

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний аерокосмічний університет імені М. Є. Жуковського
«Харківський авіаційний інститут»



С. Ф. Гуцу, А. О. Гордеюк, В. І. Павликівський,
Н. Є. Філіпенко, Н. А. Федосенко

ІТ-ПРАВО

Навчальний посібник

Харків «ХАІ» 2025

Рекомендовано до друку
Радою гуманітарно-правового факультету
Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авіаційний інститут»,
протокол № 3 від 18 листопада 2024 року
Науково-методичною комісією № 3
Національного аерокосмічного університету
імені М. Є. Жуковського «Харківський авіаційний інститут»,
протокол № 3 від 22 листопада 2024 року

Рецензенти:

МОЖАЄВ Михайло Олександрович, доктор технічних наук, директор Науково-дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України.

ОРЛОВ Юрій Володимирович, доктор юридичних наук, професор, завідувач кафедри кримінального права і кримінології навчально-наукового інституту № 1 Харківського національного університету внутрішніх справ.

Г 93

ІТ-право [Електронний ресурс] : навч. посіб. / С. Ф. Гуцу, А. О. Гордеюк, В. І. Павликівський, Н. Є. Філіпенко, Н. А. Федосенко ; 2-ге вид. доповн. і переробл. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т»; 2025. – 149 с.

У посібнику досліджено основи правового регулювання ІТ-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».

Іл. 2. Бібліогр.: 107 назв.

УДК 347.772.3

© Гуцу С. Ф., Гордеюк А.О., Павликівський В.І.,
Філіпенко Н. Є., Федосенко Н. А., 2025
© Національний аерокосмічний університет
імені М. Є. Жуковського
«Харківський авіаційний інститут», 2025

ЗМІСТ

ПЕРЕДМОВА	5
РОЗДІЛ 1. ІТ-ПРАВО ЯК НОВА ПРАВОВА КАТЕГОРІЯ	7
Запитання для самоконтролю і самостійного опрацювання	11
РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ МЕРЕЖІ ІНТЕРНЕТ	12
2.1. Визначення і співвідношення понять «Інтернет» і «цифрове середовище»	12
2.2. Регулювання мережі Інтернет	15
Запитання для самоконтролю і самостійного опрацювання	18
РОЗДІЛ 3. ДОМЕННІ ІМЕНА	19
3.1. Як виникла система доменних імен (DNS)	19
3.2. Правове регулювання доменних імен	20
3.3. Юридичний захист прав на домене ім'я	26
Запитання для самоконтролю і самостійного опрацювання	31
РОЗДІЛ 4. ОХОРОНА ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ	32
4.1. Охорона авторських і суміжних прав в мережі Інтернет	32
4.2. Комп'ютерна програма як об'єкт правової охорони	35
4.3. Веб-сайт як складний об'єкт права Інтелектуальної власності	43
4.4. Авторські права на службовий твір та твори, створені за замовленням	46
4.5. Захист авторського права і суміжних прав	48
Запитання для самоконтролю і самостійного опрацювання	53
РОЗДІЛ 5. ДОГОВОРИ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ІТ)	54
5.1. Загальні положення щодо договірних відносин в цифровому середовищі та їх види	54
5.2. Ліцензійні угоди в сфері ІТ	57
5.3. Договори на розробку програмного забезпечення	64
5.4. Договори на надання ІТ-послуг	68
5.5. Договори на технічну підтримку та обслуговування	69
Запитання для самоконтролю і самостійного опрацювання	71
РОЗДІЛ 6. ГОСПОДАРСЬКА ДІЯЛЬНІСТЬ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ. ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ	72
6.1. Електронна комерція	72
6.2. Електронний документообіг	76
Запитання для самоконтролю і самостійного опрацювання	81
РОЗДІЛ 7. ЕЛЕКТРОННІ ГРОШІ: ПОНЯТТЯ, ЗМІСТ ТА ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ В УКРАЇНІ	82
Запитання для самоконтролю і самостійного опрацювання	87
РОЗДІЛ 8. ПРАВОВИЙ РЕЖИМ ВІРТУАЛЬНОЇ ВАЛЮТИ (КРИПТОВАЛЮТИ)	88
8.1. Зміст та юридична природа криптовалюти	88
8.2. Правовий режим криптовалют у світі: підходи до регулювання	94
Запитання для самоконтролю і самостійного опрацювання	97
РОЗДІЛ 9. ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ	98

9.1. Загальні відомості про юридичну відповідальність в ІТ-сфері	99
9.2. Адміністративна відповідальність за порушення у сфері використання інформаційно-комунікаційних технологій	104
Запитання для самоконтролю і самостійного опрацювання	108
РОЗДІЛ 10. КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ	109
10.1. Підстави кримінальної відповідальності за порушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку	110
10.2. Склад кримінального правопорушення як підстава притягнення до кримінальної відповідальності.....	111
Запитання для самоконтролю і самостійного опрацювання	126
РОЗДІЛ 11. ПРАКТИЧНІ ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ	127
До розділу 1: ІТ-право як нова правова категорія	127
До розділу 2: Правове регулювання мережі Інтернет	127
До розділу 3: Доменні імена	127
До розділу 4: Охорона прав інтелектуальної власності в цифровому середовищі	129
До розділу 5: Договірні відносини в цифровому середовищі	129
До розділу 6: Господарська діяльність з використанням інформаційних технологій. Електронний документообіг	132
До розділів 7-8: Електронні гроші: поняття, зміст та особливості правового регулювання в Україні. Правовий режим віртуальної валюти (криптовалюти)	136
До розділів 9-10: Юридична відповідальність за порушення законодавства у сфері використання інформаційно-комунікаційних технологій. Кримінальна відповідальність за порушення у сфері використання інформаційних технологій	137
ПИТАННЯ ДО ПІДСУМКОВОГО КОНТРОЛЮ З ДИСЦИПЛІНИ «ІТ-ПРАВО»	139
БІБЛІОГРАФІЧНИЙ СПИСОК	141

ПЕРЕДМОВА

Сучасний світ переживає четверту промислову революцію, характерними рисами якої є побудова глобального цифрового світу. Ми живемо в інформаційному суспільстві, що постійно розширюється. Глобальні комп'ютерні мережі, мобільна телефонія та цифрова аудіовізуальна передача не лише охоплюють практично всі види комунікації, але все більше стають основою функціонування сучасного людського суспільства. Тому варто розглянути, який вплив ці технології мають на право, основним завданням якого є забезпечення функціонування держави та суспільства і, насамперед, безпеки людини. Залишення ІКТ-технологій без не лише чіткого, але й адаптованого до нового комунікаційного середовища законодавства створює небезпеку порушення інтересів особи, особливо права на приватність. Важливо забезпечити комплексний – як технічний, так і юридичний – захист ІКТ-систем. Підтримка балансу між свободою та безпекою особистості є старим і все ще актуальним складним викликом у новій технологічній комунікаційній реальності. Правові стандарти є і мають бути неминуче спрямовані на збереження обох цих фундаментальних цінностей¹.

