого на криптобіржі, на власний картковий рахунок в іноземній валюті у зв'язку з правовою невизначеністю статусу криптовалюти*. Позивач звернувся до Печерського районного суду міста Києва з позовом до АТ КБ «Приватбанк» про захист прав споживача та стягнення грошових коштів у вигляді пені за прострочення проведення Банком відповідного переказу. Рішенням від 23 липня 2020 року, підтриманим постановою Київського апеляційного суду у справі № 757/46845/19-ц, суд частково задовольнив згадуваний позов, стягнув із Банку пеню та визнав, що фінансові операції можуть бути зупинені банками виняткова на підставі ст. 17 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». Крім того, суд установив, що операції з купівлі-продажу криптовалют не належать до арбітражних операцій на ринку FOREX та визнав криптовалюту цифровою (віртуальною) валютою і фактично, підтвердив законність операцій із нею у вигляді укладання публічних електронних договорів, розміщених на сайті криптобіржі [83].*

- Криптобіржі блокують криптоактиви на електронних гаманцях за запитами правоохоронців*. Ознайомившись із рішенням Одеського окружного адміністративного суду від 24.12.2020р. у справі 420/7905/20, можна зробити висновок, що інспектори департаменту кіберполіції Національної поліції України розуміють, що таке криптовалюта і які*

потрібно вчиняти оперативні дії в разі її крадіжки. Відповідно до змісту згадуваного рішення, інспектор відділу управління протидії кіберзлочинам в Одеській області департаменту кіберполіції Національної поліції України у формі письмового звернення до криптобіржі просив заблокувати виведення криптовалюти з електронних гаманців у зв'язку з розслідуванням інциденту з крадіжкою цієї криптовалюти в інших осіб і наявністю підстав вважати, що викрадена криптовалюта була переведена на відповідні електронні гаманці, які необхідно заблокувати. У результаті належно складеного звернення біржа його задовольнила, відповідні електронні гаманці було заблоковано [84].

9.2. Правовий режим криптовалют у світі: підходи до регулювання

На думку експертів визнання на державному рівні технології блокчейн і одного з продуктів її реалізації – криптовалюти, можуть суттєво трансформувати українську економіку та сприяти побудові цифрової держави.

Більшість передових країн вже активно експериментують із впровадженням блокчейну у сферах державної та економічної діяльності. Розглянемо міжнародний досвід регулювання сфери віртуальних валют на прикладі окремих країн.

Першими країнами, де було офіційно визнано біткоїн як віртуальну валюту, стали Німеччина і Сальвадор. У **Німеччині** віртуальна валюта не належить до законного платіжного засобу, а її створення чи використання як засобу оплати не потребує будь-яких дозволів. Проте здійснення операцій з продажу криптовалюти та будь-яке її комерційне використання вимагають наявності відповідної ліцензії. У **Сальвадорі** біткоїн є офіційним засобом платежу нарівні зі звичайною валютою. Тепер ціни в країні можуть встановлювати в біткоїнах, в криптовалюті можна буде платити податки. Також обмін біткоїнів не оподатковуватиметься. В **Ісландії**

криптовалюта законом віднесена до цифрових валют, але одночасно законом введено фактичну заборону юридичним особам здійснювати обмінні операції віртуальною валютою. Тобто вони не можуть купувати біткоїни у закордонних контрагентів, адже це розглядається як перерахування коштів за кордон. Натомість заборони на продаж біткоїнів немає. **Республіка Польща** визначає криптовалюту як «цифрове представлення активів, що не видаються центральним банком, кредитною установою або організацією з електронних грошей, яка за певних умов може бути використана як альтернатива грошам». Отже, Польща у визначенні криптовалюти звертає увагу на її децентралізованість («не видаються центральним банком, кредитною установою або організацією з електронних грошей»), проте не заперечує можливість її використання на заміну законним платіжним засобам [85]. У **Болгарії** криптовалюта визнана фінансовим активом. У **Білорусі** дозволено проводити з криптовалютою процедуру обміну, купівлі або продажу, передачі у спадок і зберігання в спеціальних гаманцях. У **Фінляндії** криптовалюта визначається як фінансовий інструмент, операції з ними вважаються приватними угодами й звільнені від ПДВ. У **Росії** криптовалюта визнана засобом платежів, інвестицій і накопичень. У **Хорватії, Киргизстані, Індонезії** та **Литві** криптовалюта не визнана легальним засобом платежу, а в **Болівії та Бангладеш** її обіг взагалі заборонений.

В науковій літературі заведено виділяти декілька підходів до правового регулювання ринку криптовалют.

Так, *економічно орієнтований підхід* передбачає інтеграцію криптоіндустрії в економіку держави та забезпечення належних умов для її розвитку. Держава не створює спеціального законодавства, а тільки вносить відповідні зміни до актів, що вже регулюють фінансову діяльність у країні (Канада, США, Японія). Наприклад, в Японії технологія блокчейн і криптовалюти є складовою державної стратегії розвитку цифрових фінансів та побудови «безготівкового суспільства». У квітні 2017 року Японія визнала криптовалюти легальними засобами платежу і прийняла відповідний закон про платіжні

послуги. Отже, японське законодавство дозволяє купівлю, продаж. віртуальної валюти та її обмін на інші криптоактиви. Крім цього, законодавство спрямовано на захист споживачів і підвищення регуляторної визначеності. Постачальники послуг віртуальних активів підлягають обов'язковій державній реєстрації – в Агентстві фінансових послуг Японії (FSA), а криптобіржі та криптообмінники взаємодіють з фіатними грошима, контроль за якими здійснюють державні органи. Зареєстровані криптовалютні компанії сплачують податок на споживання від продажу криптовалют. Японський регулятор посилив вимоги до кібербезпеки і дотримання вимог фінансового моніторингу (AML/CFT), головне завдання якого – запобігання та протидія відмиванню коштів, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення.

Підхід спостереження або так звані «регуляторні фінтех-пісочниці» передбачає створення спеціальних правових зон для криптоіндустрії, які дозволяють регуляторам спостерігати за розвитком та функціонуванням криптобізнесу, перш ніж регулювати його на законодавчому рівні. Регулятори не прагнуть заборонити чи обмежити розвиток криптоіндустрії. Прикладом реалізації такого підходу є Швейцарія, де операції з криптовалютами є законні. Правила ведення бізнесу для місцевої криптоіндустрії встановлює державний регулятор – Служба з нагляду за фінансовими ринками (FINMA). Для комфортної роботи на території країни криптобіржі та криптобмінники повинні отримати ліцензію у фінансовому управлінні Швейцарії. Швейцарське законодавство розглядає криптовалюти як активи, операції з якими обкладаються податком на майно. Влада швейцарського кантону Цуг – місцевої Криптодолини – дозволяє компаніям і приватним особам сплачувати податки в двох найпопулярніших криптовалютах – BTC і ETH.

Підхід до мінімізації ризиків вирізняється нейтральним або нейтрально-позитивним ставленням до криптовалют. Держави приймають мінімально необхідні

закони, щоб контролювати ринок віртуальних активів, але не перешкоджати розвитку криптоіндустрії.

Наприклад, у Великобританії криптовалюти не є легальним засобом платежу в країні. Водночас криптовалютні біржі та криптообмінники повинні отримати державну реєстрацію в Управлінні з фінансового регулювання і нагляду (FCA).

Обмежувального підходу дотримуються держави, які сприймають криптоіндустрію як цілковиту загрозу їхній фінансовій стабільності та вживають відповідні стримувальні заходи. Цей підхід характеризується повною або частковою забороною діяльності, що пов'язана з криптовалютами.

Подібна ситуація спостерігається в Китаї, де 2017 року влада КНР заборонила проведення ICO і діяльність криптовалютних бірж. Попри те, що в Китаї є правове визначення біткоїна як віртуального товару, – будь-які операції з криптовалютою на території КНР незаконні.

Таким чином на сучасному етапі розвитку нормативного забезпечення можна зазначити, що в жодних юрисдикціях немає єдиних стандартів регулювання криптовалют і кожен центральний банк та уповноважений орган керується власними підходами: від формального дозволу або застосування загальних принципів регулювання у сфері платежів до повної заборони такої діяльності. Якщо розглянути, які можуть бути наслідки в умовах формального дозволу здійснювати діяльність із цифровими валютами, то центральним банкам, які дотримуються такого підходу, слід звернути увагу, що є ризик шахрайств, хакерських атак і махінацій. Здійснення повної заборони на зазначену діяльність може призвести до згортання інноваційних проєктів у цій сфері і перенесення їх у прозорішу регулятивну юрисдикцію [81].

Запитання для самоконтролю і самостійного опрацювання

1. Який підхід державного регулювання обігу криптовалют, на ваш погляд, найбільш ефективний або перспективний?

2. Чим криптовалюта відрізняється від електронних грошей?

3. Назвіть ознаки криптовалюти.

4. Чи потрібне матеріальне забезпечення криптовалюті?

5. Які форми правового захисту власників криптовалюти існують на сьогодні?

Рекомендована література:

1. Міжнародний досвід законодавчого регулювання питання функціонування криптовалют, криптовалютних бірж, майнінгу та виводу в фіат (Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром). URL: https://radaprogram.org/sites/ default/files/infocenter/piblications/65.pdf

2. Кремінський О. Правовий режим віртуальної валюти (криптовалюти) в Україні. *Path of Science*. 2020. Vol. 6, No 4. URL: file:///C:/Users/%D0%9B%D0%B0%D0%BD%D0%BE%D1%87%D0%BA%D0%B0/Downloads/732-2165-1-PB.pdf

3. Казначєєва Д. В., Дорош А. О., Криптовалюта: проблеми правового регулювання. *Вісник Кримінологічної асоціації України*. № 2(23). 2020. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9575/Kryptovaliuta_%20problemy%20pravovoho%20rehuliuvannia_Kaznachieieva_Dorosh_2020.pdf?sequence=1&isAllowed=y

4. Шинкаренко О. М., Рогова Н. В., Панівнік І. А. Особливості нормативного регулювання криптовалют: світовий досвід. *Фінансовий простір*. 2018, № 3 (31). С. 139-144.

5. The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon. URL: https://blog.chainalysis.com/ reports/2020-global-cryptocurrency-adoptionindex-2020

6. Лясківський І. Новий закон про віртуальні активи – нові можливості для бізнесу. URL: https://ain.ua/2021/09/13/novij-zakon-pro-virtualni-aktivi-novi-mozhlivosti-dlya-biznesu-kolonka-yurista/

РОЗДІЛ 10.

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

10.1. Загальні відомості про юридичну відповідальність за порушення законодавства у сфері використання інформаційно-комунікаційних технологій

Сучасний етап розвитку України безпосередньо впливає на стан її інформаційної безпеки. При цьому висхідна роль інформаційних відносин є ключовим компонентом діяльності органів державної влади, державного управління та інститутів громадянського суспільства, пов'язаних зі створенням, перетворенням і споживанням інформації.

Розвиток інформаційно-комунікаційних технологій, обумовлене технологічним проривом і широким застосуванням інновацій, стало визначальним фактором повсюдного впровадження і використання інформаційно-комунікаційних технологій у всіх сферах життя людей, що представляє підвищені вимоги до розв'язання питань інформаційної безпеки.

Реальні темпи розвитку і поширення інформаційно-комунікаційних технологій у всіх сферах життєдіяльності суспільства є факторообразуючими елементами, які необхідно враховувати в процесі визначення ключових проблем в області інформаційної безпеки.

Наразі, згідно з висновками Академії електронного управління Естонії, яка щороку оприлюднює національні індекси кібербезпеки, Україна має 25-й національний індекс кібербезпеки; 78-й глобальний індекс кібербезпеки;

79-й індекс розвитку ІКТ та 64-й індекс мережевої готовності [86].

При цьому необхідно відзначити, що і в міждержавних відносинах наростає тенденція використання інформаційного тиску як дієвого механізму глобальної конкуренції. Використання різних засобів інформаційної пропаганди та інформаційної експансії стало невід'ємним інструментом вирішення різноманітних соціальних, економічних і політичних конфліктів. Певні країни світу, які мають можливість здійснення глобального моніторингу поширюваної інформації, використовують його результати для отримання односторонніх переваг в політичних, економічних, військових, екологічних та інших аспектах міждержавних відносин.

Екстремістські й терористичні організації та групи все активніше використовують можливості глобальних інформаційно-комунікаційних мереж для пропаганди своєї ідеології, вербування та навчання однодумців, підтримки зв'язку і фінансування різних терористичних груп [87]. Істотну проблему становить поширення інформаційної злочинності (кіберзлочинності), в тому числі діяльність організованих транснаціональних злочинних груп. Боротьба з інформаційною злочинністю вимагає від правоохоронних органів і спеціальних служб адекватного оперативного реагування шляхом проведення спільних скоординованих дій зі спеціальними службами та правоохоронними органами закордонних країн. Посилюється роль і вплив глобальних засобів масової інформації та комунікаційних механізмів на розвиток економічної, політичної та соціальної ситуації в різних країнах світу. Фундаментальні зміни, що відбулися в останні роки в країнах з різними економічними й політичними умовами, вказують на ключову роль в цих процесах нових технологій управління масами, в тому числі за допомогою використання інформаційно-комунікаційних технологій: сайтів, соціальних мереж і мобільних додатків [88].

Тому не випадково питання забезпечення інформаційної безпеки включені практично в усі розділи,

присвячені реалізації стратегічних національних пріоритетів, нову редакцію Стратегії національної безпеки України [89]. Окреслені в Стратегії положення отримали свій розвиток і в Стратегії воєнної безпеки України [90]. У цих документах не тільки дана оцінка сучасному стану інформаційної безпеки України, а й визначено перелік загроз, а також сукупність засобів, здатних забезпечити належний рівень захисту інформаційної безпеки держави.

Питання забезпечення інформаційної безпеки держави та юридичної відповідальності за порушення законодавства у сфері використання інформаційно-комунікаційних технологій, до сьогодні не отримали свого широкого висвітлення. Окремі аспекти кримінальної чи адміністративної відповідальності за правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку досліджувалися такими вченими, як Ю. М. Батурін, К. В. Басін, П. Д. Біленчук, А. Б. Венгеров, В. С.Венедіктов, В. В. Вертузаєв, М. В. Вєхов, О. Г. Волєводз, О. А. Гаврилов, В. В. Голіна, В. В. Голубєв, П. А. Дубров, О. В. Іваненко, А. М. Жодзишський, М. А. Зубань, Р. А. Калюжний, М. В. Карчевський, М. М. Коваленко, В. К. Колпаков, А. Т. Комзюк, О. В. Кохановська, В. В. Кузнєцов, Т. В. Міхайліна, М. І. Панов, В. В. Пиво-варов, М. С. Полєвой, В. А. Северин, С. І. Семилєтов, В. В. Сидоренко, К. С. Скоромніков, Ф. П. Тарасенко, Л. К. Терещенко, Т. І. Тарахонич, Б. С. Українцев, Н. Є. Філіпенко, В. С. Фролов, А. В. Черних, С. В. Ясечко та інші.

У своїх наукових пощуках[3] автори звертаються до різних площин юридичної відповідальності за порушення законодавства у сфері використання інформаційно-комунікаційних технологій, як в межах фундаментальних розробок, так й прикладних досліджень. Але багато

[3] Див. Список використаних джерел вітчизняних науковців та дисертаційних досліджень.

аспектів цієї складної проблеми ще потребують свого нагального вирішення.

На сучасному етапі до правових засобів забезпечення інформаційної безпеки України слід віднести необхідність підготовки й прийняття нових нормативних правових актів, а також уточнення наявних концептуальних та доктринальних документів, які б адекватно показували національні інтереси України, в тому числі у сфері використання інформаційно-комунікаційних технологій, і сприяли реалізації задач забезпечення інформаційної безпеки країни, виходячи з динаміки сучасних загроз.

Соціально-економічна обумовленість правової охорони інформаційної безпеки України пов'язана з розвитком в нашій країні нового типу суспільства, в якому наріжним каменем стоять інформація та інформаційно-комунікаційні технології. Економічний розвиток держави також залежить від цих технологій — сировинна економіка перетворюється в економіку цифрову. Духовні та соціальні потреби у людей переорієнтовані на швидкий пошук необхідних відомостей, своєчасне і повне отримання правдивої та якісної інформації, можливість оперативного обміну нею. Тобто формування інформаційного суспільства[4]. У загальнотеоретичному розумінні до

[4] Вперше в достатньо чіткому вигляді ідея інформаційного суспільства була сформульована наприкінці 60-х – початку 70-х рр. XX століття. Винахід самого терміну «інформаційне суспільство» приписується, зокрема, Ю. Хаяші, професору Токійського технологічного інституту. Контури інформаційного суспільства були окреслені в аналітичних звітах, поданих до японського уряду декількома організаціями: Агентством економічного планування, Інститутом розробки використання комп'ютерів, Радою зі структури промисловості. У згаданих звітах інформаційне суспільство визначалося як таке, де процес комп'ютеризації дасть людям доступ до надійних джерел інформації, позбавить їх від рутинної роботи, забезпечить високий рівень автоматизації виробництва. При цьому зміниться і саме виробництво : продукт його стане більш «інформаційно-містким», що означає збільшення частки інновацій, дизайну і маркетингу в його вартості; виробництво інформаційного

ресурсів інформаційного суспільства відносять: інформацію (information, database, BigData, англ.) інформаційні технології (Information Technology – IT, англ.) та знання (knowledge, англ.). Актуальність таких ресурсів була обумовлена розвитком легкої економіки, яка протягом останніх десятиліть була кардинально видозмінена інформатизаційними процесами та, звичайно, діджиталізацією (digitalization, англ.) соціально-економічних відносин.