Право Інформаційних Технологій або кіберправо, охоплює широкий спектр правових питань, пов'язаних із використанням технологій, комп'ютерів, Інтернету та інформації. Так, ІТ-закони захищають права та інтереси фізичних осіб, підприємств і організацій, які працюють у цифровій сфері. Ці закони встановлюють керівні принципи та стандарти відповідального та законного використання технологій для запобігання зловживанням і захисту користувачів. Захищаючи права інтелектуальної власності та створюючи законодавчу базу для технологій, ІТ-закони заохочують інновації та технологічний прогрес. Закони про кібербезпеку допомагають у захисті систем і даних, що має вирішальне значення в епоху, коли кіберзагрози переважають. Норми про електронну комерцію забезпечують правову структуру, яка підтримує бізнес-операції в Інтернеті, сприяючи економічному зростанню та торгівлі. Закони про захист даних заохочують права осіб на конфіденційність, встановлюючи спосіб збору, зберігання та використання особистої інформації. 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».

У науковій літературі ряд вчених наполягає, що Право інформаційних технологій – це неологізм в науковому обігу, доктринальне поняття, яке не використовується в чинному законодавстві України та уявляє собою «сукупність уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з правовим впорядкуванням суспільних відносин, пов'язаних зі створенням та використанням ІТ»². Інші обґрунтовують введення в науковий обіг нової комплексної галузі права – права інформаційних технологій. Наголошуючи, що ІТ-право – «не штучний феномен, а закономірний

¹ Malgorzata Skorzevska-Amberg Impact of ICT. Technology, Society and Sustainability: Selected Concepts, Issues and Cases. 2017/03/03. https://www.researchgate.net/publication/314196632_Impact_of_ICT_on_the_law

² Харитонов Є. О. Право інформаційних технологій // Енциклопедія соціогуманітарної інформології / коорд. проекту та заг. ред. проф. К. І. Беляков. Київ : Видавничий дім «Гельветика», 2020. Т. 1. С. 190-194.

результат розвитку економічних відносин, котрі виникають, змінюються та припиняються в сфері інформаційних технологій. Тому слід говорити про початок його формування і потрібно докласти чимало зусиль для розробки і становлення права інформаційних технологій як одного з найбільш перспективних напрямів розвитку сучасної юриспруденції».³

Таким чином, треба визнати що право інформаційних технологій сьогодні виступає в якості складного явища, що містить в собі норми з різних галузей права і правових інститутів, але при цьому регулює особливий блок суспільних відносин які функціонують у цифровому середовищі.

У підготовці навчального посібника брали участь:

кандидат юридичних наук, доцент С. Ф. Гуцу (Розділи 1, 2, 3 (п.3.1), 6, 7, 8, 11),
кандидат юридичних наук, доцент А. О. Гордеюк (розділ 3 (п.3.2, п.3.3), розділ 4),
доктор юридичних наук, професор В. І. Павликівський (розділ 10),
доктор юридичних наук, професор Н. Є. Філіпенко (розділ 9, 11),
доцент Н. А. Федосенко (розділ 5, 11).

³ Тицька, Я. О., Поварчук, Н. С. Доктринальні підходи щодо визначення статусу права інформаційних технологій. Київський часопис права, 2023, № 1. С. 41-46. DOI: <https://doi.org/10.32782/kj/2023.1.6>.

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. Сфера застосування інформаційних технологій спричинила появу специфічної, раніше невідомої людству сфери суспільних відносин – відносин у цифровому (віртуальному) просторі. Ситуація, котра складається в останнє десятиліття в правотворчій сфері, характеризується бурхливим розвитком вітчизняного законодавства. Одним із факторів, який впливає на це є цифрові технології, котрі створюють нову реальність. Природно, що поява нових і актуалізація існуючих сфер соціальної діяльності не може не впливати на систему права. Більше того, цифрові технології починають диктувати свої умови, до яких необхідно адаптувати систему права⁴.

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 ХХ 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. Прихильники такої позиції звертають увагу на той факт, що одні й ті ж самі проблеми досліджуються в працях з інформаційного права та права інформаційних технологій, з тією лише різницею, що в більш давніх публікаціях використовується термін «інформаційне право», а в публікаціях останніх десяти років використовується термін «право інформаційних технологій» чи «ІТ-право», тобто є більш сучасною варіацією терміну «інформаційне право». 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 правового 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

⁴ Тицька, Я. О., Поварчук, Н. С. Доктринальні підходи щодо визначення статусу права інформаційних технологій // *Київський часопис права*, 2023, № 1. С. 41-46. DOI: <https://doi.org/10.32782/kj/2023.1.6>.

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 тощо⁵. 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.

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»⁶. 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? З цього питання у науковій літературі продовжуються активні дискусії. Серед дослідників склалось декілька протилежних підходів. Одні визнають право інформаційних технологій повноцінною комплексною галуззю права, інші стверджують, що воно знаходиться лише на стадії становлення, треті заперечують можливість визнання ІТ-права в якості самостійної галузі права. Також в юридичній літературі зустрічаються позиції, відповідно до яких право інформаційних технологій – це галузь законодавства чи навіть практики.

⁵ 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/>

⁶ Харитонов, Є. Харитонova, О. Сутність ІТ-права: пошук парадигми // Право України, 2018, №1. С. 18-29.