Вплив інформаційних технологій на цивілізацію та процеси інформатизації на соціально-економічну та політичну сфери визначаються як суцільний позитив, одначе у світі щоденно виникають (у тому числі трансформуються) і втручаються у сталі системи життєдіяльності новітні девіантні прояви. Окремі з них є позитивними, сприяють розвитку суспільних відносин в цілому і виступають рушійними силами прогресу у техніці, економіці, культурі, навіть – змінюють застарілі схеми моралі та естетики. Однак, деякі з них, навпаки, породжують негативні зміни, руйнують усталені суспільні відносини заради настання негативних для суспільств явища [91].

З метою повного та всебічного розкриття питання юридичної відповідальності за порушення законодавства у сфері використання інформаційно-комунікаційних технологій, необхідним є теоретичне визначення та аналіз категорій, якими ми оперуємо надалі.

У положеннях нормативно-правових актів України та роботах українських та закордонних авторів ми знаходимо декілька термінів, що є майже тотожними: «інформаційні технології» та «інформаційно-комунікаційні технології».

У ст. 1 Закону України «Про Національну програму інформатизації» зазначається, що інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів

продукту, а не продукту матеріального, буде рушійною силою освіти й розвитку суспільства (Masuda Y. The Information Society as Postindustrial Society. Wash. : World Future Soc., 1983. P. 29).

обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [62]. За визначенням Г. Швачича й В.Толстого, інформаційна технологія — це технологія обробки даних (інформаційного ресурсу), яка складається з сукупності технологічних елементів: збирання, накопичення, пошуку, обробки, передачі даних користувачам на основі сучасних технічних засобів. Інформаційно-комунікаційні технології (ІКТ, від англ. Information and communications technology, ICT) — часто використовується як синонім до інформаційних технологій (ІТ), хоча ІКТ це загальніший термін, який підкреслює роль уніфікованих технологій та інтеграцію телекомунікацій (телефонних ліній та бездротових з'єднань), комп'ютерів, підпрограмного забезпечення, програмного забезпечення, накопичувальних та аудіовізуальних систем, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію. Іншими словами, ІКТ складається з ІТ, а також телекомунікацій, медіатрансляцій, усіх видів аудіо і відеообробки, передачі, мережевих функцій управління та моніторингу [92].

Інформаційно-комунікаційні технології (ІКТ) — це узагальнений термін, який охоплює всі технології для передачі інформації [93]. Саме поняття ІКТ є досить широким і розуміється науковцями у різних варіаціях. Проте найбільш поширеною сентенцією є, зокрема, те, що комунікативні технології є раціонально організованим комплексом дій в інформаційному просторі з цілеспрямованого виробництва і поширення інформації задля впливу на визначену аудиторію. Комунікативні технології — «запланований вплив на цільові групи» [94].

Інформаційно-комунікаційні технології — сукупність технологій, що забезпечують фіксацію інформації, її обробку та обмін інформацією (передачу, поширення, розкриття). Інформаційні технології — це методи і засоби отримання, перетворення, передачі, зберігання і використання інформації [95].

Таким чином, ІКТ можна визначити як комплекс дій, пов'язаних з обробкою, зберіганням та інтерпретацією інформації, внаслідок якого вона видозмінюється відповідно до потреб конкретного суб'єкта. У такому вигляді дані потрапляють у суспільний інформаційний потік, провокуючи певну (частіше за все передбачену та сплановану) реакцію аудиторії впливу. ІКТ – це сукупність методів, засобів і прийомів, що використовуються для добору, опрацювання, зберігання, поширення інформації в інтересах її користувачів [96].

Головні напрями правого регулювання безпечного функціонування і розвитку інформаційних технологій, на думку О. А. Степанова, обумовлюються необхідністю обмеження використання інформаційно-електронних систем при проведенні генетичних експериментів, встановлення порядку доступу та використання електронних банків даних конфіденційної інформації, відомостей, що стосуються розвитку біоелектронних, психокомп'ютерних систем, а також розробки процедури пред'явлення позовів при порушенні балансу суспільних та особистих інтересів, що передбачають вирішення конфліктних ситуацій, які виникають у зв'язку з функціонуванням і розвитком інформаційно-електронних систем [97]. Певно, така думка має враховуватися у питаннях визначення підстав криміналізації діяння, зокрема, при оцінці ризиків, яким має протидіяти держава шляхом вироблення ефективної кримінально-правової політики.

Поняття юридичної відповідальності належить до числа загальнотеоретичних і застосовуються в різних галузях права. Юридична відповідальність встановлює певні межі правового зв'язку індивіда в державі та через обов'язки визначає міру його соціальної свободи. Юридична відповідальність є одним із соціально-правових явищ, яке взаємно пов'язує державу та інститути громадянського суспільства. Вона є однією із гарантій забезпечення конституційного ладу, верховенства права, прав і свобод людини та громадянина, законності,

правопорядку; одним з елементів процесу правового регулювання суспільних відносин [98].

Юридична відповідальність є інститутом об'єктивного права й елементом змісту правовідносин. Юридична відповідальність як інститут об'єктивного права — це передбачені санкціями норм права, забезпечені можливістю застосування державного примусу, несприятливі наслідки особистого, майнового чи організаційного характеру, яких відповідний суб'єкт права зазнає за вчинене правопорушення і які процесуально закріплені в передбаченому законодавством порядку. Юридична відповідальність як елемент змісту правовідносин — це передбачені санкціями норм права вид і міра обов'язку суб'єкта права зазнати позбавлення особистого, майнового, організаційного характеру у правовідносинах, що виникають з факту правопорушення [98].

Основними відмітними ознаками юридичної відповідальності від інших правових форм державно-правового примусу є:

1) специфічність мети: а) метою попередження є захист публічного порядку та безпеки, недопущення (попередження) вчинення правопорушення; б) метою правовідновлювальної форми є відновлення незаконно порушених прав, примусове виконання невиконаних обов'язків та усунення протиправних станів; в) примусові заходи застосовуються із метою припинення протиправної поведінки, усунення шкідливих наслідків протиправної поведінки та створення необхідних умов для можливого у майбутньому притягнення винної особи до відповідальності; г) юридична відповідальність застосовується із метою перевиховання та покарання правопорушника, а також попередження, запобігання порушення вимог норм права, відновлення порушених прав і свобод;

2) особливі фактичні підстави застосування: а) фактичними підставами застосування попередження є об'єктивні умови, які прямо або безпосередньо пов'язані з життєдіяльністю людини, а також умови, які тісно пов'язані з юридично значущою поведінкою конкретного

суб'єкта права; б) припинення застосовується для припинення правопорушення лише у момент його вчинення; в) правовідновлювальна форма державно-правового примусу застосовується у випадку скоєння правопорушення, скоєння об'єктивно протиправного діяння (у визначених законом, договором випадках); г) юридична відповідальність як правило застосовується у випадку скоєння правопорушення;

3) особливі юридичні підстави застосування: а) зміст (обмежень та заборон) попередження міститься у диспозиції норм права; б) зміст (обмежень та заборон) примусових заходів міститься у диспозиції норми права; в) зміст правовідновлювальних заходів міститься у правовідновлювальних санкціях правових норм; г) зміст юридичної відповідальності міститься у охоронних (каральних) санкціях правових норм; 4) значення державного примусу для реалізації його правових форм: на відміну від юридичної відповідальності, у межах реалізації попередження, припинення та поновлення державний примус має допоміжне значення. Потенційна можливість застосування державного примусу забезпечує та гарантує добровільне виконання суб'єктами права обмежень і заборон зазначених форм державно-правового примусу.

Юридична відповідальність, як теоретична категорія, має певну неоднозначність до підходів її розгляду. Доктринального підходу до даної категорії перешкоджають відмінності у вихідних правових позиціях вчених, які знайшли відображення в численних роботах, присвячених проблемам юридичної відповідальності. Ще однією проблемою є відсутність сутності цього поняття у нормативно-правових актах України [91]. Наприклад, Конституція України не згадує відповідальність в будь-якому іншому розумінні ніж ретроспективна юридична відповідальність, а всі питання відношення людей до правових норм викладені у ст. 68 Конституції: «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» [99].

Аналізуючи фахові джерела можна стверджувати, що у правничих науках існує декілька основних підходів до розуміння природи, сутності та змісту юридичної відповідальності. Перший підхід – моністичне розуміння юридичної відповідальності. Прихильники цього підходу визнають лише ретроспективний (негативний) аспект юридичної відповідальності. Правомірна поведінка, на думку вчених, не входить до інституту юридичної відповідальності. У межах моністичного підходу до розуміння сутності юридичної відповідальності остання пов'язується з правопорушенням, протиправною поведінкою. У загальному вигляді вона передбачає застосування державного примусу, покарання за порушення встановлених юридичними нормами правил поведінки [98].

Другий підхід полягає у тому, що юридична відповідальність – закріплений у законодавстві й забезпечуваний державою юридичний обов'язок правопорушника зазнати примусового позбавлення певних цінностей, що належали йому [100].

Третя група науковців підходить до вивчення змісту юридичної відповідальності у якості дуалістичної категорії. Послідовники даного підходу розглядають юридичну відповідальність, з однієї сторони, як негативне явище, реакцію держави на протиправну поведінку суб'єкта права, а, з іншої, – як позитивне явище, правомірну поведінку, свідоме, добровільне виконання суб'єктами права обов'язків, що передбачені юридичними нормами [98]. Наприклад, І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін. вважають, що юридична відповідальність за інформаційні делікти – це регламентована інформаційно-деліктними правовими нормами реакція з боку уповноважених суб'єктів на діяння фізичних або юридичних осіб (колективних суб'єктів), що можуть виявлятися у недотриманні встановлених законом заборон, невиконанні обов'язків, порушенні правових зобов'язань, заподіюванні шкоди або завданні збитків та відображена у застосуванні до осіб, які вчинили такі діяння, засобів впливу, що тягнуть за собою обмеження особистого [91].

Бувши одним їх юридичних засобів, що нейтралізують наслідки неналежної поведінки суб'єкта, який порушує права та охоронювані законом інтереси інших осіб, юридична відповідальність виступає як реакція держави на вчинене правопорушення. Ця реакція має владний, примусовий характер, яке спонукає правопорушника зазнати несприятливі для нього наслідки у вигляді позбавлення певних матеріальних або нематеріальних благ. Виходячи з цього, змістом юридичної відповідальності виступатиме державний владний примус, що проявляє себе в різних формах. Однак, не всякий державний примус слід вважати відповідальністю. Наприклад, примусовий (судовий) вплив, що спонукає порушника до виконання своїх обов'язків, не буде мірою відповідальності, оскільки в такому випадку відсутній елемент додаткових несприятливих наслідків для порушника, тобто тих самих обмежень, які виходять за рамки примусово виконання обов'язків.

Юридична відповідальність за порушення законодавства у сфері використання інформаційно-комунікаційних технологій, має ряд специфічних особливостей. Ці особливості полягають в наступному: правопорушення, що підпадають під застосування тих чи інших заходів впливу на суб'єкта, який їх вчинив, завжди пов'язані з інформацією; правопорушення можна розглядати в якості інформаційно-правових, якщо їх зв'язок з інформацією є не тільки безпосередній, але й опосередкованої наявністю її матеріального носія. Як і будь-яка юридична відповідальність, відповідальність за правопорушення в інформаційній сфері реалізується в рамках правоохоронних правовідносин, суб'єктами яких виступають порушник інформаційно-правових норм і держава в особі уповноважених на застосування санкцій органів. Особа, яка притягається до відповідальності, має право на захист від незаконного залучення. У доктрині виділяють принципи юридичної відповідальності, які повною мірою поширюються і на відповідальність в інформаційній сфері. До їх числа відносяться: принцип законності, що означає, що відповідальність має місце

лише за правопорушення в інформаційній сфері, визнаються як такі законом; принцип обґрунтованості, що полягає у встановленні факту вчинення особою конкретного правопорушення; принцип справедливості, що означає, зокрема, що відповідальність повинна бути порівнянна тяжкості вчиненого правопорушення; принцип невідворотності, що передбачає неминучість настання для правопорушника несприятливих наслідків; принцип доцільності, що полягає в індивідуалізації заходів впливу на правопорушника і відповідність цих заходів цілям юридичної відповідальності. Державний примус здійснюється шляхом застосування до порушника різних заходів впливу. Від характеру цих заходів і характеру наслідків їх застосування залежить галузева приналежність юридичної відповідальності за порушення законодавства в інформаційній сфері. Якщо несприятливі наслідки носять майновий характер і виражаються у відшкодуванні збитків, сплату неустойки, відшкодування шкоди, має місце цивільно-правова відповідальність. Якщо несприятливі наслідки виражаються в санкціях, передбачених нормами адміністративного або кримінального законодавства, має місце адміністративно-правова або кримінальна відповідальність.

10.2. Кримінальна відповідальність за порушення у сфері використання інформаційно-комунікаційних технологій

Кримінальна відповідальність відноситься до одного з видів юридичної відповідальності та є, за своїм змістом, найбільш суворим з них. Кримінальна відповідальність — це передбачені законом обмеження прав і свобод особи, яка вчинила злочин, що полягають в її офіційному осуді, можливому покаранні та визнанні судимою.

Ознаки кримінальної відповідальності: різновид юридичної відповідальності (існує поряд з іншими її видами, зокрема адміністративною, цивільною тощо); застосовується до особи, яка вчинила кримінальне правопорушення; характеризується передбаченими законом про кримінальну відповідальність

несприятливими наслідками (засудження (осуд), покарання, судимість, випробування); полягає в обмеженні прав і свобод особи.

Слід зазначити, що інформаційні відносини стали об'єктом злочинного зазіхання й отримали в чинному Кримінальному кодексі України (далі – КК) певний кримінально-правовий захист. Підтвердженням цьому служать кримінально-правові норми, включені законодавцем до багатьох розділів Кодексу. Ми повністю погоджуємося із думкою науковців, що окремим, особливим критерієм, який докорінним чином змінює бачення кримінальним правом можливостей вчинення кримінальних правопорушень у сфері використання інформаційно-комунікаційних технологій є вчинення діянь у спосіб дистанційних комунікацій. По суті, дистанційною слід вважати комунікацію, котра здійснюється між віддаленими суб'єктами з використанням ІТ. Саме технології, завдяки яким людина має можливість миттєво здійснювати інформаційні обміни на відстані, є особливістю відносин в інформаційному суспільстві, прогресу XXI сторіччя, що, безумовно, сприяє дієвості глобалізаційних процесів [91]. Таким чином, якщо до кримінальних правопорушень, описаних у КК застосовувати належне сучасне бачення, а саме: можливості вчинення діяння у спосіб дистанційних комунікацій; вчинення діянь відносно віртуальних предметів; вчинення діянь з використанням віртуальних засобів впливу, до діянь, які посягають на ресурси, що належать до сфери інформаційних відносин; повною мірою можна віднести великі групи традиційних злочинів, відповідно, по розділах КК.

Наприклад, ст. 114 КК України «Шпигунство», під яким розуміється передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства [101]. Однією з актуальних прикмет сьогодення виступає таке злочинне явище як «кібершпигунство». У загальному вигляді під ним слід

розуміти незаконне збирання, викрадення, передачу або зберігання інформації в інформаційно-телекомунікаційних мережах, що належать іноземній державі, в разі, якщо вони не знаходяться у відкритому доступі. Не завжди кібершпигунство здійснюється щодо відомостей, що становлять державну таємницю. Так, наприклад, Національне управління контррозвідки представило конгресу США доповідь під назвою «Іноземні шпигуни крадуть американські економічні секрети в кіберпросторі» [102], в якому вказується, що Китай і Росія використовують кібершпигунство для розкрадання торгових і технологічних секретів США. Автори доповіді вважають, що таким чином зазначені країни розвивають власну економіку, в результаті чого для процвітання і безпеки США створюється значна загроза. У доповіді американських контррозвідників також повідомляється, що одні тільки китайські хакери зуміли протягом останніх двох років отримати максимальний доступ до комп'ютерних мережах численних енергетичних, нафтових і військово-промислових компаній США. Фахівці із кібербезпеки опублікували звіт по одній з найбільших операцій щодо кібершпигунства «Red October». Атака була спрямована на різні державні структури, дипломатичні організації та компанії в різних країнах світу. Red October здатний також знімати дані з мобільних пристроїв; збирати інформацію з мережевого обладнання; здійснювати збір файлів з USB-дисків; копіювати поштові бази даних з локального сховища поштової програми або з віддаленої поштового сервера, а також витягувати файли з локальних серверів в сеті. Таким чином, об'єктом кібершпигунства може бути будь-яка інша інформація з обмеженим доступом (відомості, що становлять банківську таємницю; персональні дані тощо). При цьому вже сам факт незаконного втручання, незалежно від настання наслідків, повинен бути кримінально караний.

І таких прикладів можна наводити безліч. Насамперед у КК традиційно передбачена відповідальність за вчинення діянь, які посягають на суть «відносини в інформаційній сфері», тобто ті, які вчинюються щодо

інформації, або щодо її обігу чи безпеки (у тому числі – щодо порушення доступу до неї). Такі діяння містяться майже в кожному розділі Особливої частини КК, і, при цьому, на рівні диспозицій такі діяння викладені таким чином, що, здебільшого інформація в них виступає або предметом, або знаряддям (засобом вчинення діяння). Перелік їх коливається від «Дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або захоплення державної влади» у формі закликів до таких дій, у т. ч. через ЗМІ (ч. 2, 3 ст. 109), або «Державної зради» (ст. 111) до «Незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала» (ст. 445). І в сучасному світі вони майже всі можуть вчинюватися з використанням дистанційних комунікацій, завдяки яким стають як корисливими, так і уразливими всі суспільні відносини, предмети яких були піддані діджиталізації [91]. На жаль, обсяг цієї роботи не дає змогу проаналізувати їх усі, тому ми більш докладно зупинимося на кримінальних правопорушеннях, в яких прямо вказано на відповідальність за порушення законодавства у сфері використання інформаційно-комунікаційних технологій.

Розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [101].

Але, перш ніж докладно розглянути кримінально-правову характеристику зазначених правопорушень, хочемо зупинитися на загальнотеоретичних поняттях, до яких відноситься категорія «об’єкт правопорушення».

До кримінальних правопорушень у сфері використання інформаційно-комунікаційних технологій слід відносити заборонені законом суспільно-небезпечні діяння, які посягають на суспільні відносини, що забезпечують безпеку процесів і методів пошуку, збору, зберігання, обробки, надання, поширення інформації за допомогою засобів електронно-обчислювальних машин (комп'ютерів), систем та інформаційно-телекомунікаційних мереж. Стосовно кримінального права, будь-який об’єкт

кримінального правопорушення є системою суспільних відносин, що охороняються законом.

Однак таке розуміння об'єкта кримінального правопорушення поділяється не всіма вченими. Наприклад, погляди вчених 19 сторіччя мали суттєві розбіжності. Перша група фахівців, трансформувавши ідеї німецького криміналіста А. Фейєрбаха, вважала розуміння об'єкта злочину як частини суб'єктивного права індивіда. Так, В. Д. Спасович злочином вважав посягання на чиєсь право, що охороняється державою за допомогою покарання [103]. Провівши аналіз цього висловлювання, можемо зробити декілька важливих висновків. На його думку, носіями (власниками або суб'єктами прав) може бути виключно людина (одна чи декілька), тому посягання може бути спрямоване тільки проти конкретної особи. Також, якщо держава не буде охороняти суб'єктивне право, то таке порушення виключається із категорії кримінально караних. Прихильниками цих поглядів можна вважати І. Я. Фойницького, Л. С. Белогріц-Котляревського та ін. Другу групу науковців об'єднували погляди стосовно того, що об'єкта злочину є певним еквівалентом «правового блага», в основі якого постулат про захист правом конкретного життєвого інтересу. Також були відомі підходи до розуміння об'єкта злочину як охоронюваних нормами права життєвих інтересів (Ф. Лист), як правового блага (Н. Вельцель), як цінностей, що є умовами здорового існування суспільства (К. Биндинг) тощо.

Одним із перших фахівців теорії кримінального права, який синтезував сучасний підхід щодо сутності категорії «об'єкт», був дореволюційний науковець М. С. Таганцев [104], який зазначав, що кримінально-караним відзначається діяння, яке посягає на юридичну норму в її реальному бутті … діяння, що посягає на такі охоронювані нормою закону інтереси життя, які в даній країні, в цей час, визнаються істотними й держава, зважаючи на недостатність інших заходів охорони, загрожує тим, хто посягає на них покаранням [105]. З наведеного визначення вбачається, що науковець об'єктом злочину бачив не тільки юридичну норму, але й

інтереси/блага, які вона охоплює. Критикуючи теорію розуміння об'єкта як суб'єктивного права, а також нормативну теорію, С. В. Познишев відзначав, що об'єктами злочинів є ті конкретні відносини, речі та стан осіб або речей, які охороняються законом під страхом покарання [106]. На початку 20 сторіччя класичне поняття об'єкта злочину, як сукупності суспільних відносин, у теорію кримінального права було введено низкою видатних науковців, зокрема А. А. Піонтковським, М. Й. Коржанським, М. І. Бажановим. Але, як справедливо зазначав В. Я. Тацій, не можна не відзначити, що однією з тенденцій сучасної теорії кримінального права є намагання дослідників відійти від розуміння об'єкта злочину як суспільних відносин, оскільки таке розуміння об'єкта злочину, на їх думку, засноване на абстрактних умоглядних ідеологічних постулатах, штучно запроваджених у дійсність [107].

У цьому зв'язку ми повністю погоджуємося із висновком В. Я. Тація, що сьогодні ще не вдалося створити досконалої теорії об'єкта злочину. Безумовно, чимало наявних наукових підходів до визначення об'єкта злочину мають право на існування. Щобільше, деякі з них виглядають достатньо переконливими під час дослідження конкретного складу злочину [107]. Проте водночас вони містять у собі і резерв для обґрунтованої критики. Зокрема, якщо розглядати більшість із названих теорій крізь призму структури суспільних відносин, то можна встановити, що вони переважно зводяться до якогось структурного елементу суспільних відносин – їх предмета, суб'єктів або ж соціального зв'язку, який становить зміст цих відносин. Так, теорія соціальних цінностей, попри такий її безспірний позитивний момент, як відповідність Конституції України (ст. 3), в якій найвищою соціальною цінністю визнаються людина, її життя й здоров'я, честь і гідність, недоторканність і безпека, не позбавлена недоліків. Зокрема, аксіологічний підхід до визначення об'єкта злочину не дає достатніх підстав для автоматичного та беззаперечного перенесення поняття «соціальні цінності» на ґрунт кримінального права. Те, що законодавець у ст. 1 КК України вказує на такі найвищі

цінності, як права і свободи людини та громадянина, аж ніяк не свідчить про те, що вони охороняються кримінальним правом поза межами суспільних відносин, адже відомо, що цінність життя та здоров'я людини, власності тощо забезпечується лише їх існуванням у суспільстві; поза межами нього будь-яке регулювання та охорона взагалі втрачають свій сенс. А тому юридична конструкція ст. 1 КК України є лише своєрідним законодавчим прийомом, який дозволяє підкреслити важливість охорони суспільних відносин, що забезпечують указані соціальні цінності. До того ж соціальні цінності, на наш погляд, є узагальнюючим поняттям, що охоплює різноманітні предмети суспільних відносин (блага, інтереси, суб'єктивні права тощо), які їх забезпечують. Це є доказом того, що теорія соціальних цінностей звужує поняття об'єкта злочину до такого елементу суспільних відносин, як їх предмет. Не можна не вказати й на те, що за такого підходу не зовсім ураховуються історичні традиції, специфіка кримінально-правової галузі та її окремих інститутів. Аналогічний висновок можна зробити й щодо позиції про визнання об'єктом злочину певного блага, поняття якого є ще вужчим, ніж соціальні цінності [107]. Слід погодитися з висловленою в літературі думкою про те, що категорією «благо» неможливо охопити всі реалії дійсності, які охороняються законом про кримінальну відповідальність. Якщо віднесення до категорії «благо» таких реалій дійсності, як життя, здоров'я, свобода, гідність, безпека людини, її майновий стан і соціальний статус, не викликає сумніву, то цього не можна сказати, наприклад, про діяльність пенітенціарної системи, що є вимушеним атрибутом державної влади, який навряд чи можна назвати благом для людини та людства. Фашистський та інші тоталітарні політичні режими підводяться в ранг блага його натхненниками й сприймаються як такі однією частиною населення країни, але не сприймаються як благо іншою частиною населення країни й усіма демократичними державами, а, навпаки, розглядаються як зло, що має бути знищене. Не можна скидати з рахунку й ті ситуації, коли законодавство про

кримінальну відповідальність продовжує охороняти ті категорії й умови дійсності, які давно вже не відповідають уявленням про благо, слугують лише гальмом у суспільному розвитку та потребують скорішої зміни та декриміналізації [108].

Ми дотримуємося розуміння об'єкта кримінального правопорушення як охоронюваних кримінальним законом суспільних відносин, погоджуючись з тим, що визнання суспільних відносин об'єктом злочину – це результат деякої абстракції. В основі будь-яких суспільних відносин, в тому числі й взятих під кримінально-правову охорону, лежать певні інтереси (особистості, суспільства або держави) чи правові блага, тобто ті ж інтереси, що охороняються законом.

Отже, об'єкт кримінальних правопорушень у сфері використання інформаційно-комунікаційних технологій являє собою відкриту динамічну систему суспільних відносин. Відкритість цієї системи обумовлена тим, що вона не може мати постійний, незмінний характер (хоча б тому, що із плином часу виникають нові види правопорушень, й такі діяння криміналізуються, або, навпаки, декриміналізуються). Як об'єкт кримінально-правової охорони інформаційна безпека являє собою відкриту динамічну систему суспільних відносин, що забезпечують реалізацію інтересів особистості, суспільства і держави в інформаційній сфері. Структура інформаційної безпеки, як об'єкта кримінально-правової охорони, не може бути визначена лінійно. Нелінійна класифікація структури інформаційної безпеки обумовлена складністю самої інформаційної сфери.

У Доктрині інформаційної безпеки України [109] зазначається, що національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави: захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації; захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної й релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України; всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до перевіреної та об'єктивної інформації; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток та захист національної інформаційної інфраструктури; збереження і примноження духовних, культурних і моральних цінностей Українського народу; забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України; вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування; зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності; розвиток медіа-культури суспільства та соціально відповідального медіа-середовища; формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів; створення з урахуванням норм міжнародного права системи та механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди; розвиток інформаційного суспільства, зокрема його технологічної інфраструктури; безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір; розвиток системи стратегічних комунікацій України; ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері; забезпечення розвитку

інформаційно-комунікаційних технологій та інформаційних ресурсів України; захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом; формування позитивного іміджу України у світі, донесення оперативної, правдивої і об'єктивної інформації про події в Україні до міжнародної спільноти; розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України [109]. Названі суспільні відносини, які були нами наведені, також входять до переліку відносин, що охороняються чинним кримінальним законодавством України. Тому структура інформаційної безпеки охоплює: суспільні відносини, що забезпечують реалізацію права на інформацію й на охорону інформації від незаконного втручання; суспільні відносини, що забезпечують безпеку інформаційних ресурсів; суспільні відносини, що забезпечують безпеку у сфері використання інформаційно-комунікаційних технологій.

Слід зазначити, що інформаційна безпека як об'єкт кримінально-правової охорони представляє певну складність. Це обумовлено тим, що інформаційні технології проникли в усі сфери життєдіяльності особистості, суспільства і держави. Інформаційна безпека, своєю чергою, активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України. Від рівня її захищеності залежить стан інших складових національної безпеки держави, що дозволяє говорити про інформаційний аспект політичної, економічної, екологічної та інших видів безпеки.

Що стосується теорії кримінального права, вищевикладене дозволяє висунути гіпотезу про те, що інформаційна безпека може виступати як *основним*, так і *додатковим* об'єктом кримінального правопорушення. Інформаційна безпека як додаткового об'єкта кримінального правопорушення присутня у значній кількості складів, відповідальність за які передбачена нормами Особливої частини Кримінального кодексу. Їх можна відносити до зазіхань на інформаційну безпеку з

деякою часткою умовності. Таким чином, представляється необхідним конкретизувати родовий об'єкт даної групи кримінальних правопорушень як суспільних відносин, що забезпечують інформаційну безпеку.

Родовим об'єктом правопорушень, передбачених у розділі XVI Кримінального кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», є частина інформаційних відносин, які можна визначити як інформаційні відносини, засобом забезпечення яких є електронно-обчислювальні машини, системи, комп'ютерні мережі та мережі електрозв'язку [101]. Інакше кажучи, кримінальні правопорушення, передбачені цим розділом, посягають на певну частину інформаційних відносин — інформаційні відносини, пов'язані із застосуванням спеціальних технічних засобів, які широко відомі та досить добре розповсюдженні у наш час [110].

З визначенням родового об'єкта злочинів у сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж і мереж електрозв'язку пов'язана проблема — проблема найменування злочинів, які посягають на цей об'єкт. Закон визначає ці діяння поняттям «кримінальні правопорушення у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку». У літературі ж все частіше використовується термін «комп'ютерні злочини». Видається, що достатньо поширене розуміння комп'ютерних правопорушень як таких, що вчиняються з використанням комп'ютерної техніки або відносно комп'ютерної інформації, є неправильним, таким, що не дозволяє відбити їх сутність, специфіку та відрізнити від інших злочинів, у яких комп'ютер є лише знаряддям, засобом або предметом. Аналізуючи це питання, слід перш за все розмежувати терміни комп'ютерні злочини та кримінальні правопорушення, пов'язані з комп'ютерною технікою.

У кримінальному законі наводяться чотири види таких спеціальних технічних засобів:

- автоматизовані електронно-обчислювальні машини (комп'ютери, АЕОМ), у т.ч. персональні – комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань [111]. Також окремі положення чинного українського законодавства відносять до цієї групи й екранні пристрої – електронні засоби для відтворення будь-якої графічної або алфавітно-цифрової інформації (на основі електронно-променевої трубки, рідкокристалічні, плазмові, проєкційні, органічні світлодіодні монітори та інші новітні розробки у сфері інформаційних технологій) [112];

- автоматизована система (в інформаційних технологіях) – система, що реалізує інформаційну технологію виконання встановлених функцій за допомогою персоналу і комплексу засобів автоматизації [113]. При узагальненні судової практики із названого виду кримінальних правопорушень, під автоматизованою системою також розуміється організаційно-технічна система, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей і персоналу, що здійснює цю діяльність. Зокрема, такими системами слід вважати сукупність ЕОМ, засобів зв'язку та програм, за допомогою яких ведеться документообіг, формуються, оновлюються та використовуються бази даних, накопичується та обробляється інформація. Оскільки обробка певних даних можлива і в результаті роботи одного комп'ютера, то автоматизована система – це й окремо взятий комп'ютер разом з його програмним забезпеченням [111].

- комп'ютерна мережа – сукупність територіально розосереджених систем опрацювання даних, засобів і (або) систем зв'язку та передавання даних, що забезпечує користувачам дистанційний доступ до її ресурсів і колективне використання цих ресурсів [113]. У законодавчих актах також використовується термін «мережа Інтернет (Інтернет)» – глобальна електронна комунікаційна мережа, що призначена для передачі даних

та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні Інтернет-протоколів, визначених міжнародними стандартами [21];

- телекомунікаційна мережа (мережа електрозв'язку) — комплекс технічних засобів телекомунікацій і споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого роду за допомогою радіо, проводових, оптичних чи інших електромагнітних систем між кінцевим обладнанням. У Законі України «Про електронні комунікації» під електронною комунікаційною мережею розуміється комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг. Своєю чергою електронна комунікація (телекомунікація) — передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій [21].

Залежно від цих засобів інформаційні відносини, які є родовим об'єктом досліджуваних злочинів, можуть бути поділені на чотири види:

1) інформаційні відносини, засобом забезпечення яких є комп'ютери;

2) інформаційні відносини, засобом забезпечення яких є комп'ютерні системи;

3) інформаційні відносини, засобом забезпечення яких є комп'ютерні мережі;

4) інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку.

Перший вид цих інформаційних відносин — це найпростіша форма застосування комп'ютерної техніки для роботи з інформацією. Суб'єкти таких відносин використовують комп'ютерну техніку для виконання порівняно нескладних операцій, таких як підготування документів, проведення інженерних розрахунків, організація та робота з базами даних. Зазначимо, що під

електронно-обчислювальною машиною розуміються не тільки комп'ютери в їх «класичному», можна сказати звичному, вигляді, тобто «системний блок — монітор — клавіатура — принтер», але й інше устаткування, яке містить процесор і може виконувати розрахунки без участі людини.