Так, відповідно до точки зору О. Марценюка: «інформаційне право України виступає самостійною комплексною галуззю національного права, що вимагає теоретичного обґрунтування окремих інститутів інформаційного права при їх комплексному застосуванні в українській правовій системі, встановлення самостійного методу інформаційного права»⁷. В свою чергу 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»⁸. Професорка О. С. Яворська вважає, що ІТ-право – це комплексна галузь права, що регулює відносини у цифровому середовищі⁹. З погляду загальної теорії права існування комплексних галузей можливе, але із застереженням, що вести мову про такі комплексні утворення правових норм варто не щодо галузей права, а стосовно галузей законодавства. Тому в юридичній літературі висловлюється точка зору, що більш виправданою убачається оцінка права інформаційних технологій як сукупності актів законодавства, що «регулюють ІТ-відносини, які з певною мірою умовності може іменуватися «ІТ-законодавством» (Д. Гетьманцев, Б. Кормич).

Для відповіді на питання про статус ІТ-права, 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 різномірні 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 різномірними 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. Харітонова 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 вчені

⁷ Марценюк О. Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію : дис. ... канд. юрид. наук : 12.00.07. Київ, 2009. 266 с.

⁸ Харітонова О. І. Проблемні питання визначення системи (структури) ІТ-права // ІТ-право: проблеми і перспективи розвитку в Україні. URL: <http://aphd.ua/publication-186/>

⁹ . ІТ право / за заг. ред. проф. О.С. Яворської. – Львів: Видавництво «Левада», 2017. – 470 с.

роблять висновок про те, що з позицій нормативістського праворозуміння галузі ІТ-права (так само й Інтернет-права, інформаційного права як галузей права) не існує ¹⁰.

Цікавою є позиція щодо віднесення ІТ-права до галуззі юридичної практики. Так, Дацюк В.Б. спираючись на західний досвід, зазначає, що у західній юриспруденції ІТ-право здебільшого розглядається не як самостійна галузь права у класичному її розумінні, а як галузь практики, яка стосується різних правових аспектів стосовно договорів у сфері інформаційних технологій, інтелектуальної власності, конфіденційності та захисту інформації тощо. На думку науковця: «ІТ-право сьогодні слід розглядати у першу чергу як галузь практики, яка виникла і розвивається незалежно від волі законодавця та становить собою сукупність норм різних галузей законодавства, які так чи інакше регулюють специфічні відносини, що складаються у сфері інформаційних технологій. ІТ-право як індустрія в праві охоплює такі аспекти правового забезпечення ІТ-сфери як:

- 1) правовий супровід стартапів в ІТ-сфері;
- 2) вибір юрисдикції та реєстрація ІТ-бізнесу;
- 3) договірні відносини, електронна комерція та ЗЕД-контракти у сфері ІТ;
- 4) податкове структурування ІТ-бізнесу;
- 5) питання щодо антимонопольного права в ІТ-секторі;
- 6) особливості валютного регулювання та банківських відносин у сфері ІТ;
- 7) трудові відносини в ІТ-компаніях;
- 8) реєстрація авторських прав та реєстрація знаків для товарів та послуг;
- 9) захист персональних даних;
- 10) правове забезпечення кібербезпеки;
- 11) правова допомога у вирішенні конфліктів в ІТ-сфері (досудове та судове врегулювання спорів) тощо»¹¹.

До об'єктів ІТ права можна віднести:

1. Конфіденційність і захист даних: це включає нормативні акти та закони, що регулюють збір, зберігання та використання персональних даних, наприклад GDPR (Загальний регламент захисту даних) у Європі, Закон «Про захист персональних даних» в Україні або аналогічні закони в інших країнах.

2. Кібербезпека: закони, що стосуються заходів захисту мереж, систем і даних від несанкціонованого доступу, порушень і кібератак.

3. Інтелектуальна власність: захист прав інтелектуальної власності в цифровій сфері, що охоплює такі питання, як авторське право, патенти, торгові марки та комерційні таємниці щодо цифрового вмісту та винаходів.

4. Електронна комерція та цифрові транзакції: управління онлайн-діловими транзакціями, контрактами, електронними підписами та захистом споживачів під час онлайн-покупок.

5. Телекомунікації: правила, що стосуються комунікаційних мереж, широкосмугового зв'язку, послуг Інтернету, а також правила, пов'язані з мережевою нейтральністю та доступом.

¹⁰ Є. Харитонов, О. Харитонova «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>

¹¹ Дацюк, В. Б.. ІТ-право та економічні свободи [Текст] / В. Б. Дацюк // Правове регулювання та економічні свободи і права : монографія / Ужгород. нац. ун-т, НДІ порівнял. публіч. права та міжнар. права. - Ужгород : Рік-У, 2020. - Розд. 4. - С. 110-141. ISBN 978-617-7692-74-3.

6. Кіберзлочини: закони, які стосуються таких правопорушень, як хакерство, фішинг, кіберзалякування, онлайн-шахрайство, крадіжка особистих даних та інші незаконні дії, що здійснюються в кіберпросторі.

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. З точки зору усталених наукових підходів до структурування системи права, ІТ-право уже давно вийшло за рамки міжгалузевого правового інституту, але ще не «виросло» у самостійну галузь права в класичному її розумінні. 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. ІТ-Право є галуззю нового покоління, характерною рисою якого є поєднання публічних та приватних інтересів при явному домінуванні перших. В юридичній літературі висловлюється точка зору, відповідно до якої головне призначення галузей права нового покоління – обслуговування нових чи модифікація усталених функцій держави¹².

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.

¹² Тицька, Я. О., Поварчук, Н. С. Доктринальні підходи щодо визначення статусу права інформаційних технологій. // *Київський часопис права*, 2023. № 1. С. 41-46. DOI: <https://doi.org/10.32782/kjp/2023.1.6>.

РОЗДІЛ 2. ПРАВОВЕ РЕГУЛЮВАННЯ МЕРЕЖІ ІНТЕРНЕТ

2.1. Визначення і співвідношення понять «Інтернет» і «цифрове середовище»

Сьогодні вже важко уявити собі сучасне людське суспільство без комп'ютерних мереж. Вперше ідея зв'язати кілька незалежно працюючих комп'ютерів в єдину розподілену обчислювальну систему виникла в середині 60-х років XX століття у США. Першою була створена мережа **ARPANET** для спілкування науковців різних інститутів, що працювали над військовими проблемами. Головним заданням було створення мережі, яка могла б розширюватися, щоб приєднання чи вихід з ладу одного з вузлів не впливало на функціонування інших. Однак протокол NCP, згідно з яким працювала ARPANet, не передбачав взаємодії між мережами різної архітектури, тому в 1973 році було створено новий протокол TCP/IP. Перехід мережі на новий протокол дав їй змогу в 1984 р. розділитися на дві: **MILNet** – для військового відомства і **ARPANET** – для невійськового використання. У 1990 р. ARPANet припинила своє існування.