Використання комп'ютерних систем відноситься до більш складних інформаційних відносин. Автоматизовані системи використовуються для виконання широкого кола завдань: управління підприємством, технологічне підготування виробництва, контроль і випробування промислової продукції, управління службами життєзабезпечення підприємства і т. ін.

Третій вид інформаційних відносин, які утворюють досліджуваний родовий об'єкт, пов'язаний із використанням комп'ютерних мереж, що бувають двох видів: локальні, які об'єднують комп'ютери в межах однієї організації, і глобальні, які забезпечують зв'язок між різними організаціями, юридичними та фізичними особами. Найвідомішою і найпоширенішою глобальною комп'ютерною мережею є Інтернет, що застосовується в основному для таких видів роботи з інформацією: електронна пошта; передавання файлів; віддалений доступ — можливість підключатися до віддаленого комп'ютера й працювати з ним в інтерактивному режимі.

Інформаційні відносини, засобом забезпечення яких є мережі електрозв'язку, полягають у наданні й отриманні послуг електричного зв'язку, тобто у використанні мереж електрозв'язку для передачі або прийняття інформації. Стосовно до визначення змісту цих суспільних відносин певний інтерес становить питання їх відмежування від інформаційних відносин, засобом забезпечення яких є комп'ютерні мережі. Аналіз чинного законодавства у сфері телекомунікації дозволяє стверджувати, що наявність у законі про кримінальну відповідальність одночасно терміном «мережа електрозв'язку» іншого — «комп'ютерна мережа» — фактично приводить до того, що під мережею електрозв'язку треба розуміти всі телекомунікаційні мережі, крім комп'ютерних (мережі

міського, міжміського та міжнародного телефонного зв'язку, рухомого (мобільного) зв'язку, проводового радіомовлення, ефірного телерадіомовлення тощо). Таким чином, під інформаційними відносинами, засобом забезпечення яких виступають мережі електрозв'язку, слід розуміти суспільні відносини у сфері використання телекомунікаційних мереж, за винятком комп'ютерних мереж.

Таким чином, **родовий об'єкт** названих кримінальних правопорушень – інформаційна безпека, **безпосередній** – нормальне функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, комп'ютерної інформації та мереж електрозв'язку.

Предмет кримінальних правопорушень:

1) електронно-обчислювальна машина (комп'ютер);

2) автоматизовані системи (АС);

3) комп'ютерні мережі (мережа ЕОМ);

4) мережі електрозв'язку;

5) інформація, що передається мережами електрозв'язку (телекомунікаційними мережами) – будь-які відомості, подані у вигляді сигналів, знаків, звуків, зображень чи в інший спосіб (телефонні повідомлення, радіо- та телепередачі тощо), у тому числі та за допомогою комп'ютера, якщо вона передається через мережі електрозв'язку.

6) комп'ютерна інформація. Це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, явища, що існує в електронному вигляді й знаходиться в ЕОМ, АС чи в комп'ютерній мережі, а також зберігається на відповідних електронних носіях, до яких належать гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти та ін. Інформація носіїв може використовуватися, оброблятися чи змінюватися за допомогою ЕОМ (комп'ютерів) [114].

Думки щодо кола предметів злочинів, передбачених Розділом XVI КК України, мають багато розбіжностей. При цьому слід зауважити, що певна група фахівців взагалі не

виділяє комп'ютерну інформацію як предмет злочину, встановленого ст. 361 КК, яка прямо вказана в цій нормі як предмет, на перекручення або знищення якого спрямовані дії злочинця [115]. Ми повністю погоджуємося із думками науковців [116], які вважають, що невизнання комп'ютерної інформації у якості предмета злочину обумовлено «матеріалістичним» підходом класичної теорії кримінального права до визначення предмета злочину як певних матеріальних цінностей, які мають обов'язкову фізичну ознаку. Науковці, які вбачають цю категорію у якості предмета кримінальних правопорушень, передбачених статтями 361-363 КК, по-різному розглядають саму комп'ютерну інформацію. Перші розглядають її як матеріальний предмет об'єктивного світу і, таким чином, автоматично визнавали її предметом злочинів, встановлених статтями Розділу XVI КК України. Так, Д. С. Азаров підкреслює, що єдиним можливим предметом злочинів є комп'ютерна інформація, яку він відносить до «матеріальних утворень» [117], предметів матеріального світу. Погоджуючись з доктринальною концепцією такого визначення щодо необхідності визначення комп'ютерної інформації як предмета злочину взагалі, не можемо погодитися з постулатом науковця про те, що це є єдиний предмет названих кримінальних правопорушень. Друга група фахівців ототожнюють комп'ютерну інформацію з матеріальним носієм, на якому вона може бути закріплена. Наприклад, В. М. Карчевський зазначає, що фізична ознака комп'ютерної інформації, як предмета злочину, полягає в її носії, який зазвичай розуміється як предмет, річ, властивості якої використовуються для передавання, зберігання та опрацювання інформації [118]. Тобто, фізичною ознакою комп'ютерної інформації, на його думку, є наявність її носія, який і включається в систему суспільних відносин. Проте, ми вважаємо, що комп'ютерна інформація є цифровим відображенням фізичного світу та може існувати, певним чином, окремо від її носіїв. Разом з цим, комп'ютерну інформацію не можна ототожнювати з її носієм, оскільки, по-перше, вона може бути зафіксована на

різних типах носіїв і не завжди право власності на такий носій збігається з правом власності на саму комп'ютерну інформацію і, по-друге, комп'ютерна інформація може передаватися за допомогою каналів зв'язку, де і може бути вчинене суспільно небезпечне посягання на неї (наприклад, викрадення, знищення) [116]. Третя група дослідників визначає комп'ютерну інформацію як один з альтернативних предметів злочину [119]. Ми погоджуємося із цими міркуваннями, тому що комп'ютерна інформація прямо вказана в кримінальному законі як предмет, на який впливає особа при вчиненні аналізованих злочинів.

Також доречним буде наступне зауваження: якщо під матеріальним предметом розуміється будь-яке конкретне матеріальне явище, що сприймається органами чуття [120] (так би мовити, тілесний предмет матеріального світу) [121], то віртуальним предметом є предмет «умовний, фізично відсутній», але який може набути зовнішнього представлення «за допомогою спеціальних методів, наданих у розпорядження [122]. Тобто, під віртуальним предметом нами розуміється такий предмет, який не має зовнішнього представлення, але може набути такого за допомогою використання спеціальних засобів та способів. Таким чином, комп'ютерна інформація є предметом віртуальним, оскільки сама по собі вона не має зовнішнього представлення, але може набути його завдяки застосуванню щодо неї спеціальних засобів та способів — комп'ютерних систем, які надають їй форму, придатну для сприйняття та обробки [116].

У законодавстві закордонних країн вживаються такі терміни як, «цифрова інформація» (digital information) і «дані» (data). Своєю чергою, «дані» є більш широким поняттям, ніж «цифрова інформація». Український законодавець виділяє «дані» в окреме поняття (розглядаючи їх як інформацію, яка подана у формі, придатній для її оброблення електронними засобами) [67], представляється необхідним поняття «комп'ютерна інформація» замінити на поняття «електронна інформація». Термін «електронний» не новий для вітчизняного законодавства. У Законі України «Про

електронні документи та електронний документообіг» (ст. 5) наведено наступне визначення цієї категорії: електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [67]. 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. Виходячи із тексту Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи, електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, який містить обов'язкові реквізити документа, правовий статус якого засвідчено кваліфікованим електронним підписом автора та «електронна копія паперового документа» – документ в електронній формі, що містить візуальне подання паперового документа, отримане шляхом сканування (фотографування) паперового документа. Відповідність оригіналу та правовий статус електронної копії паперового документа засвідчуються кваліфікованим електронним підписом особи, що створила таку копію [123]. Законом України «Про електронні довірчі послуги» законодавчо закріплено поняття «електронного підпису» як електронних даних, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис [68].

Об'єктивна сторона цих кримінальних правопорушень може виражатися в активних діях (наприклад, при несанкціонованому втручанні в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, чи створення з метою використання, розповсюдження або збуту шкідливих програмних або технічних засобів, а також їх розповсюдження або збут) або в злочинній бездіяльності (наприклад, при порушенні правил експлуатації електронно-обчислювальних машин

(комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється.

Для об'єктивної сторони деяких злочинів потрібно не тільки вчинення суспільно небезпечного діяння (умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів), а й настання суспільно небезпечних наслідків – матеріальні склади злочинів: призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) тощо. В інших випадках розглядувані злочини сформульовані як склади злочинів з формальним складом (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут).

Суб'єктивна сторона цих кримінальних правопорушень передбачає, як правило, умисну вину. Можлива і необережність – при порушенні правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється. *Мотиви та цілі можуть бути різними* – помста, прагнення до заволодіння інформацією. Якщо ж викрадення інформації вчиняється з корисливих мотивів і містить ознаки шахрайства, вчинене слід кваліфікувати за сукупністю злочинів – за статтями 362 і 190 КК.

Кримінальні правопорушення, що аналізуються, містять спільні **кваліфікуючі ознаки**:

- вчинення комп'ютерного злочину повторно;

- вчинення комп'ютерного злочину за попередньою змовою групою осіб;

- вчинення комп'ютерного злочину, який заподіяв значну шкоду.

Оскільки у розділі XVI Особливої частини КК України не передбачено повторності однорідних кримінальних правопорушень, діяння слід вважати вчиненим повторно у випадках, коли особа два або більше

рази вчинила його та який було кваліфіковано за однією статтею даного розділу. При цьому вчинення декількох таких кримінальних правопорушень не охоплювалося єдиним умислом (злочин не був продовжуваним), особа не звільнялася від кримінальної відповідальності за тотожне кримінальне правопорушення, не закінчилися строки давності притягнення до кримінальної відповідальності за раніше вчинене або судимість не було погашено чи знято.

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів) буде вважатися вчиненим групою осіб за попередньою змовою за наявності відповідних об'єктивних і суб'єктивних ознак. Об'єктивна сторона його може бути такою:

- діяння вчиняється двома або більше виконавцями, кожен із яких виконує всі дії, що утворюють об'єктивну сторону складу (наприклад, декілька осіб здійснюють несанкціоноване втручання з окремих терміналів і знищують певну інформацію);

- кримінальне правопорушення вчиняється двома або більше співвиконавцями, кожен із яких виконує частину дій, що характеризують об'єктивну сторону (наприклад, одна особа вчиняє несанкціоноване втручання й перекручує комп'ютерну інформацію про користувачів комп'ютерної мережі та паролі їх доступу, а інша знищує комп'ютерну інформацію);

- кримінальне правопорушення вчиняється двома або більше особами, при цьому лише одна з них відіграє роль виконавця, а інші є підбурювачами, пособниками або організаторами (наприклад, одна особа забезпечує іншу необхідним устаткуванням, а остання вчиняє розповсюдження шкідливої комп'ютерної програми). При цьому кожен зі співвиконавців повинен мати всі ознаки суб'єкта, тобто бути фізичною, осудною особою та досягти віку кримінальної відповідальності (ст. 18 КК України). У випадку, коли особа не була поінформована про те, що вчиняє кримінальне правопорушення разом із малолітнім або неосудним, її дії слід кваліфікувати за правилами фактичної помилки як замах на вчинення кримінального правопорушення групою осіб за попередньою змовою.

До об'єктивних ознак вчинення кримінального правопорушення за попередньою змовою групою осіб відноситься також спільність, що характеризується взаємозумовленістю дій, загальним для всіх співучасників наслідком і наявністю причинового зв'язку між діями співучасників і кримінальним правопорушенням, якого вчинив виконавець. Певну специфіку має суб'єктивна сторона кримінального правопорушення в разі його вчинення за попередньою змовою групою осіб. Домовленість про спільне вчинення цього злочину може бути досягнута без особистого знайомства співвиконавців. У практиці правоохоронних органів мав місце випадок, коли за допомогою комп'ютерної мережі Інтернет рядом осіб було вчинено розкрадання, причому ці суб'єкти один одного особисто навіть не бачили, оскільки спілкувалися за допомогою електронної мережі, у якій кожен мав свій псевдонім.

Значною шкодою в статтях, що аналізуються, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян (примітка до ст. 361 КК). Зазвичай ця шкода полягає в заподіянні позитивних матеріальних збитків. У такому випадку її необхідно оцінювати, виходячи з витрат власника на придбання комп'ютерної інформації. Але стосовно значної шкоди як кваліфікуючої ознаки кримінального правопорушення слід зауважити, що іноді вона може виражатися і в упущеній вигоді. Це пояснюється тим, що на сучасному етапі будь-яка діяльність як необхідний елемент включає інформаційне забезпечення. Ефективність діяльності багато в чому залежить від кількості та якості вхідної інформації, тому перекручення або знищення інформації, що має порівняно невелику ціну, здатне заподіяти значних матеріальних збитків у вигляді упущеної вигоди. Саме тому видається правильним, крім втрати або зменшення обсягу інформації, якою володіє потерпілий, у розмір матеріальних збитків від комп'ютерного злочину включати також і упущену вигоду,

яка може полягати в укладанні невигідних договорів, падінні авторитету, невиконанні умов договорів тощо.

Крім матеріальної шкоди, суспільно небезпечні наслідки при вчиненні комп'ютерного злочину можуть виражатись і в нематеріальних видах шкоди, що зумовлено використанням ЕОМ, систем і комп'ютерних мереж для контролю над складними технологічними процесами, об'єктами та керування ними. Це така шкода, як порушення нормальної роботи підприємств, зупинення або порушення складних технологічних процесів, погіршення обороноздатності держави, підрив авторитету державних органів, підприємств, установ або організацій, створення загрози або заподіяння шкоди життю та здоров'ю громадян, порушення безпеки руху транспорту тощо.

Суб'єкт кримінального правопорушення – загальний, особа фізична, осудна, що досягла 16-річного віку. У деяких випадках суб'єкт *спеціальний* – особа, яка відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку або повинна забезпечувати порядок чи виконання правил захисту інформації, яка в них обробляється (ст. 363 КК).

Таким чином, кримінальними правопорушеннями проти безпеки інформаційно-телекомунікаційних технологій є заборонені кримінальним законом суспільно небезпечні діяння, що посягають на суспільні відносини, які забезпечують безпеку процесів і методів пошуку, збору, зберігання, обробки, надання, поширення інформації за допомогою засобів обчислювальної техніки та інформаційно-телекомунікаційних мереж.

10.3. Адміністративна відповідальність за порушення у сфері використання інформаційно-комунікаційних технологій

Кодекс України про адміністративні правопорушення (далі – КУпАП) є досить розгалуженим та складним нормативно-правовим актом, що регулює матеріальні, компетенційні та процесуальні відносини адміністративної відповідальності. Нажаль, багато в чому КУпАП зберіг спадкоємність й структуру свого радянського попередника,

адже його основою виступили «Основи законодавства Союзу РСР та союзних республік про адміністративні правопорушення». Кодекс України про адміністративні правопорушення, в його сучасному вигляді, недостатньо оснащений проти сучасного рівня розвитку інформаційних технологій, можливості віддаленого доступу до інформаційних ресурсів, формування електронних банків даних, автоматизованих інформаційних систем.

Підстави юридичної відповідальності, з точки зору логіки розвитку правового регулювання, є похідними від виду юридичної відповідальності. Положення ст. 9 Кодексу України про адміністративні правопорушення вказано, що адміністративним правопорушенням (проступком) визнається протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на громадський порядок, власність, права і свободи громадян, на встановлений порядок управління і за яку законом передбачено адміністративну відповідальність. Адміністративна відповідальність за правопорушення, передбачені цим Кодексом, настає, якщо ці порушення за своїм характером не тягнуть за собою відповідно до закону кримінальної відповідальності [124]. Враховуючи дане положення можна зробити висновок, що діяння набуває якості адміністративного саме тому, що за нього передбачена саме адміністративна, а не будь-яка інша відповідальність.

Особа, яка вчинила адміністративне правопорушення, підлягає відповідальності на підставі закону, що діяв під час і за місцем вчинення адміністративного правопорушення. Адміністративна відповідальність — це застосування до правопорушників загальнообов'язкових стягнень, що зумовлюють для цих осіб обтяжливі наслідки матеріального чи морального характеру.

Фактично нормативно-правове визначення такої категорії як «адміністративна відповідальність» в чинному законодавстві відсутнє. Усі дефініції адміністративної відповідальності, як правило, надаються у наукових виданнях та мають дослідницький характер.

Наприклад, юридична енциклопедія визначає, що це вид юридичної відповідальності, що полягає в застосуванні до особи, яка вчинила адміністративний проступок, певного адміністративного стягнення. Адміністративна відповідальність настає за порушення загальнообов'язкових правил у різних галузях державного управління навіть тоді, коли порушення не потягло за собою конкретних шкідливих наслідків [125].