Сьогодні у світі існує безліч локальних і декілька глобальних (WideArea Network, WAN, INTERNET, Bitnet, DECnet та інші) комп'ютерних мереж. Мережа Інтернет це на сьогодні найбільша і найпопулярніша глобальна комп'ютерна мережа. За даними компанії GlobalLogic, понад 66 відсотків усіх людей на Землі зараз користуються Інтернетом, а за останніми даними загальна кількість користувачів у всьому світі становить 5,35 мільярда станом на початок 2024 року. За останні 12 місяців кількість користувачів Інтернету зросла на 1,8 відсотка завдяки 97 мільйонам нових користувачів з початку 2023 року. На початок 2024 року в Україні було 29,64 мільйона користувачів Інтернету, тоді рівень проникнення становив 79,2 відсотка від населення країни¹³.

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»)¹⁴.

Визначення поняття «цифрове середовище» у чинному законодавстві України наводиться у Законі України «Про цифровий контент та цифрові послуги». За ним: **«цифрове середовище - апаратне, програмне забезпечення та будь-яке мережеве підключення, що використовується з метою отримання доступу до цифрового контенту та/або цифрової послуги та забезпечує можливість їх**

¹³ Digital 2024: Country Headlines Report. // <https://datareportal.com/reports/digital-2024-local-country-headlines>.

¹⁴ ІТ право / за заг. ред. проф. О.С. Яворської. – Львів: Видавництво «Левада», 2017. – 470 с.

використання споживачем»¹⁵. Крім того, у Проекті 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]. Таким чином, в цьому посібнику будемо розглядати мережу Інтернет як складову частину цифрового середовища (простору).

Основими *ознаками* мережі Інтернет вважають такі: 1) Інтернет як технологічна система, що забезпечує обмін інформацією між комп'ютерами, є різновидом мережі електрозв'язку – телекомунікаційної мережі; 2) Інтернет як система інформаційного зв'язку регулює суспільні відносини з приводу обміну даними; 3) Інтернет має глобальний, екстериторіальний, міжнародний характер; 4) Інтернет відкритий для використання всіма фізичними та юридичними особами, тобто є мережею зв'язку загального користування; 5) мережа Інтернет призначена для передачі (обміну) електронних даних.

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. Відповідно 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, Невзоров І.В. визначив **Інтернет** як здійснюване з використанням електрозв'язку для передачі закодованої інформації з'єднання максимального (найбільшого) на конкретний момент часу числа електроннообчислювальних 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.

В свою чергу Катерина 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 майбутньому¹⁶.

Схожу позицію щодо сутності Інтернет мережі висловлює Руслан Еннан: «Інтернет є екстериторіальним інформаційним простором, який має глобальний, міжнародний характер. Інтернет – це єдиний інформаційний простір, у якому

¹⁵ Про цифровий контент та цифрові послуги: Закон України від 10.08.2023р.

¹⁶ Єфремова К. В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспект. Право та інноваційне суспільство. 2014. № 1. С. 5–11.

відбуваються глобальні процеси соціальних комунікацій та якому притаманний всесвітній загальний характер доступу»¹⁷.

Одне з перших законодавчих визначень поняття «Інтернет» було 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.

Варто зазначити, що Організація Об'єднаних Націй (далі – ООН) визнає право на доступ до Інтернету одним з невід'ємних прав людини. Ця позиція відображена в резолюції Ради з прав людини ООН про право на свободу вираження поглядів в Інтернеті від 5 липня 2012 року. Резолюція закликає всі держави «заохочувати і підтримувати міжнародне співробітництво з метою сприяння доступу до Інтернету і розвитку засобів масової інформації та комунікацій у всіх країнах». Регламент ЄС про відкритий доступ до Інтернету (2015/2120) зазначає, що: «Інтернет розвивався як відкрита платформа для інновацій з низькими бар'єрами доступу для кінцевих користувачів, постачальників контенту, програм і послуг, а також постачальників послуг доступу до Інтернету».¹⁸

У Законі України «Про електронні комунікації»¹⁹ 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, в основу наведеного поняття законодавець покладає технічний критерій, тоді як соціальне значення мережі Інтернет залишається поза його увагою. Майже так саме в літературі та законодавстві розділяють і види правовідносин, що відбуваються в сфері регулювання мережі Інтернет. А саме: 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.

Розглядаючи види інформаційної діяльності, які проводяться в межах або за допомогою мережі Інтернет, потрібно звернути уваги на їхню неоднорідність. Саме тому необхідно виділяти відносини що, *пов'язані функціонуванням мережі Інтернет* і суспільні відносини, що *виникають у зв'язку з використанням* цієї глобальної комп'ютерної мережі. В науковій літературі під **Інтернет-відносинами** розуміють суспільні відносини в кіберпросторі, учасники яких є носіями суб'єктивних прав і обов'язків у мережі Інтернет. Інтернет-відносини – це особливі суспільні відносини, що виникають у результаті впливу норм інформаційного, комп'ютерного, міжнародного й інших галузей права, міжнародних договорів на поведінку суб'єктів

¹⁷ Еннан, Р. Поняття, ознаки, сутність, специфіка та види відносин у мережі Інтернет //Теорія і практика інтелектуальної власності. 2013. № 3. С. 10–19. - Режим доступу:http://nbuv.gov.ua/UJRN/Tpiv_2013_3_3

¹⁸ REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG&toc=OJ:L:2015:310:TOC

¹⁹ Про електронні комунікації Закон України від 16.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

цих відносин. Інтернет-відносини – це новий тип суспільних відносин, які виникають, змінюються та припиняються в кіберпросторі. Це не лише правові, фактичні, етичні відносини, це складні соціальні зв'язки особливої правової, інформаційної та технічної природи.