Адміністративна відповідальність, на думку О. В. Кузьменко – це передбачене законодавством, примусове, з додержанням встановленої процедури, застосування правомочним суб'єктом до осіб, які вчинили адміністративні проступки заходів впливу, реалізація яких юридично визнана [126].

Аналізуючи думки науковців з цього приводу слід зазначити, що сучасна вітчизняна адміністративно-правова наука під адміністративною відповідальністю визнає примусове застосування правомочними органами чи особами до суб'єкта адміністративного правопорушення (проступку) передбачених законом адміністративних стягнень та інших заходів впливу, реалізація яких юридично зафіксована [127].

Така реалізація підтверджується юридичною фіксацією. Видами реалізації є: а) виконання суб'єктом стягнень; б) юридичне визнання доречності звільнення від їх виконання; в) юридичним визнанням неможливості фактичного їх виконання. З цього визначення випливає, що реальна адміністративна відповідальність настає за наявністю нормативних, фактичних і документальних підстав.

Даний вид юридичної відповідальності завжди носить публічний характер, оскільки адміністративне покарання є встановленої державою мірою відповідальності за вчинене правопорушення і застосовується з метою запобігання вчиненню нових правопорушень як самим правопорушником, так і іншими особами.

Виходячи зі змісту питань, що розглядаються, адміністративно-інформаційна правова відповідальність характерна тим, що вона реалізується в адміністративному

порядку, у процесі реалізації державним органом своїх виконавчо-розпорядчих повноважень. Переважна більшість органів адміністративної юрисдикції, наділених повноваженнями щодо розгляду справ про адміністративні правопорушення, за своїм правовим статусом є органами виконавчої влади і, крім того, наділеними контрольними повноваженнями у сфері інформаційних відносин, які є об'єктом відповідних деліктів. Тобто, притягнення до адміністративної відповідальності чиниться цими органами переважно у процесі здійснення державного управління, а точніше – при реалізації ними такої важливої функції державного управління як контроль. При цьому, з процесуальної точки зору, процедура притягнення до адміністративної відповідальності оформлена адміністративно-правовими нормами у вигляді адміністративного провадження з усіма притаманними йому ознаками. Такі ознаки адміністративної відповідальності досить легко виділяються у відповідних нормативно-правових актах, що дає можливість переконливо довести адміністративно-правову природу відповідальності передбаченої інформаційно-деліктним законодавством. Навіть у тих випадках, коли справи про адміністративні правопорушення в інформаційній сфері розглядаються судами, можна стверджувати про наявність того ж самого адміністративного порядку притягнення до відповідальності [128].

Тобто, ознаками адміністративної відповідальності є:

- притягнення до адміністративної відповідальності можливо тільки в результаті вчинення адміністративного проступку;

- адміністративна відповідальність полягає в застосуванні до винних адміністративних стягнень. У ст. 23 КУпАП «Мета адміністративного стягнення» зазначено, що адміністративне стягнення є міра відповідальності;

- мета адміністративної відповідальності полягає: а) у вихованні особи в дусі додержання законів, поваги до правил співжиття; б) запобіганні здійснення нових проступків;

- право притягнення до адміністративної відповідальності надано багатьом суб'єктам, серед яких – органи державної виконавчої влади, місцевого самоврядування, суди (ст. 213 КУпАП «Органи (посадові особи), уповноважені розглядати справи про адміністративні правопорушення»);

- акт про притягнення до адміністративної відповідальності може прийматися: а) індивідуально (судді та посадові особи відповідних органів); б) колегіально шляхом голосування (виконавчі комітети й адміністративні комісії);

- законодавством встановлений особливий порядок притягнення до адміністративної відповідальності (складання протоколу, збір і оцінка доказів, винесення постанови і т. ін.);

- норми, що регламентують адміністративну відповідальність, містяться у різних за своєю правовою природою актах: а) кодексах; б) законах; в) правилах. Правила можуть затверджуватися Кабінетом Міністрів, органами виконавчої влади, встановлюватися рішеннями місцевих рад і навіть корпоративними актами [128].

У сфері інформаційних відносин адміністративна відповідальність виконує ті ж самі функції, що і в інших сферах соціально-господарської системи держави, тобто здійснює їх захист притаманними їй засобами [129].

В. Я. Настюк та В. В. Білевцова характеризують адміністративне правопорушення у галузі зв'язку та інформатизації як протиправну, винну (умисну або необережну) дію чи бездіяльність конкретного суб'єкта, що вчиняє замах на встановлений інформаційний правопорядок і завдає шкоду інформаційній сфері або створює реальну загрозу такого спричинення, за яку законом встановлено адміністративну відповідальність [130].

Говорячи критеріями адміністративно-деліктного регулювання інформаційних відносин, до категорії адміністративних правопорушень в інформаційній сфері належать передбачені актами адміністративно-деліктного законодавства склади деліктів, предметом протиправного посягання яких виступають інформація, інформаційні

ресурси чи технології або інформаційна сфера в цілому, а також ті, об'єктом в яких виступають інформаційні права, свободи особи, правові режими інформації чи гарантований державою публічний інформаційний правопорядок [131].

Адміністративна відповідальність, так само як й інші види юридичної відповідальності, настає за наявністю нормативних, фактичних і документальних підстав:

- фактичні підстави це юридичні факти, пов'язані з проступком, зокрема, це факт вчинення проступку і факт виконання заходів відповідальності, крім того, до них відносяться факти затримання, огляду, подання звернень, визнання доказами фактичних даних тощо;

- юридичні (нормативні) підстави утворюють норми за якими діяння визнається адміністративним проступком (правопорушенням), визначаються заходи примусу за виконання складу проступку, суб'єкти відповідальності і юрисдикції, правила, за якими накладаються і виконуються стягнення, забезпечується законність, права учасників провадження тощо;

- процесуальні (документальні) підстави — це наявність процесуальних норм, які забезпечують притягнення винної особи до адміністративної відповідальності та документів, оформлених відповідно до встановлених вимог та за визначеною законодавством процедурою, в першу чергу, це протокол про адміністративне правопорушення і постанова по справі про адміністративне правопорушення, а також сюди відносяться акти, довідки, звернення, облікові документи тощо.

Як слушно зазначає О. А. Заярний, будучи явищем реальної дійсності, адміністративні інформаційні правопорушення характеризуються різними властивостями, які залежно від правових властивостей можуть мати юридичне значення або не мати його (наприклад, у разі розголошення державної, службової чи конфіденційної інформації — розмір носія такої інформації, місце розголошення, правовий статус суб'єкта протиправної поведінки). Характерною особливістю

адміністративних інформаційних правопорушень є те, що, як різновиду інформаційних деліктів, їм властиві не лише загальні, але й спеціальні (родові ознаки), що відображають специфіку цієї категорії соціально шкідливих діянь в інформаційній сфері [132, 133].

Кодекс України про адміністративні правопорушення містить понад 40 статей, у назві яких застосовано термін «інформація», або вони містять диспозицію правопорушень у сфері використання інформаційно-комунікаційних технологій. Вони розташовані у 6 главах [131]. Проведений аналіз складів адміністративних правопорушень у сфері інформаційної безпеки та використання інформаційно-комунікаційних технологій, які містяться в КУпАП, дозволяє розподілити їх на три групи, а саме: а) забезпечення доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; б) забезпечення обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб, або національній безпеці; в) забезпечення безпеки у сфері медіа-інформації.

Узагальнення змісту нормативних ознак адміністративних правопорушень дає підстави нам розглядати це поняття в межах інформаційної сфери як протиправне, соціально шкідливе, винне діяння (дію чи бездіяльність), вчинене суб'єктом публічної адміністрації, його посадовою особою, іншим деліктоздатним суб'єктом публічно-правових інформаційних відносин, яке порушує інформаційні права особи, суспільний інформаційний правопорядок, встановлений актами законодавства України правовий режим інформації, інформаційних ресурсів та технологій, посягає на об'єкти права власності в інформаційній сфері чи перешкоджає правомірній інформаційній діяльності, чим створює загрозу для національної інформаційної безпеки, і за яке законом встановлено адміністративну відповідальність. Наведене визначення за своїм змістом охоплює низку властивостей, які дозволяють виокремити адміністративні інформаційні

правопорушення в самостійний вид деліктів, що увібрали в себе властивості адміністративних та інформаційних правопорушень, відмежувати їх від інших категорій протиправних діянь, що вчиняються в інформаційній сфері.

Серед властивостей адміністративних інформаційних правопорушень, що створюють основу для виділення цих деліктів в окремий вид протиправних діянь учасників інформаційних відносин, можна виділити такі:

1) адміністративні інформаційні правопорушення є соціально шкідливими деліктами, які виражаються у порушенні інформаційних прав особи, суспільного інформаційного правопорядку, встановленого актами законодавства України правового режиму інформації, інформаційних ресурсів та технологій, посяганні на об'єкти права власності в інформаційній сфері чи створенні перешкод правомірній інформаційній діяльності, що не мають ознак злочину.

2) адміністративні інформаційні правопорушення мають міжгалузеву сутність, тобто не лише посягають на охоронювані законом публічні інтереси, інформаційні права особи, правові режими інформації, встановлені законом правила інформаційної діяльності, але й мають місце у сфері фінансів, державної служби, де інформація виступає спеціальним предметом правового регулювання.

3) бувши правовим та соціальним антиподом правомірної поведінки учасників інформаційних відносин, адміністративне інформаційне правопорушення виступає безпосередньою підставою адміністративної відповідальності, що має виключно нормативний характер.

4) адміністративне інформаційне правопорушення є відхиленням від заданих в інформаційній сфері нормативних координат діяльності публічної адміністрації, а у випадках, прямо передбачених законом, — фізичних та юридичних осіб приватного права, у зв'язку з чим така поведінка визнається протиправною та забороняється законом.

5) адміністративні правопорушення, які посягають на встановлені правові режими інформації, інформаційних

ресурсів чи технологій, вчиняються в особливій сфері правового регулювання – інформаційній сфері – з використанням засобів та знарядь, придатних для протиправного впливу на предмети правової охорони в інформаційному просторі України.

6) адміністративне інформаційне правопорушення виступає різновидом соціальних конфліктів, зумовлених невиконанням чи неналежним виконанням суб'єктами публічної адміністрації, їх посадовими особами, іншими особами, які виконують делеговані повноваження, сервісно-регуляторних функцій держави чи порушенням процедур надання публічних інформаційно-комунікаційних послуг.

7) адміністративні інформаційні правопорушення, виступаючи об'єктивним вираженням причин, умов, що сприяють розвитку адміністративної деліктності, становлять пряму загрозу для регіональної, національної, міжнародної інформаційної безпеки [131].

8) предметом посягання в адміністративних правопорушеннях, що вчиняються в інформаційній сфері, завжди є інформація, інформаційні ресурси, ІКТ, що перебувають під правовою охороною держави, інших володільців та розпорядників інформації. Наведені ознаки у своїй сукупності зумовлюють міжгалузеву (комплексну) сутність адміністративних інформаційних правопорушень [131].

Підбиваючи підсумок викладеному можемо констатувати, що нормативно-правове забезпечення адміністративної відповідальності у сфері забезпечення інформаційної безпеки та використання інформаційно-комунікаційних технологій проявляється у значній застарілості норм КУпАП і, як наслідок, недостатньому охопленні адміністративно-правовими нормами усієї сукупності суспільних відносин в інформаційній сфері.

Запитання для самоконтролю і самостійного опрацювання:

1. В чому полягає ціль юридичної відповідальності?
2. Які види юридичної відповідальності передбачені за порушення у сфері інформаційних технологій?

3. За якими критеріями розрізняється адміністративна та кримінальна відповідальність?

4. Що є характерною особливістю адміністративних інформаційних правопорушень?

5. Що є ознаками адміністративної відповідальності?

6. Що є національними інтересами України в інформаційній сфері?

7. Що може бути предметом кримінального правопорушення?

Рекомендована література:

1. Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями : Наказ Міністерства соціальної політики України від 14.02.2018 № 207. URL: https://zakon.rada.gov.ua/laws/show/z0508-18#Text

2. Кібершпигуни з Китаю та Росії атакують компанії США : доповідь. https://news.obozrevatel.com/ukr/abroad/60549-kibershpiguni-z-kitayu-ta-rosii-atakuyut-kompanii-ssha-dopovid.htm

3. Кочубей Л. Особливості сучасних інформаційно-комунікативних технологій в Україні. *Наукові записки ІПіЕНД ім. І.Ф. Кураса НАН України*. Випуск 3(89). — С. 44-70.

4. Настюк В. Я., Білєвцева В. В. Загальноправова характеристика адміністративної відповідальності за інформаційні правопорушення. *Інформація і право*. 2013. № 1. — С. 151–157.

5. Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника. М. І. Хавронюка. К., 2001.

6. Офіційний сайт Академії електронного управління Естонії. URL: https://ncsi.ega.ee/country/ua/

7. Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи: Рішення Вищої ради правосуддя від 17 серпня 2021 року № 1845/0/15-21.

РОЗДІЛ 11.

ПРАКТИЧНІ ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

До розділу 1: Поняття ІТ-права.

Завдання 1. Надайте характеристику американській та європейській моделям інформаційного суспільства. Проаналізуйте положення Окінавської хартії глобального інформаційного суспільства. Порівняйте з моделлю інформаційного суспільства в Україні. Проаналізуйте положення Закону України «Про Основні засади розвитку інформаційного суспільства України на 2007–2015 роки».

Завдання 2. Надайте визначення поняття «цифрова економіка» відповідно до Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки, схваленої розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Що таке «цифровізація»? Які принципи цифровізації визначені Концепцією? Проаналізуйте напрями цифрового розвитку відповідно до цього акта.

Завдання 3. Ознайомтеся із Декларацією принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» 2003 року. Що є необхідними умовами існування інформаційного суспільства?

Завдання 4. Проаналізуйте особливості ІТ права як галузі законодавства. Порівняйте ІТ право з цивільним правом і інформаційним правом.

До розділу 2: Правове регулювання мережі Інтернет

Завдання 1. **Ознайомтеся з висновками неурядової організації Freedom on the Net:** «Свобода в мережі 2021

Глобальне прагнення до контролю над великими технологіями», «Свобода в мережі 2019: криза соціальних мереж», «Свобода в мережі 2018: зростання цифрового авторитаризму». Які висновки щодо регулювання мережі Інтернет і соціальних мереж можна зробити?

Завдання 2. **Ознайомтеся з документом** «Поради і Рекомендації представника ОБСЄ з питань свободи ЗМІ, прийняті на Амстердамській конференції з питань свободи масової інформації в Інтернеті (2004)» Дайте відповіді на питання:

- З чого складається свобода Інтернет?
- Як висвітлюється питання «мови ненависті»?

До розділу 3: Доменні імена

Тестові завдання.

1. Визначення терміну «доменне ім'я» міститься в:

a) Законі України «Про телекомунікації»

b) Законі України «Про охорону прав на знаки для товарів і послуг»

c) Цивільному кодексі України

d) Закон України «Про інформацію»

e) Постанові Кабінету Міністрів України «Про затвердження Порядку підключення до глобальних мереж передачі даних»

2. В доменному імені khai.edu.ua загальним верхнім доменом є:

a) .edu

b) .ua

c) ._

d) khai

3. Зареєструвати домен можна на термін:

a) від 1 до 10 років

b) від 1 до 5 років

c) від 1 року

d) не більш ніж 5 років

4. Вирішення конфліктів, пов'язаних з недобросовісним використанням доменних імен в Україні провадяться в:

a) в національних судах
b) Антимонопольним Комітетом України
c) Процедура UDRP
d) «Український мережний інформаційний центр»

5. Захоплення доменних імен в глобальній електронній мережі отримало назву:
a) копірайт
b) кіберсквоттинг
c) ліцензування

6. Правила реєстрації доменних імен першого рівня встановлює організація:
a) Інтернет-корпорацією з призначення адрес та імен (ICANN)
b) ТОВ «Хостмастер»
c) «Український мережний інформаційний центр»

7. Реєстрація популярної Інтернет-адреси, що звичайно включає назви компаній або товарних знаків з метою продажу її законному власникові, має назву:
a) кіберсквоттинг
b) домейнінг
c) тайпсквоттинг

8. Чи є доменне ім'я об'єктом права інтелектуальної власності?
a) так
b) ні
c) в деяких випадках, так

9. Оберіть Загальні домени:
a) .com
b) .org
c) .edu
d) .UK
e) .UA

10. Чи можлива реєстрація доменів на кирилиці (російськими або українськими літерами)?
a) так
b) ні

11. Кореневі або нульові домени в імені *khai.edu.ua.* це:
a) khai.edu.ua.
b) khai.edu.ua.

c) khai.edu.ua.
d) khai.edu.ua.

11. В якому домені Доменні імена реєструються на підставі свідоцтва на знак для товарів і послуг?

a) ua
b) com
c) net

12. У доменному імені *khai.edu.ua.* національним доменом верхнього рівня є:

a) khai.edu.ua._
b) khai.edu.ua.
c) khai.edu.ua.
d) khai.edu.ua.