Інтернет-правовідносини можна класифікувати за такими ознаками:

1. Залежно від суб'єктів: між розробниками інформаційних мереж і їхніми партнерами; між спеціалістами, які створюють (виробляють) і розповсюджують інформацію в Інтернеті; між інформаційними провайдерами, які надають ліцензії на здійснення он- лайнових послуг; між громадянами, організаціями, фірмами й іншими споживачами (користувачами);

2. Залежно від державної приналежності фізичних і юридичних осіб: між вітчизняними й іноземними провайдерами; між іноземними провайдерами та вітчизняними користувачами; між вітчизняними юридичними особами й іноземними громадянами; між вітчизняними та іноземними розробниками мереж; між фахівцями;

3. Залежно від мети виникнення відносин та інформаційного впливу: внутрішні відносини (відбуваються в кіберпросторі); зовнішні відносини (пов'язані з наданням зовнішніх інформаційних послуг)²⁰.

До **суб'єктів** Інтернет-правовідносин відносять:

1) операторів та провайдерів телекомунікацій, що забезпечують функціонування мережі Інтернет як інформаційної системи;

2) виробників, власників й розповсюджувачів інформації та інформаційних ресурсів, які створюють інформаційне наповнення мережі Інтернет;

3) суб'єктів, котрі надають специфічні послуги з укладання електронних (мережевих) угод (договорів) за допомогою мережі Інтернет, тобто все те, що охоплюється терміном «електронна комерція (торгівля)»;

4) споживачів (користувачів) телекомунікаційних послуг.

2.2. 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

²⁰ Еннан, Р. Поняття, ознаки, сутність, специфіка та види відносин у мережі Інтернет // Теорія і практика інтелектуальної власності. 2013. № 3. С. 10–19. - Режим доступу: http://nbuv.gov.ua/UJRN/Tpiv_2013_3_3

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»²¹. 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»²². 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 Інтернетмережі. 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 IANA²³. 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 корпорації ICANN відповідним країнам. В більшості випадків – це організації самоуправління, що діють відповідно до

²¹ Новицький, А.М. Міжнародний досвід правового регулювання Інтернет. Юридичний вісник. Повітряне і космічне право. 2014. No 2. С. 52–58.

²² Barlow J. A Declaration of the Independence of Cyberspace / John Perry Barlow // February 8, 1996 from Davos, Switzerland

²³ Internet Assigned Numbers Authority (IANA). URL: <https://www.iana.org/>

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?

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 мережеских адрес і зрозумілих людині імен в спеціальному файлі. Отже, користувач вводив ім'я потрібного йому комп'ютера, а комп'ютер дивився в файл, 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)²⁴ (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.

²⁴ Postel, J. RFC1591: Domain Name System Structure and Delegation.: RFC Editor. United States. 1994. URL: <https://dl.acm.org/doi/10.17487/RFC1591#cited-by-sec>

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»²⁵, 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 подолати 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 кирилических 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.

3.2. Правове регулювання 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-адресу²⁶ [19].

Правове положення доменів визначається правилами Інтернет-корпорації з присвоєння імен та номерів (Internet Corporation For Assigned Names and Numbers, далі – ICANN) та низкою вітчизняних нормативно-правових актів. На сьогодні, це насамперед Закон України «Про використання доменних імен у спеціальному публічному імені .gov.ua». від 28.07.2023 № 3284-IX. Цей Закон визначає правові та організаційні засади використання доменних імен у спеціальному публічному домені gov.ua органами місцевого самоврядування та підприємствами, установами організаціями державної форми власності. Відповідно до ст. 1 ч. 1 п. 7 зазначеного Закону: «доменне ім'я – унікальна назва, що ідентифікує домен та складається з символічного позначення, що використовується в адресному просторі Інтернет»²⁷.

Також правовий статус доменного імені певною мірою визначено Законами України "Про охорону прав на знаки для товарів і послуг", Законом України «Про електронні комунікації» через поняття доменного імені (домену).

Так, згідно зі ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг», **доменне ім'я** – це ім'я, яке використовується для адресації комп'ютерів і ресурсів в Інтернеті, а у п. 22 ч. 2 ст. 2 Закону України «Про електронні комунікації»,

²⁵ Офіційний сайт ТОВ «Хостмастер». <https://www.hostmaster.ua/>

²⁶ 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. (Ірпін, 28 листопада 2019 р.). Ірпін : Університет державної фіскальної служби України, 2019. С. 93–96.

²⁷ Закон України «Про використання доменних імен у спеціальному публічному імені .gov.ua». від 28.07.2023 № 3284-IX. <https://zakon.rada.gov.ua/laws/show/3284-IX#Text>

надається поняття домену, а саме: **«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»²⁸.**

Виходячи із зазначених вище легальних понять домену та доменного ім'я, можемо визначити їх співвідношення, тобто **домен – це частина ієрархічного адресного простору мережі Інтернет, а доменне ім'я його унікальна назва, що відрізняє його від інших доменів.**

Заслуговує уваги також «Регламент публічного домену» від 24 січня 2020 року, що був розроблений спільно ТОВ «Хостмайстер», адміністраторами публічних доменів та реєстраторами визначає *Домен* як символічне позначення областей в мережі Інтернет, що базується на ієрархічній структурі, що дозволяє визначити доменні імена, а *Доменне ім'я* як символічне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (вебсайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі²⁹.

В свою чергу «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».

В науковій літературі дискусійні питання щодо юридичної природи домену аналізуються в дослідженнях Н. М. Булата, К. Г. Некіт, Ю. Є. Атаманова, Д. Жуванова, Є. Стогнія, О. Смотров, Р. Смірнова, В.В. Бонтлаба, Д.В. Бойко, А.В. Попцова.

Зокрема Наталія Булат пропонує наступне визначення терміну «доменне ім'я» – це унікальний набір символів, який використовується для адресації комп'ютерів і є засобом індивідуалізації Інтернет-ресурсу³⁰. Науковиця 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 зору науковиці обидві основні функції доменного імені тісно пов'язані одна з одною. З інформаційно-технічного погляду перша функція полягає в адресації ресурсів у мережі. Проте, з позиції права інтелектуальної власності, доменні імена не просто слугують для адресації ресурсів,

²⁸ Про електронні комунікації : Закон України від 16.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

²⁹ Офіційний сайт ТОВ «Хостмастер». URL: <https://hostmaster.ua/policy/2ld.ua/>

³⁰ Булат Н.М. Поняття та ознаки доменного імені. Development of modern technologies and scientific potential of the world : coll. of scientific papers «öööö» with materials of the international scientific-practical conf., London, July 29, 2019. London : NGO «European Scientific Platform», 2019. Vol. 2. 118 p. P. 33–36.

їх роль полягає в індивідуалізації Інтернет-ресурсів, наданні останнім певної унікальності.

Такі науковці як В.В. Бонтлаб³¹, Д.В. Бойко³², аналізуючи правову природу доменного імені, вказують на нього як на засіб адресації інформаційного ресурсу юридичних чи фізичних осіб у кіберпросторі. На їх думку доменне ім'я здійснює ідентифікаційну функцію аналогічну той, що виконують знаки для товарів та послуг (торговельні марки) або комерційні (фірмові) найменування для користувачів цими товарами або послугами. Така подібність функціоналу названих об'єктів не могла не призвести до виникненню певних правових колізій. Вчені дійшли до висновку, що для усунення цих колізій необхідно розмежування правового режиму охорони знаків для товарів і послуг (торгівельних марок) і доменних імен.

Як самостійний об'єкт права інтелектуальної власності доменне ім'я у законодавстві про інтелектуальну власність не визначається. Зокрема, у Законі України «Про охорону прав на знаки для товарів і послуг», законодавець визначає доменне ім'я тільки як *один із способів використання знаку для товарів і послуг (торгової марки)*. У п. 4 ст. 16 Закону прописано, що: «Використанням знаку визнається його використання, в тому числі, в Інтернет». Виходячи з цього положення, знак для товарів і послуг (торговельна марка) та доменне ім'я ототожнюються як об'єкти інтелектуальної власності, що індивідуалізують учасників цивільного (господарського) обороту. Різниця між ними полягає тільки в тому, що перші ідентифікують певні товари, послуги виконання роботи у реальному світі, а другі – у віртуальному. Але з такою позицією законодавця складно погодитись з огляду на те, що ці об'єкти можна розмежувати як за середовищем їх застосування, так і за правовою природою. По-перше, товарні знаки (торговельні марки) є дійсними тільки на території їх реєстрації, доменним же іменам (як й іншим об'єктам інтелектуальної власності, що використовуються у кіберпросторі) притаманна транскордонність.

По-друге, знаки для товарів і послуг (торговельні марки) використовуються суб'єктами приватного права (фізичними та юридичними особами) для їх ідентифікації у цивільному (господарському) обороті. А доменні імена поділяються за їх призначенням на дві категорії: публічні, тобто ті, що адмініструються в інтересах громадськості; приватні, тобто такі, що адмініструються певною особою в своїх власних інтересах.

По-третє, у цих об'єктів різне позначення. Так, відповідно до ст. 5 Закону України «Про охорону прав на знаки для товарів і послуг» та ст. 492 ЦКУ у якості товарного знаку (торговельної марки) можуть використовуватися будь-які позначення чи комбінація позначень, зокрема слова, у тому числі власні імена, літери, цифри, зображувальні елементи, кольори та комбінація кольорів. А у якості доменних імен може мати місце буквено-цифровий вираз, що ідентифікує будь-який комп'ютер абонента у мережі Інтернет, тобто використовується лише буквено-цифрова послідовність символів з певною довжиною, зокрема (до 63 символів).

Відсутність чіткої правової ідентифікації доменних імен призвела до так званого кіберсквоттингу (від англ. Cybersquatting – піратство, захоплення) або

³¹ Бонтлаб В. В. Цивільно-правове регулювання доменних імен : автореф. дис...канд. юрид. наук. Київ, 2006. 20 с.

³² Бойко Д. В. Правова природа доменних імен Інтернет : автореф. дис... канд. юрид. наук. Харків, 2005. 19 с

киберзахоплення доменних імен недобросовісними суб'єктами, що використовують їх у подальшому для власних комерційних цілей. У ч. 2 ст. 20 Закону України «Про охорону прав на знаки для товарів і послуг» зазначено, що порушенням прав власників свідоцтва (що є охоронним документом права інтелектуальної власності для власника знаку для товарів та послуг (торгівельної марки)) вважається використання без їх згоди в доменних іменах знаків і позначень відповідно до п. 5 ст. 16 цього ж Закону. Однак ця норма надає можливість власникам знаків для товарів і послуг відстоювати свої інтелектуальні права, встановленими законодавством способами, але не враховує інтереси власників доменних імен.

Заслугує уваги наукова позиція В.В. Бонтлоба про необхідність створення доменного законодавства, а саме: прийняття Закону «Про доменні імена» і доповнення ЦКУ окремою главою що врегулює правові аспекти виникнення прав на доменні імена та зміст прав володільців доменних імен.

Таким чином, наразі неможливо точно схарактеризувати правову природу прав на доменне ім'я. Досі існують різні точки зору щодо цього питання, тому пролонгуються дискусії щодо того, чи слід вважати доменне ім'я майном, і, відповідно, об'єктом права власності, чи це є об'єкт права інтелектуальної власності. 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 імен³³.

Частина юристів вважає, що оскільки права на доменне ім'я виникають на підставі договору з відповідним реєстратором і в рамках умов такого договору, то доменне ім'я – всього лише послуга реєстратора за укладеним договором. У науковій літературі 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». За цими правилами 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 домену³⁴, 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).

³³ Некіт К. Г. Доменне ім'я як об'єкт цивільних прав. Часопис цивілістики. 2017. Вип. 23. – С. 40-44.

³⁴ Регламент публічного домену (версія 3.5), вступив у дію з 24 січня 2020 року. https://www.hostmaster.ua/policy/Reglament2ld_3.5_UK.pdf

Прихильники процедурного підходу обґрунтовують свою позицію тим, що права і обов'язки щодо використання доменного імені виникають в рамках відповідного договору за яким 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:

- період фактичної реєстрації (Registered);
- період автоматичного продовження (Auto Renew Grace Period);
- період відновлення домену після видалення (Redemption Grace Period);
- 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: «Реєстрація доменного імені не має статусу торгової марки».

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 неможливо³⁵.

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**.

³⁵ Булат Н. М. Доменне ім'я як засіб індивідуалізації інтернет-ресурсів. Право і суспільство. № 2 / 2020. С. 154-160.