До розділу 4: Охорона прав інтелектуальної власності в цифровому середовищі.

Завдання 1. Проаналізуйте основні Інтернет-договори ВОІВ і Директиви ЄС у сфері інтелектуальної власності щодо здійснення та захисту прав інтелектуальної власності в мережі Інтернет.

Як в міжнародних нормативно-правових актах вирішується питання захисту прав інтелектуальної власності, що порушені в мережі Інтернет?

Завдання 2. Проаналізуйте Інтернет-сайт і комп'ютерну гру як об'єкти інтелектуального права, що є результатом творчої праці. Визначте, які об'єкти інтелектуального права можуть використовуватися при створенні та використанні веб-сайту і комп'ютерних ігор.

Завдання 3. Проаналізуйте будь-яку сторінку на платформі Youtube. З яких об'єктів інтелектуальної власності складається контент сторінки?

До розділу 5: Договірні відносини в цифровому середовищі

Тестові завдання

1. Оберіть правильну відповідь, в якій зазначено вид вільних публічних ліцензій:

a) Public License

b) General License
c) Ordinary License
d) Practical License
e) GNU Public License

2. Оберіть правильну відповідь, в якій зазначено вид вільних публічних ліцензій:

a) Public License
b) General License
c) Ordinary License
d) Practical License
e) Creative Commons

3.Оберіть правильну відповідь, в якій зазначено вид договору щодо розпорядження майновими правами інтелектуальної власності в цифровому середовищі:

a) корпоративний договір
b) договір про надання послуг
c) договір позики
d) договір оренди
e) договір про розробку дизайну веб-сайту на замовлення

4. Оберіть правильну відповідь, в якій зазначено вид договору щодо розпорядження майновими правами інтелектуальної власності в цифровому середовищі:

a) корпоративний договір
b) договір про надання послуг
c) договір позики
d) договір оренди
e) ліцензійний договір

5. Оберіть правильну відповідь, в якій зазначено вид договору щодо розпорядження майновими правами інтелектуальної власності в цифровому середовищі:

a) корпоративний договір
b) договір про надання послуг
c) договір позики
d) договір оренди
e) договір про передання виключних майнових прав інтелектуальної власності на веб-сайт

6. Оберіть правильну відповідь, в якій зазначено види договорів щодо розпорядження майновими правами

інтелектуальної власності в цифровому середовищі за їх закріпленістю (урегульованістю) в законодавстві:

a) зовнішні та внутрішні
b) загальні та одиничні
c) прості та змішані
d) строкові та безстрокові
e) пойменовані та не пойменований

7. Оберіть правильну відповідь, в якій зазначено види договорів щодо розпорядження майновими правами інтелектуальної власності в цифровому середовищі залежно від встановлення в договорі його строку:

a) зовнішні та внутрішні
b) загальні та одиничні
c) прості та змішані
d) пойменований та не пойменований
e) строкові та безстрокові

Завдання 2. **Ситуаційне завдання**:

Гр. Зубик І. Л. розробив комп'ютерну програму «Логіст-офіс», яка виявилась зручною для організації роботи магазинів гуртової торгівлі. Він уклав ліцензійні договори щодо використання даної програми з мережею гуртової торгівлі «Алколайф» (без зазначення строку). Згодом до нього звернулись представники ПП «Програміст», які прагнули доопрацювати програму та почати її серійний продаж. У результаті переговорів між гр. Зубиком та ПП «Програміст» було укладено договір «Про передання комплексу виключних майнових прав на комп'ютерну програму «Логіст-офіс». Після укладення договору ПП «Програміст» вирішило розірвати ліцензійний договір з «Алколайфом», на що представник мережі зауважив, що: 1) умови ліцензійного договору МГТ «Алколайф» не порушувались, отже підстав для розірвання договору немає; 2) укладення договору про передання виключних прав інтелектуальної власності не впливає на ліцензійні договори, які були укладені раніше, а це означає що право розірвати договір має лише Зубик І. Л., який й надалі є ліцензіаром. Проаналізуйте ситуацію та дайте їй правову оцінку

Тестові завдання

1. Інформаційно-комунікаційна технологія (ІКТ) – це:

а) сукупність методів, комунікацій, засобів, об'єднаних у технологічний ланцюг, що забезпечує збирання, зберігання, оброблення та передавання інформації з метою підвищення ефективності діяльності людей;

б) цілеспрямована сукупність методів, процесів, комунікацій, засобів та програмно-технічних засобів, об'єднаних у технологічний ланцюг, що забезпечує збирання, зберігання, оброблення та передачу інформації з метою підвищення ефективності діяльності людей;

в) сукупність інформаційних ресурсів економічної системи і технологій їх оброблення, зберігання та передавання інформаційних систем і телекомунікаційних засобів, які функціонують на основі єдиних принципів та загальних правил;

г) сукупність інформаційних ресурсів економічної системи і технологій їх оброблення, зберігання та передавання інформаційних систем і телекомунікаційних мереж, які функціонують з метою підвищення ефективності діяльності людей.

2. Інформаційно-економічний простір – це:

а) сукупність інформаційних ресурсів економічної системи і технологій їх оброблення, зберігання та передавання інформації разом з телекомунікаційними засобами;

б) інформаційні технології оброблення, зберігання та передавання інформації разом з телекомунікаційними засобами;

в) простір виробництва та надання інформаційних послуг їх обміну, де основним ресурсом є інформація;

г) методи, комунікації, мережі, об'єднані у технологічний ланцюг, що забезпечують збирання, зберігання, оброблення та передавання інформації з метою підвищення ефективності діяльності людей.

3. Інформаційні ресурси – це:

а) сукупність інформаційних ресурсів економічної системи і технологій їх оброблення, зберігання та передавання інформаційних систем і телекомунікаційних ятерів, які функціонують на основі єдиних принципів та загальних правив;

б) сукупність методів, комунікацій, засобів, об'єднаних у технологічний ланцюг, що забезпечує збирання, зберігання, оброблення та передавання інформації з метою підвищення ефективності діяльності людей;

в) інформація, що має цінність у певній предметній області та може бути використана людиною в економічній діяльності для досягнення певної мети;

г) економічна інформація, яка може бути використана людиною в будь-якій діяльності для досягнення певної мети.

4. Інформаційна економіка – це:

а) електронний бізнес, який здійснюється за допомогою ІКТ з метою отримання прибутків;

б) виробнича діяльність у сфері інформаційних послуг їх виробництва та обміну;

в) електронна економічна діяльність, яка здійснюється за допомогою ІКТ для поліпшення виробничих процесів;

г) електронна економічна діяльність, де переважає господарська діяльність у сфері інформаційних послуг їх виробництва та обміну, де основними ресурсами є інформація та знання.

5. Електронний бізнес – це:

а) електронна економічна діяльність, яка здійснюється за допомогою ІКТ з метою отримання прибутків;

б) надання фінансовими інститутами фінансових послуг своїм клієнтам щодо ефективного оперування коштами на фінансових ринках за допомогою ІКТ;

в) економічна діяльність на електронному ринку для всіх суб'єктів цього ринку;

г) підприємницька діяльність на електронному ринку.

6. Електронна комерція — це:

а) електронна економічна діяльність, що забезпечує повний замкнутий цикл бізнес-процесів, який включає замовлення товарів чи послуг, проведення платежів, доставляння товарів чи послуг шляхом ІКТ і забезпечує передачу має рацію користування або власності юридичних чи фізичних осіб іншим персонам;

б) сукупність інформаційних ресурсів економічної системи і технологій їх оброблення, зберігання та передавання інформаційних систем і телекомунікаційних засобів, які функціонують на основі єдиних принципів та загальних правил;

в) технології здійснення комерційних операцій в мережі Інтернет;

г) здійснення комерційних угод за допомогою ІКТ.

7. Інтернет-трейдинг — це:

а) фінансова посередницька діяльність, яка здійснюється на електронному ринку;

б) надання фінансовими інститутами послуг для ефективного використання фінансових інструментів на фінансових ринках за допомогою ІКТ;

в) надання інформаційних послуг на електронному ринку;

г) посередницька діяльність, яка здійснюється на фондових та грошових ринках.

8. Web-сайт, який забезпечує рекламу інформації, вибір товарів чи послуг, приймання замовлень, проведення взаєморозрахунків, контроль виконання замовлень та їх доставляння, — це:

а) електронний торговельний майданчик;

б) портал підприємства;

в) електронний магазин;

г) портал.

9. CRM-система — це:

а) система управління закупівлями;

б) система управління ланцюжком постачальників;

в) система управління продажем;

г) система супроводження споживачів;

10. Типовими рішеннями систем управління закупівлями є:

а) система закупівель інтегрована з ERP-систему або спеціалізована система управління закупівлями;

б) портал;

в) Інтернет-вітрина;

г) галузевий електронний каталог.

11. Система управління продажем – це:

а) електронний торговельний майданчик;

б) електронний магазин;

в) фронт-офіс і бек-офіс компанії з відповідними підсистемами;

г) галузевий електронний каталог.

До розділу 7: Електронний документообіг. Цифровий підпис

Завдання 1. **Надайте розгорнуту відповідь на питання:** Що таке електронний підпис і кваліфікований електронний підпис, яка різниця між ними?

Тестові завдання

1. За Законом електронним документом вважається:

а) інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

b) відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

c) інформація документаційного типу, що має електронну форму і призначена для зчитування, обробки та передачі за допомогою інформаційних і комп'ютерних систем.

2. Чи можна передати право підписання документів ключем ЕЦП від власника до іншої особи?

а) так

b) ні

3. Чи можна передати право підписання документів ключем ЕЦП від власника до іншої особи?

а) так

b) ні

4. Для ідентифікації повідомлення і перевірки його аутентифікації використовується ключ ЕЦП:

a) відкритий

b) закритий

5. Чи може підприємство використовувати електронну печатку якщо у нього немає традиційної печатки?

a) так

b) ні

c) в залежності від виду підприємства

6. Ознаки електронного документа:

a) є програмно-технічно залежним продуктом

b) має широкий спектр інформаційного відображення: текстові, графічні, електронні таблиці, бази даних, мультимедійні

c) документ може зберігаються у декількох різних файлах

d) зберігає юридичну силу при роздрукуванні на папері

e) має більш тривалий термін зберігання ніж паперовий документ

7. Використання кваліфікованих електронних підписів та печаток забезпечує:

a) високий рівень довіри до схем електронної ідентифікації

b) середній рівень довіри до схем електронної ідентифікації

c) низький рівень довіри до схем електронної ідентифікації

8. Використання удосконалених електронних підписів та печаток забезпечує:

a) середній рівень довіри до схем електронної ідентифікації

b) низький рівень довіри до схем електронної ідентифікації

c) високий рівень довіри до схем електронної ідентифікації

9. Чи повинен кваліфікований надавач електронних довірчих послуг забезпечувати свою діяльність внесенням у банк грошових коштів або страхуванням ризиків цивільно-правової відповідальності? Якщо так, в якому розмірі має бути внесок?

a) ні, не потрібно робити внесок. Діяльність в цій сфері не має обмежень щодо фінансового забезпечення.

b) так, не менш 1000 мінімальних розмірів заробітної плати.

c) так потрібно, але розмір внеску законодавством не визначається

d) потрібно якщо користувач вимагає такого забезпечення.

10. Електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу, це –

a) електронна позначка часу

b) момент укладання документа

c) електронна послуга

d) фіксація чинності документа

11. Які встановлено вимоги до обов'язкових реквізитів електронних документів?

a) має реквізити, аналогічні документу з паперовим носієм інформації

b) має реквізити, аналогічні документу з паперовим носієм інформації, з деякими особливостями.

c) вимоги до форм і видів реквізитів електронного документа абсолютно відрізняються від вимог до паперових документів.

12. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, який з них буде вважатися оригіналом і мати більшу юридичну силу?

a) електронний документ

b) паперовий документ

c) паперовий, якщо він має "живий" підпис і печатку

d) кожен з документів є оригіналом і має однакову юридичну силу.

13. Що є моментом завершення створення електронного документа?

a) момент накладанням електронного підпису

b) момент збереження його останньої версії на технічному пристрої

c) дата і час відправлення електронного документа адресату

14. Електронний документ не може бути застосовано як оригінал:

a) свідоцтва про право на спадщину;

b) без електронної позначки часу

c) без електронного підпису

d) без накладеної електронної печатки

e) без паперового примірника.

15. Обов'язковими реквізитами електронного документа є:

a) електронний підпис автора

b) електронна позначка часу

c) візуальна форма відображення

d) печатка та підпис власника або уповноваженої особи

16. При співвідношенні документів на електронному та паперовому носії пріоритет має:

a) електронний документ

b) паперовий документ

c) мають однакову силу в разі своєї ідентичності.

17. Який ключ ЕЦП застосовується для підписання електронних документів:

a) закритий

b) відкритий.

18. Чи допускається використання несертифікованих засобів ЕЦП:

a) ні

b) так.

До розділів 8-9: Електронні гроші. Правовий режим віртуальної валюти (криптовалюти)

Тестові завдання

1. Обліковий запис емітента/користувача, що згенерований/створений в програмному забезпеченні емітента для обліку, зберігання та здійснення з електронними грошима операцій, це -

a) електронний гаманець
b) електронний кабінет
c) картковий рахунок
d) усі відповіді вірні

2. Криптовалюти відносяться до:

a) національних валют
b) електронних грошей
c) цифрових грошей
d) фіатних грошей
e) немає правильної відповіді

3. Особа, яка здійснює випуск електронних грошей за межами України для їх використання в міжнародній системі Інтернет-розрахунків, відомості щодо якої внесено до Реєстру платіжних систем, систем розрахунків, учасників цих систем та операторів послуг платіжної інфраструктури –

a) емітент
b) емітент-нерезидент
c) комерційний агент
d) користувач

4. Емітенту забороняється:

a) надавати кредит з коштів, які є зобов'язанням цього емітента за випущеними ним електронними грошима;

b) залучати агентів для випуску електронних грошей.

c) здійснювати операції, пов'язані з використанням електронних грошей, через окремий поточний рахунок, відкритий в емітента

d) застосовувати знак (торговельну марку, комерційне найменування), використання якого узгоджено емітентом з Національним банком.

5. Електронний гаманець користувача – суб'єкта господарювання використовується виключно для таких операцій:

a) списання електронних грошей на користь торговців для оплати товарів.

b) зарахування електронних грошей від емітента/агента з поповнення/агента з розповсюдження, які отримані в обмін на безготівкові кошти.

c) списання електронних грошей на користь агента з розрахунків для обміну на безготівкові кошти.

d) зарахування електронних грошей від користувачів за реалізовані товари.

6. Електронні гроші, це –

a) національна валюта України.

b) фіатні гроші.

c) валюта іноземної держави.

d) криптовалюта.

7. Емітент електронних грошей:

a) суб'єкт господарювання, що приймає електронні гроші як засіб платежу за товари законодавства України.

b) банківська установа.

c) має право здійснювати обмінні операції з випущеними ним електронними грошима на електронні гроші, випущені іншими емітентами, а також укладати договори з банками (агентами з обмінних операцій) про здійснення ними такої діяльності.

d) розміщує інформацію про узгодження правил використання електронних грошей на сторінці Офіційного Інтернет-представництва Національного банку.

До розділу 10: Адміністративна та кримінальна відповідальність за порушення у сфері використання інформаційних технологій

Завдання 1. **Ситуаційне завдання**:

Громадянин М., в період з січня по липень 2020 р. перебуваючи за місцем свого проживання в будинку № 5 по

вул. Сонячній у м. Харкові, використовуючи свій власний ноутбук «Соні», моделі SVZ1311CHXXI, серійний номер 5421547907003574 з можливістю доступу до мережі Інтернет, а також власний досвід у створенні програмного забезпечення на мові програмування «Visual C++», умисно, шляхом написання вихідних кодів створив функціональні модулі (складові частини) шкідливого програмного засобу під назвою «ZeuS 2.0.8.9.» у вигляді електронного файлу «zsb.exe», за допомогою якого, вказана шкідлива програма могла несанкціоновано потрапляти на комп'ютер фізичної чи юридичної особи, де без відома вказаних осіб серед інформації, яка обробляється і зберігається на вказаному комп'ютері, автоматично відшукувати будь-яку інформацію, у тому числі й паролі та ключі доступу до програмного забезпечення «клієнт-банк», а також щодо банківських рахунків, а після відшукання необхідної інформації, самостійно та несанкціоновано, тобто без дозволу власника комп'ютера, пересилатиме її через мережу Інтернет на сервер, заздалегідь визначений користувачем даної шкідливої програми, а також через мережу Інтернет буде надавати своєму користувачеві віддалений доступ до цього комп'ютера, за допомогою якого ним можливо було повністю управляти із будь-якого місця та без відома власника. За вказаний період громадянин М. отримав 109000 тис. грн неправомірного доходу.