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:

- право на використання доменного імені;
- виключне право дозволяти використання доменного імені;
- виключне право перешкоджати неправомірному використанню доменного імені, у тому числі забороняти таке використання;
- право делегувати домени нижчого рівня у своєму доменному імені;
- 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 законом³⁶.

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 норм³⁷.

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;

³⁶ 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.

³⁷ Доменні спори: українська й міжнародна актуальна практика. Юрист & Закон, 2019, №38. Електронне видання. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013152.

- 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 власник торгівельної марки може 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 перепорою для подання заяви до BOIB 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 два 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)³⁸. 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.

³⁸ UDRP спір та UDRP правила. Допоможе юрист? URL: https://legalitgroup.com/domenni-batli-worldwide/?gclid=Cj0KCQiA8vSOBhCkARIsAGdp6RQnHZjnInvaep0Gk89OhsBVyEwzmI5doJAEN18kOr8xRTLY4IBR6e8aAvtjEALw_wcB

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. 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 цивільноправового 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»).

Юристи-практики зазначають, що 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 врегулювання³⁹.

Можливі способи захисту:

- *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.

- *Делегування.* Це процес надання можливості правоволодільцю торговельної марки користуватися доменним іменем (тобто передача права користування доменом від реєстранта до власника ТМ).

³⁹ Пономарьов М. Узагальнення судової практики розгляду судами справ у спорах, пов'язаних із використанням імен доменів. URL: <http://artimmer.com/ua/publicacii/uzagalnennyasudovoi-praktyky/269-uzagal%60nennya-sudovo%D1%97-praktikirozglyadu-sudami-sprav-u-sporax,-pov-yazanix-%D1%96zvikoristannyam-%D1%96men-domen%D1%96>.

- Заборона використання у доменному імені знаку чи комерційного найменування. Але цікавіше його тотальна (або, як пишуть науковців, прогібаторна) 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?

РОЗДІЛ 4. ОХОРОНА ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ЦИФРОВОМУ СЕРЕДОВИЩІ

4.1. Охорона авторських і суміжних прав в мережі Інтернет

Авторське право і суміжні права – це один з правових інститутів в системі права інтелектуальної власності. Правова регламентація у сфері авторського права і суміжних прав забезпечується на міжнародному рівні Бернською конвенцією про охорону літературних та художніх творів (1886 р.), Римською конвенцією про охорону інтересів артистів-виконавців, виробників фонограм, відеограм і організацій мовлення та окремими договорами і директивами Всесвітньої Організації Інтелектуальної Власності (ВОІВ), що стосуються охорони об'єктів авторського права і суміжних прав в цифровому середовищі (мережі Інтернет). В Україні правове регулювання цієї сфери здійснюється Цивільним кодексом України (глави 36, 37) (далі – ЦКУ), Законом України «Про авторське право і суміжні права» від 01.12.2022 р., який вступив у силу 01.01.2023 р. (далі – Закон) тощо. Необхідно зазначити, що законодавство про авторське право і суміжні права в Україні, навіть під час воєнного стану, потребувало змін з оглядом на євроінтеграційні процеси у державі та активний розвиток технологій, що вимагало приведення чинних норм у відповідність до сучасних реалій. Попередній Закон України «Про авторське право і суміжні права», прийнятий у 1993 році, пережив 15 редакцій і вже не міг слугувати потужним правовим підґрунтям для вирішення накопичених проблем у силу втрати своєї актуальності.

В *об'єктивному розумінні* авторське право являє собою сукупність норм, які регулюють суспільні відносини щодо створення, використання та охорони творів літератури, науки, мистецтва та інших об'єктів, що за своїм правовим режимом дорівнюють до творів. Твір відповідно до п. 56 ст. 1 Закону – це оригінальне творіння автора (авторів) у сфері науки, літератури, мистецтва тощо, виражене в об'єктивній формі. Тобто зазначені твори є об'єктами авторського права і відповідно до ч. 1 ст. 433 ЦКУ і ст. 6 Закону це:

- 1) літературні та художні твори, зокрема романи, поеми, статті та інші письмові твори; лекції, промови, проповіді та інші усні твори; драматичні, музично-драматичні твори, пантоміми, хореографічні, інші сценічні твори; музичні твори (з текстом або без тексту); аудіовізуальні твори; твори живопису, архітектури, скульптури та графіки; фотографічні твори; твори ужиткового мистецтва; ілюстрації, карти, плани, ескізи і пластичні твори, що стосуються географії, топографії, архітектури або науки; переклади, адаптації, аранжування та інші переробки літературних або художніх творів; збірники творів, якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;
- 2) комп'ютерні програми;
- 3) компіляції даних (бази даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;
- 4) інші твори.

Також законодавець визначає у ст. 434 ЦКУ та ст. 8 Закону твори, які не є об'єктами авторського права, а саме: 1) акти органів державної влади та органів місцевого самоврядування (закони, укази, постанови, рішення тощо), а також їх офіційні переклади; 2) державні символи України, грошові знаки, емблеми тощо, затверджені органами державної влади; 3) повідомлення про новини дня або інше факти, що мають характер звичайної прес-інформації; 4) інші твори, встановлені законом.

Твори є об'єктами авторського права без виконання будь-яких формальностей щодо них та незалежно від їх завершеності, призначення, цінності тощо, а також способу чи форми їх вираження (презумпція авторства). Авторське право на твір виникає внаслідок факту його створення. Твір вважається створеним з моменту первинного надання йому будь-якої об'єктивної форми (письмової, речової, електронної (цифрової) тощо (ч. 2 ст. 433 ЦКУ, ч. 1 ст. 9 Закону).

В *суб'єктивному розумінні* авторське право – це інтелектуальні права (особисті немайнові та майнові права, що становлять зміст авторського права відповідно до ч. 1 ст. 5 Закону) автора (авторів), які виникають у них у зв'язку зі створенням об'єкта авторського права (ч. 1 ст. 433 ЦКУ, ст. 6 Закону) або виникають у інших юридичних та фізичних осіб на підставі правочину (договору) або закону (ч. 3 ст. 435 ЦКУ, ч. 2 ст. 5 Закону).

Автор – це фізична особа, яка своєю творчою діяльністю створила твір (п. 56 ч. 1 ст. 1 Закону). Якщо йдеться про авторів, то мається на увазі співавторство, тобто коли спільною співпрацею авторів створено твір або інший об'єкт, який охороняється як твір (комп'ютерна програма, база даних). Правовий режим співавторства прописаний у ст. 436 ЦКУ та ст. 13 Закону.