1. Здійсніть юридичний аналіз ситуації.

2. Який вид юридичної відповідальності передбачено за порушення, вчинене громадянином М. (адміністративна чи кримінальна)?

3. Кваліфікуйте дії громадянина М.

4. Чи зміниться кваліфікація діяння, якщо грошова сума, яку незаконно отримав громадянин М. буде складати менш як 1500 грн.?

Питання до підсумкового контролю з дисципліни «ІТ-право»

1. Поняття та характеристика ІТ-права.
2. Поняття мережі Інтернет та цифрового середовища. Співвідношення понять між ними.
3. Інтернет-сайт як об'єкт права інтелектуальної власності.
4. Правовий режим веб-сторінки.
5. Поняття та ознаки правовідносин у цифровому середовищі.
6. Елементи правовідносин у цифровому середовищі: суб'єкти, об'єкти, зміст.
7. Види правовідносин, які виникають між учасниками у цифровому середовищі:
8. Порядок надання телекомунікаційних послуг.
9. Поняття, ознаки та характеристика електронного документа. Правове регулювання електронних документів.
10. Види електронних документів.
11. Електронний документообіг: поняття, ознаки, суб'єкти, сфера застосування, умови функціонування.
12. Порядок відправлення, передавання та одержання електронних документів. Правове значення.
13. Електронний цифровий підпис: поняття, види, значення, сфера застосування.
14. Поняття електронної комерції та електронної торгівлі.
15. Види електронної комерції. Функції електронної комерції.
16. Правове регулювання електронної комерції: Суб'єкти електронної комерції; вимоги до продавця і покупця.
17. Постачальники послуг проміжного характеру в інформаційній сфері як учасники відносин у сфері електронної комерції.
18. Електронні магазини, електронні аукціони, електронні біржі як учасники відносин у сфері електронної комерції.
19. Поняття та характеристика електронного правочину: предмет, сторони, особливості.
20. Правове регулювання електронних грошей в Україні та ЄС.

21. Поняття та ознаки електронних грошей, їх значення та правова природа.

22. Види електронних грошей.

23. Криптовалюта як продукт інформаційних технологій: поняття та ознаки.

24. Правовий режим криптовалюти. Проблеми правового регулювання.

25. Майнінг криптовалюти та можливості її використання.

26. Охорона авторських і суміжних прав у цифровому середовищі: основні засади та правове регулювання:

27. Технічні засоби захисту авторських і суміжних прав.

28. Способи захисту авторських і суміжних прав у мережі Інтернет: загальні та спеціальні.

29. Використання майнових авторських і суміжних прав на підставі вільних публічних ліцензій: поняття, ознаки та характеристика вільних публічних ліцензій.

30. Поняття комп'ютерної програми як об'єкта правової охорони, її ознаки.

31. Суб'єкти права інтелектуальної власності на комп'ютерну програму.

32. Особисті немайнові та майнові права інтелектуальної власності на комп'ютерну програму.

33. Випадки вільного використання комп'ютерної програми.

34. Компіляція (база) даних як об'єкт правової охорони.

35. Охорона прав на комерційні найменування, торговельні марки та інші комерційні позначення в мережі Інтернет: загальна характеристика, способи використання комерційних позначень в мережі Інтернет.

36. Доменне ім'я: поняття та ознаки.

37. Інтернет-корпорація з призначення доменних імен та номерів (ICANN): характеристика та функції.

38. Загальна характеристика договорів щодо розпорядження майновими правами інтелектуальної власності в цифровому середовищі.

39. Ліцензійний договір як договір щодо передання прав інтелектуальної власності у цифровому середовищі.

40. Особливості та види реклами в Інтернеті.

41. Юридична відповідальність за правопорушення в IT-сфері.

Додаток А

1	Об'єкт правової охорони	**Об´єкти авторського права:** 1) літературні письмові твори белетристичного, публіцистичного, наукового, технічного або іншого характеру (книги, брошури, статті тощо); 2) виступи, лекції, промови, проповіді та інші усні твори; 3) комп'ютерні програми; 4) бази даних; 5) музичні твори з текстом і без тексту; 6) драматичні, музично-драматичні твори, пантоміми, хореографічні та інші твори, створені для сценічного показу, та їх постановки; 7) аудіовізуальні твори; 8) твори образотворчого мистецтва; 9) твори архітектури, містобудування і садово-паркового мистецтва; 10) фотографічні твори, у тому числі твори, виконані способами, подібними до фотографії; 11) твори ужиткового мистецтва, у тому числі твори декоративного ткацтва, кераміки, різьблення, ливарства, з художнього скла, ювелірні вироби тощо; 12) ілюстрації, карти, плани, креслення, ескізи, пластичні твори, що стосуються географії, геології, топографії, техніки, архітектури та інших сфер діяльності; 13) сценічні обробки творів, зазначених у пункті 1 цієї частини, і обробки фольклору, придатні для сценічного показу
	Строк дії охорони прав	Авторське право діє протягом *усього життя* автора і *70 років* після його смерті Закон України «Про авторське право і суміжні права»
	Охоронний документ	Суб'єкт авторського права у будь-який час протягом строку охорони авторського права може зареєструвати своє авторське право у відповідних державних реєстрах і отримати *свідоцтво*
2	Об'єкт правової	**Об'єкти суміжних прав**: 1) виконання літературних, драматичних,

	охорони	музичних, музично-драматичних, хореографічних, фольклорних та інших творів; 2) фонограми, відеограми; 3) передачі (програми) організацій мовлення.
	Строк дії охорони прав	1. Майнові права виконавців охороняються *протягом 50 років* від дати першого запису виконання. Особисті немайнові права виконавців, передбачені частиною першою ст. 38 Закону «Про авторське право і суміжні права», охороняються *безстроково*. 2. Права виробників фонограм і відеограм охороняються протягом *50 років* від дати першого опублікування фонограми (відеограми) або їх першого звукозапису (відеозапису), якщо фонограма (відеограма) не була опублікована протягом зазначеного часу. 3. Організації мовлення користуються наданими цим Законом правами протягом *50 років* від дати першого публічного сповіщення передачі. 4. Закінчення строків захисту суміжних прав настає 1 січня року, наступного за роком, у якому закінчилися передбачені строки захисту.
	Охоронний документ (знак)	Для виникнення і здійснення суміжних прав *не вимагається* виконання будь-яких формальностей. Виконавець, виробник фонограми, виробник відеограми для сповіщення про свої суміжні права на фонограмах, відеограмах і всіх їх примірниках, що розповсюджуються серед публіки на законних підставах, або їх упаковках можуть використовувати **знак охорони** суміжних прав. Цей знак складається з таких елементів: латинська літера "Р", обведена колом, – (зображення знака не наводиться); імена (назви) осіб, які мають щодо цих фонограм (відеограм) суміжні права; рік першої публікації фонограми (відеограми).
3	Об'єкт правової охорони	**Наукове відкриття**
	Строк дії охорони прав	Не визначено (ст. 458 ЦК України)

	Охоронний документ	*Диплом*
4	Об'єкт правової охорони	**Винахід, корисна модель, промисловий зразок**
	Строк дії охорони прав	Строк на **винахід** спливає через *двадцять років*, від дати подання заявки. На **корисну модель** спливає через *десять років* від дати подання заявки. На **промисловий зразок** спливає через *п'ятнадцять років* від дати подання заявки
	Охоронний документ	Набуття права інтелектуальної власності засвідчується *патентом*
5	Об'єкт правової охорони	**Компонування інтегральної мікросхеми**
	Строк дії охорони прав	*десять років*, від дати подання заявки (гл. 40 ЦК України)
	Охоронний документ	*Свідоцтво*
6	Об'єкт правової охорони	**Раціоналізаторська пропозиція**
	Строк дії охорони прав	Оскільки свідоцтво закріплює, насамперед, право авторство на раціоналізаторську пропозицію, то його дія не обмежується будь-яким строком
	Охоронний документ	*Свідоцтво (*видається юридичною особою, яка визнала пропозицію раціоналізаторською).
7	Об'єкт правової охорони	**Сорт рослин, порода тварин**
	Строк дії охорони прав	тридцять п'ять років, що відліковуються з 1 січня року, наступного за роком державної реєстрації цих прав (гл.42 ЦК України)
	Охоронний документ	*Патент*
8	Об'єкт правової охорони	**Комерційне найменування**
	Строк дії охорони прав	До ліквідації юридичної особи

	Охоронний документ	охороняється без обов'язкового подання заявки на нього чи його реєстрації і незалежно від того, є чи не є комерційне найменування частиною торговельної марки. Відомості про комерційне найменування можуть вноситися до реєстрів, порядок ведення яких встановлюється законом
9	Об'єкт правової охорони	**Торговельна марка**
	Строк дії охорони прав	протягом *десяти років* з дати, наступної за датою подання заявки (гл. 44 ЦК України)
	Охоронний документ	*Свідоцтво*
1	Об'єкт правової охорони	**Географічне зазначення**
	Строк дії охорони прав	*безстроково* за умови збереження характеристик товару (послуги), позначених цим зазначенням : Закон України «Про охорону прав на зазначення походження товарів»
	Охоронний документ	*Свідоцтво*
1	Об'єкт правової охорони	**Комерційна таємниця**
	Строк дії охорони прав	Поки існує сукупність ознак комерційної таємниці (гл. 46 ЦК України)
	Охоронний документ	*Не потребує*

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Охотнікова О. М., Корпачова С. В. Деякі аспекти щодо становлення та розвитку ІТ-права в Україні // ІТ-право: проблеми і перспективи розвитку в Україні (четверта міжнародна щорічна конференція) 16 листопада 2018 р. http://aphd.ua/it-pravo-problemy-i-perspektyvy-rozvytku-v-ukrani-chetverta-mizhnarodna-shchorichna-konferentsiia/
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05. 10. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 42.
3. Закон України «Про стимулювання розвитку цифрової економіки в Україні» від 15.07.2021. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text
4. Сімсон О. Е. ІТ-право v. Інформаційного права: на зламі епох // ІТ-право: проблеми і перспективи розвитку в Україні (друга міжнародна щорічна конференція). URL: http://aphd.ua/publication-389/
5. Харитонова О. І. Проблемні питання визначення системи (структури) ІТ-права // ІТ-право: проблеми і перспективи розвитку в Україні. URL: http://aphd.ua/publication-186/
6. ІТ право / за заг. ред. проф. О.С. Яворської. – Львів: Видавництво «Левада», 2017. – 470с.
7. Є. Харитонов, О. Харитонова Сутність ІТ-права: пошук парадигми. *Право України*, 2018, №1. С. 18-29. URL: file:///C:/Users/%D0%9B%D0%B0%D0%BD%D0%BE%D1%87%D0%BA%D0%B0/Downloads/prukr_2018_1_4.pdf1ёё
8. Є. Харитонов, О. Харитонова «Інтернет-відносини» та «інтернет-правовідносини»: до визначення поняття і сутності. *Університетські наукові записки*, 2017, № 63. С. 27-38. URL: http://old.univer.km.ua/visnyk/1642.pdf
9. Інформаційне агентство "Інтерфакс-Україна". URL: https://ua.interfax.com.ua/news/telecom/730770.html
10. Національна стратегія захисту дітей в цифровому середовищі на 2021 – 2026 роки. URL: https://thedigital.gov.ua/regulations/natsionalna-strategiya-zakhistu-ditey-v-tsifrovomu-seredovishchi-na-2021-2026-roki
11. Петровский, С. В. Правовое регулирование оказания Интернет-услуг: дис. ... канд. юрид. наук: 12.00.03. Москва, 2002. 189 с. URL: http://www.lib.ua-ru.net/diss/cont/100565.html
12. Тедеев А. А. Теоретические основы правового регулирования информационных отношений, формирующихся в процессе использования глобальных компьютерных сетей :

автореф. дис … доктора юрид. наук: 12.00.14. Москва, 2007. 58 с. URL:http://law.edu.ru/book/book.asp?bookID=1311722

13. Єфремова К. В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспект. *Право та інноваційне суспільство*. 2014. № 1. С. 5–11.

14. Про електронні комунікації : Закон України від 16.12.2020. URL: https:// zakon.rada.gov.ua/laws/show/1089-20#Text

15. Новицький Міжнародний досвід правового регулювання інтернет. *Юридичний вісник*. 2 (31) 2014. С. 52-58.

16. Barlow J. A Declaration of the Independence of Cyberspace / John Perry Barlow // February 8, 1996 from Davos, Switzerla

17. J. Postel. RFC1591: Domain Name System Structure and Delegation.: RFC Editor. United States. 1994. URL: https://dl.acm.org/doi/10.17487/RFC1591#cited-by-sec

18. Доменна статистика .UA за підсумками жовтня 2021 року. Hostmaster Ltd. (uk). https://hostmaster.ua/UAstat/ 2021/?202110

19. Клименко А. А., Каландей В. О. Проблеми реалізації права інтелектуальної власності на інформаційні ресурси в Україні. Актуальні проблеми приватного права: матер. Всеукр. наук.-практ. інтернет-конф. (Ірпінь, 28 листопада 2019 р.). Ірпінь : Університет державної фіскальної служби України,2019. С. 93–96.

20. Офіційний сайт ТОВ «Хостмастер». URL: https://hostmaster.ua/policy/2ld.ua/

21. Про електронні комунікації : Закон України від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

22. Булат Н.М. Поняття та ознаки доменного імені. Development of modern technologies and scientific potential of the world : coll. of scientific papers «□□□□□» with materials of the international scientific-practical conf., London, July 29, 2019. London : NGO «European Scientific Platform», 2019. V. 2. 118 p. P. 33–36.

23. Попцов А.В. Правовое регулирование доменного имени в Российской Федерации : автореф. дисс. ...канд. юрид. наук: 12.00.03. Москва, 2009. 36 с.

24. Некіт К. Г. Доменне ім'я як об'єкт цивільних прав. *Часопис цивілістики*. 2017. Вип. 23. – С. 40-44.

25. Булат Н. М. Доменне ім’я як засіб індивідуалізації інтернет-ресурсів. *Право і суспільство*. № 2 / 2020. С. 154-160.

26. Булат Н.М Основні напрями вдосконалення чинного законодавства щодо охорони доменних імен. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. Том 31 (70) Ч. 1 № 2 2020. С. 74-78

27. Доменні спори: українська й міжнародна актуальна практика. *Юрист & Закон*, 2019, №38. Електронне видання. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013152

28. UDRP спір та UDRP правила. Допоможе юрист? URL: https://legalitgroup.com/domenni-batli-

worldwide/?gclid=Cj0KCQiA8vSOBhCkARIsAGdp6RQnHZjnInvaep0Gk89OhsBVyEwzmI5doJAEN18kOr8xRTLY4IBR6e8aAvtjEALw_wcB

29. Пономарьов М. Узагальнення судової практики розгляду судами справ у спорах, пов'язаних із використанням імен доменів. URL: http://artimmer.com/ua/publicacii/uzagalnennya-suduvoi-praktyky/269-uzagal%60nennya-sudovo%D1%97-praktiki-rozglyadu-sudami-sprav-u-sporax,-pov-yazanix-%D1%96z-vikoristannyam-%D1%96men-domen%D1%96v

30. Правовий захист інтелектуальної власності в Україні: проблеми та перспективи розвитку. URL: https://zkg.ua/yurydychni-posluhy-praktyky/pravovyi-zakhyst-intelektualnoi-vlasnosti/

31. Новосельська І. В., Бобровник А. С. Теоретико-правові питання охорони авторського права в мережі інтернет. URL: https://dilegal.ua/teoretiko-pravovi-pitannya-oxoroni-avtorskogo-prava-v-merezhi-internet/

32. Водорєзова С. Р. Особливості правової охорони комп'ютерної програми як об'єкта інформаційних відносин. *Право та інновації.* № 3 (7) 2014. С. 69-76.

33. Філик Н. В., Омельченко Г. В. Комп'ютерна програма як об'єкт авторського права: проблеми правової охорони. *Юридичний вісник*. №2 (39). 2016. С. 130-137.

34. Жуванов Д. Яку форму правової охорони обрати для комп'ютерної програми. URL:http://www.romanenko.biz/ua/library/article_program.html.

35. Авдеева Г. К. Проблемы идентификации компьютерной программы как объекта авторского права URL:http://www.ipcmagazine.ru/index.php?option=com_content&view=article&id=491&Itemid=11.

36. Тарасенко Л. Л. Комп'ютерна програма як об'єкт інтелектуального права // Матеріали Міжнародної наукової конференції (круглий стіл) на тему «IT-право: проблеми і перспективи розвитку в Україні» у м. Львів, 18 листопада 2016 р. URL: http://aphd.ua/it-pravo-problemy-i-perspektyvy-rozvytku-v-ukrani-14/

37. Про авторське право і суміжні права : Закон України від 23.12.1993 № 3792-XII. *Відомості Верховної Ради України*. 1994. № 13. Ст. 64 URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text

38. Ю. Атаманова. Захист прав інтелектуальної власності у мережі Інтернет: світовий досвід та вітчизняні перспективи. *Право та інновації.* 2014 (3).

39. В. Борівська, Т. Міхайліна. Правовий режим вебсайту та його складників як об'єктів інтелектуальної власності. *Підприємництво, господарство і право*. №4, 2021. С.5-9.

40. Леонід Тарасенко. Інтернет-сайт як об'єкт іт-права . *Право України*. 2018. № 1. С. 103-113.

41. Кому належать виключні майнові права на службовий твір (комп'ютерну програму)? Зміни у зв'язку з підписанням Україною Угоди про асоціацію з Європейським союзом. URL: https://legalaid.ua/ua/komu-nalezhat-vyklyuchni-majnovi-prava-na-sluzhbovyj-tvir-komp-yuternu-programu-zminy-u-zv-yazku-z-pidpysannyam-ukrayinoyu-ugody-pro-asotsiatsiyu-z-yevropejskym-soyuzom/

42. Про затвердження Національного стандарту N 4 "Оцінка майнових прав інтелектуальної власності" : Постанова Кабінету Міністрів України; Стандарт від 03.10.2007 № 1185.

43. Рзаєв Д. О., Шарапов О. Д., Ігнатенко В. М., Дибкова Л. М. Інформатика та комп'ютерна техніка : Навч.-метод. посібник для самост. вивч. дисц. К. : КНЕУ, 2002. 486 с. URL: https://nmetau.edu.ua/file/130.pdf.

44. Верба І. І. Основи інтелектуальної власності: навчальний посібник / за ред. С. В. Чікін. 2-ге вид., перероб. і доп. К. : НТУУ «КПІ», 2013. С.132.

45. Каскадная модель. – URL: https://ru.wikipedia.org/wiki/Каскадная_модель

46. Фасій Б. В. Agile waterfall та out staff договір або договори на розробку програмного забезпечення. *Часопис цивілістики.* 26 (2017). С. 98-102.

47. Аутстаффинг – что это? Разъяснение термина, способы применения, достоинства и недостатки. URL: http://workstaff.ru/autstaffing-chto-eto-razyasnenie-termina-sposoby-primeneniya-dostoinstva-i-nedostatki-pri-ispolzovanii

48. Ткачук А. Договори NDA та NCA в IT-бізнесі URL:https://yur-gazeta.com/dumka-eksperta/navishcho-potribno-ukladati-dogovori-nda-ta-nca-v-itbiznesi.html

49. Постанова Верховного Суду. URL: https://zakononline.com.ua/court-decisions/show/80304725

50. Asaul A., Voynarenko M., Dzhulii L., Yemchuk L., Skorobohata L. and Mykoliuk O. The Latest Information Systems in the Enterprise Management and Trends in their Development. 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 409-412, doi: 10.1109/ACITT.2019.8779874

51. Клепікова О. А. Сучасний стан і місце інформаційних технологій в управлінні підприємством. *Науковий вісник міжнародного гуманітарного університету. Серія: Економіка і менеджмент.* 2013. № 5. С. 74-77.

52. Інна Головко. Електронна комерція: визнання де-юре: URL:http://www.visnuk.com.ua/ua/pubs/id/8946

53. Chaffey D. E-business and E-commerce Management / D. Chaffey// Strategy, Implementation and Practice. – Prentice Hall, 2009. – 800 p.

54. Zwass V. Electronic Commerce: Structures and Issues / V. Zwass// International Journal of Electronic Commerce. – V.1, №1, Fall, 1996. – P. 3–23.

55. Саммер А., Дункан Гр. Маркетинг. Пятая волна. E-commerce. – М. : 1999. – 152 с.

56. Treese C. Winfield, Stewart Lawrence C. Designing Systems for Internet Commerce. – AddisonWesley, 1998. – 375 p.

57. Плескач В. Л. Електронна комерція : підручник. – К. : Знання, 2007. – 535 с.

58. Маєвська А. А. Електронна комерція і право: навч.-метод. посібник. – Х. : 2010. – 256 с.

59. Електронна комерція. URL: http://www.bizmost.biz

60. Маловичко С. В. Тенденції та перспективи розвитку електронної торгівлі в Україні. *Економіка і регіон.* 2015. № 4. С. 67-73.

61. Nemat, R. (2011). Taking a Look at Different Types of E-commerce. World Applied Programming, 1 (2), 100-104.

62. Про Національну програму інформатизації : Закон України. *Відомості Верховної Ради України* (ВВР), 1998, № 27-28, ст.181.

63. Про електронну комерцію : Закон України. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

64. Тардаскіна Т. М. та ін. Електронна комерція: навчальний посібник. – Одеса : ОНАЗ ім. О.С. Попова, 2011. – 244 с.

65. Самойленко Л. Переваги застосування електронного бізнесу. *Економіка АПК*. 2003. № 8. – С. 141 – 146.

66. Гресь А. М. Удосконалення організації систем доставки товарів у електронній торгівлі в Україні. *Науковий вісник Українського державного лісотехнічного університету*. 2004. Вип.14.4. – С. 288–294.

67. Про електронні документи та електронний документообіг : Закон України. *Відомості Верховної Ради України* (ВВР), 2003, № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

68. Про електронні довірчі послуги : Закон України. *Відомості Верховної Ради України* (ВВР), 2017, № 45. Ст. 400. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534

69. Б. Дучак Електронні гроші в (У)країні третього світу / URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ000975

70. Директива європейського парламенту і ради 2009/110/ЄС від 16 вересня 2009 року про започаткування та здійснення діяльності установами-емітентами електронних грошей і пруденційний нагляд за нею, про внесення змін до директив 2005/60/ЄС і 2006/48/ЄС та про скасування Директиви 2000/46/ЄС

71. Про платіжні послуги : Закон України від 30.06. 2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#n1249

72. В. Кравчук, Д. Науменко, А. Глибовець. Електронні гроші в Україні. *Аналітичний звіт.* – К. : АльфаПІК, 2012. – 64 с.
73. Офіц веб-сторінка Нацбанку України. URL: https://bank.gov.ua/ua/payments/nocash/bank-elektron-grosh
74. The 2020 Global Crypto Adoption Index: Cryptocurrency is a Global Phenomenon URL: https://blog.chainalysis.com/reports/2020-global-cryptocurrency-adoptionindex-2020
75. Биткойн: система цифровой пиринговой наличности URL: https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf
76. Что такое биткоин? URL: https://forklog.com/chto-takoe-bitkoin/]
77. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text
78. Іван Лясківський. Новий закон про віртуальні активи — нові можливості для бізнесу. URL: //https://ain.ua/2021/09/13/novij-zakon-pro-virtualni-aktivi-novi-mozhlivosti-dlya-biznesu-kolonka-yurista/
79. Олег Кремінський Правовий режим віртуальної валюти (криптовалюти) в Україні. *Path of Science*. 2020. Vol. 6, No 4
80. Казначєєва Д. В., Дорош А. О. Криптовалюта: проблеми правового регулювання. *Вісник кримінологічної асоціації України*. № 2(23). 2020. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9575/Kryptovaliuta_%20problemy%20pravovoho%20rehuliuvannia_Kaznachieieva_Dorosh_2020.pdf?sequence=1&isAllowed=y
81. Шинкаренко О. М., Рогова Н. В., Панівнік І. А. Особливості нормативного регулювання криптовалют: світовий досвід. *Фінансовий простір*. 2018 № 3 (31). С. 139-144.
82. https://reyestr.court.gov.ua/Review/56686444)
83. Із рішенням можна ознайомитися за покликанням: https://reyestr.court.gov.ua/Review/95524461.
84. Із рішенням можна ознайомитися за покликанням: https://reyestr.court.gov.ua/Review/93786356.
85. Міжнародний досвід законодавчого регулювання питання функціонування криптовалют, криптовалютних бірж, майнінгу та виводу в фіат (Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром). URL: https://radaprogram.org/sites/default/files/infocenter/piblications/65.pdf
86. Офіційний сайт Академії електронного управління Естонії. URL: https://ncsi.ega.ee/country/ua/
87. Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206-220.

ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). URL: https://doi.org/10.1007/978-3-030-66717-7

88. Спіцина Г. О., Філіпенко Н. Є. Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 188-191.

89. Стратегія національної безпеки України. Указ Президента України №121/2021. URL: https://www.president.gov.ua/documents/3922020-35037

90. Стратегія воєнної безпеки України. Указ Президента України № 392/2020. URL: https://www.president.gov.ua/documents/1212021-37661

91. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ : КВІЦ, 2019. С 108.

92. Швачич Г. Г., Толстой В. В., Петречук Л. М., Іващенко Ю. С., Гуляєва О. А., Соболенко О. В. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. Дніпро : НМетАУ, 2017. С. 7.

93. C. G. Reddick Handbook of Research on Strategies for Local E-government Adoption and Implementation / C. G. Reddick. IGI Global, 2009. 1106 p.

94. Климанська Л. Д. Комунікативні технології моделювання політичного простору в демократичному суспільстві. URL: www.democracy.kiev.ua/publications/collections/conference_2005.

95. Навчальні матеріали з інформатики. Інформація і світ. Інформаційні й комунікаційні технології. URL: https://www.ua5.org/svit/281-nformacjjn-jj-komunkacjjn-tekhnolog.htm

96. Кочубей Л. Особливості сучасних інформаційно-комунікативних технологій в Україні. *Наукові записки ІПіЕНД ім. І.Ф. Кураса НАН України*. Випуск 3(89). С. 44-70.

97. Степанов О. А. Теоретико-правовые основы безопасного функционирования и развития информационно-электронных систем : дис. докт. юрид. наук: 12.00.01, М., 2005. 365 с.

98. Калєніченко Л. І. Юридична відповідальність як форма державно-правового примусу: загальнотеоретична характеристика : автореф. дис. д-а юридичних наук. Харківський національний університет внутрішніх справ. Харків, 2018. С. 1.

99. Конституція України. *Відомості Верховної Ради України* (ВВР), 1996, № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

100. Юридичний словник-довідник / За ред. Ю. С. Шемшученка. Київ : Феміна, 1996. С. 689.

101. Кримінальний кодекс України. *Відомості Верховної Ради України* (ВВР), 2001, № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=комп#w1_11

102. Кібершпигуни з Китаю та Росії атакують компанії США – доповідь. URL: https://news.obozrevatel.com/ukr/abroad/60549-kibershpiguni-z-kitayu-ta-rosii-atakuyut-kompanii-ssha-dopovid.htm

103. Спасович В. Д. Учебник уголовного права. Часть Общая. С.-Пб., 1863.

104. Таганцев М. С. Юридична енциклопедія : у 6 т. / ред. кол. Ю. С. Шемшученко (відп. ред.) та ін. К. : Українська енциклопедія ім. М. П. Бажана, 2004. Т. 6 : Т- Я. С. 8. ISBN 966-7492-06-0.

105. Материалы для пересмотра нашего уголовного законодательства. Сборник дополнительных узаконений к французскому и германскому уголовным уложениям. Т. 7: Вып. 1-2 / Сост.: Г. Г. Савич; Под ред.: Н. С. Таганцев. С.-Пб. Тип. Правит. Сената, 1883. 786 с.

106. Познышев С. В. Основные начала науки уголовного права. Общая часть уголовного права. М., 1912.

107. Таций В.Я. Об'єкт злочину. *Вісник Асоціації кримінального права України*, 2013, № 1(1). С. 126-143.

108. Емельянов, В. П. Концептуальные аспекты исследования объекта преступления. *Право и политика.* 2002. № 10. С. 65–66.

109. Доктрина інформаційної безпеки України. Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

110. Буга Я. Загальна характеристика комп'ютерних злочинів. URL: http://conf.inf.od.ua/doklady-konferentsii/spisok-dokladov-iii-konferentsii/78-buga-ya

111. Узагальнення судової практики розгляду Бориспільським міськрайонним судом кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI Особливої частини Кримінального кодексу України) за 2012-2014 роки. URL: https://court.gov.ua/userfiles/file/bor111/eom.pdf

112. Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. Наказ Міністерства соціальної політики України від 14.02.2018 № 207. URL: https://zakon.rada.gov.ua/laws/show/z0508-18#Text

113. ДСТУ 2938-94. Системи оброблення інформації. Основні положення. Терміни та визначення. 01.01.96. С. 3

114. Кримінальне право України: Особлива частина : підручник / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін. ; за ред. В. В. Сташиса, В. Я. Тація. 4-те вид., переробл. і допов. Х. : Право, 2010. 608 с. URL: http://library.nlu.edu.ua/POLN_TEXT/KNIGI-2010/UgolovPravoOsob.pdf

115. Науково-практичний коментар Кримінального кодексу України / За ред. М. І. Мельника. М. І. Хавронюка. К., 2001. С. 902; Науково-практичний коментар до Кримінального кодексу України / Під загальною редакцією Потебенька М. О., Гончаренка В. Г. К., 2001., у 2-х ч. Особлива частина. С. 721.

116. Мазуренко О., Розенфельд Н. Комп'ютерна інформація як предмет злочинів, передбачених Розділом XVI КК України. *Право України,* 2004, № 6. С. 80-83. URL: https://www.savinova.info/sites/default/files/all/articles/2004_01s.pdf

117. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. ... канд. юрид. наук. Київ, 2003. С. 9.

118. Карчевський В. М. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж : монографія / МВС України, Луг. акад. внутр. справ ім. 10-річчя незалежності України; Наук. ред. Л. М. Кривоченко. Луганськ, 2002. С. 56.

119. Кримінальне право України: Особлива частина: Підруч. для студ. вищ. навч. закл. освіти / М. І. Бажанов, В. Я. Тацій, В. В. Сташис, І. О. Зінченко та ін. / За ред. професорів М. І. Бажанова, В. В. Сташиса, В. Я. Тація. К. : Юрінком Інтер. Х. : Право, 2001. С. 363.

120. Академічний тлумачний словник української мови в 11 томах. URL: http://sum.in.ua/s/predmet

121. Yuriy Khodyko The concept of things in the context of determining the object of the property relationship. URL:ttps://www.researchgate.net/publication/321892948_The_concept_of_things_in_the_context_of_determining_the_object_of_the_property_relationship

122. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Видання офіційне. Київ : Держстандарт України, 1994.

123. Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи. Рішення Вищої ради правосуддя від 17 серпня 2021 року № 1845/0/15-21.

124. Кодекс України про адміністративні правопорушення. *Відомості Верховної Ради Української РСР* (ВВР) 1984, додаток до № 51, ст.1122. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text

125. Юридична енциклопедія. URL: https://leksika.com.ua/17340813/ure/administrativna_vidpovidalnist

126. Адміністративна відповідальність. Мультимедійний навчальний посібник. URL: https://arm.naiau.kiev.ua/books/adm-vidpov/pages/avtori.html

127. Колпаков В.К. Предмет адміністративного права: поняття, структура і система адміністративно-правових відносин. Питання адміністративного права. Кн. 2. Харків : Оберіг, 2018. С. 17.

128. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ : КВІЦ, 2019. 344 с.

129. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ : Видавничий дім "Гельветика", 2017. С. 55.

130. Настюк В. Я., Білєвцева В. В. Загальноправова характеристика адміністративної відповідальності за інформаційні правопорушення. *Інформація і право*. 2013. № 1. С. 151–157.

131. Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія. Київ : Видавничий дім «Гельветика», 2017. 700 с.

132. Стоєцький О. В. Адміністративна відповідальність за пору- шення у сфері інформаційної безпеки України : дис. … канд. юрид. наук : спец. 12.00.07. Нац. Акад. внутр. справ. К., 2013. 191 с.

133. Чуприна О. В. Адміністративна відповідальність за порушення права на інформацію : дис. ... канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». К., 2013.

Навчальне видання

Гуцу Світлана Федорівна
кандидат юридичних наук, доцент

Матвєєва Анастасія Володимирівна
кандидат юридичних наук, старший науковий співробітник

Спіцина Ганна Олександрівна
доктор юридичних наук, професор

Стародубцев Андрій Андрійович
доктор юридичних наук, доцент

Філіпенко Наталія Євгенівна
доктор юридичних наук, доцент,

Федосенко Наталія Анатоліївна
кандидат юридичних наук, доцент

ІТ-ПРАВО
Навчальний посібник

Зв. план, 2022. Підписано до друку 25 серпня 2022 р. Формат 60 х 84 1/16.
Ум. друк. арк. 13,0. Обл.-вид. арк. 9,8. Наклад 100 пр.
Замовлення. 10/2022.

Національний аерокосмічний університет імені М.Є. Жуковського
«Харківський авіаційний інститут»
61070, Харків-70, вул. Чкалова, 17. http://www.khai.edu
Видавничий центр «ХАІ». izdat@khai.edu
61070, Харків-70, вул. Чкалова,17

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції сер. ДК № 391 від 30.03.2001