Автори визначаються у Законі як первинні суб'єкти авторського права (ч. 1 ст. 435 ЦКУ, ч. 2 ст. 5 Закону), вторинними суб'єктами є фізичні та юридичні особи, до яких надійшли майнові права на твір на підставі правочину (договору) або закону (ч. 2 ст. 435 ЦКУ, ч. 2 ст. 5 Закону).

Серед принципів авторського права виділяють наступні: свобода творчості (ст. 41 Конституції України); поєднання особистих інтересів автора з інтересами суспільства; невідчужуваність особистих немайнових прав автора; свобода у розпорядженні майновими правами автора, у тому числі свобода авторського договору; обов'язковість наявності об'єктивної форми вираження об'єкта авторського права; відсутність обов'язкової державної реєстрації авторських прав на об'єкт авторського права (презумпція авторства); незалежність права інтелектуальної власності на об'єкт авторського права від права власності на матеріальний об'єкт; використання твору тільки за згодою автора, окрім випадків правомірного використання твору без такої згоди.

Строк чинності майнових прав інтелектуальної власності на твір за загальним правилом спливає через сімдесят років, що відраховуються з 1 січня року, наступного за роком смерті автора чи останнього із співавторів, який пережив інших співавторів, крім випадків, передбачених законом. Особисті немайнові права суб'єктів авторського права охороняються безстроково (ст. 446 ЦКУ, ст. 31 Закону).

Закінчення строку чинності майнових прав на твір означає перехід твору у суспільне надбання. Твори, які стали суспільним надбанням, можуть вільно, без

сплати винагороди використовуватися будь-якою особою, за умови дотримання особистих немайнових прав автора. Захист особистих немайнових прав на твір, що став суспільним надбанням здійснюється спадкоємцями автора, яким у складі спадкової маси перейшли майнові інтелектуальні права на твір (ст. 32 Закону).

Щодо суміжних прав, то в *об'єктивному розумінні* – це сукупність норм, які регулюють відносини щодо створення, використання та правової охорони таких об'єктів права інтелектуальної власності як: фонограми, відеограми, виконання, передачі (програми) організацій мовлення. Основне правове забезпечення інституту суміжних прав становлять гл. 37 ЦКУ та Розділ III Закону. Виходячи із зазначеного поняття та норм законодавства, об'єктами суміжних прав, незалежно від призначення, змісту, оцінки, способу і форми вираження є: а) виконання літературних, драматичних, музичних, музично-драматичних, хореографічних, фольклорних та інших творів; б) фонограми, відеограми; в) передачі (програми) організацій мовлення (ст. 449 ЦКУ, ст. 35 Закону).

Суміжні права іноді називають новим форматом авторських прав, оскільки створення відповідних об'єктів здійснюється з використанням вже створених об'єктів авторського права.

Суб'єктами суміжних прав є : а) виконавці творів, їх спадкоємці та особи, яким на законних підставах передано суміжні майнові права щодо виконання; б) виробники фонограм, їх спадкоємці (правонаступники) та особи, яким на законних підставах передано суміжні майнові права щодо фонограм; в) виробники відеограм їх спадкоємці (правонаступники) та особи, яким на законних підставах передано суміжні майнові права щодо відеограм; г) організації мовлення та їх правонаступники (ст. 450 ЦКУ, ч. 1 ст. 36 Закону).

Первинними суб'єктами суміжних прав є виконавець, виробник фонограми, виробник відеограми, організація мовлення (ст. 450 ЦКУ, ч. 1 ст. 37 Закону). Інші особи (спадкоємці або правонаступники) є по суті вторинними суб'єктами суміжних прав та отримують інтелектуальні права на підставі правочину або закону. Суб'єктам суміжних прав притаманні визначені законодавцем особисті немайнові та майнові права (ст. 452 ЦКУ, статті 38-41 Закону).

Суміжне право виникає внаслідок факту виконання твору, виробництва фонограми, виробництва відеограми, оприлюднення організації мовлення. Для виникнення і здійснення суміжних прав не вимагається виконання будь-яких формальностей (тобто мається на увазі автоматичне виникнення суміжних прав без дотримання процедури їх державної реєстрації за відсутності доказів, що створили відповідні об'єкти саме ті особи, імена (назви) яких зазначені на фонограмі, відеограмі та їх примірниках або зазначена певна організація мовлення та виконавець (виконавці)) (ст. 451 ЦКУ, частини 2,3 ст. 37 Закону) (презумпція авторства).

Строк чинності майнових суміжних прав на виконання, фонограму, відеограму, фонограму, програму мовлення спливає через 50 років, що обчислюються з 1 січня року, наступного за роком здійснення виконання, вироблення фонограми, відеограми, трансляції програми мовлення. Якщо запис виконання, фонограму, відеограму та здійснено трансляцію програми мовлення оприлюднено правомірно, строк чинності на об'єкти суміжних прав спливає через

50 років, що обчислюються з 1 січня року, наступного за роком такого оприлюднення. Особисті немайнові права первинних суб'єктів суміжних прав охороняються безстроково (ст. 456 ЦКУ, ст. 45 Закону). Закінчення строку чинності майнових прав на об'єкти суміжних прав означає їх перехід у суспільне надбання, що передбачає можливість вільного та безоплатного використання. (ст. 46 Закону).

Всі вищевказані об'єкти авторського права і суміжних прав на сьогодні активно використовуються у цифровому середовищі, зокрема у мережі-Інтернет. У п. 65 ч. 1 ст. 1 Закону прописано поняття **цифрового контенту** (електронна (цифрова) інформація) – будь-які відомості чи дані в електронній (цифровій) формі, що містять об'єкти авторського права та/або суміжних прав і можуть зберігатися та/або поширюватися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі Інтернет.

Мережа Інтернет вже давно стала невід'ємною частиною сучасного життя. Однак використання її ресурсів передбачає наявність певних правил, які виходять із законодавства. У користувачів Інтернет виникає хибне уявлення про можливість безконтрольного використання різноманітного контенту, що призводить, зокрема, до порушення авторського права і суміжних прав. Таке явище виникає дуже часто у сьогоднішньому інформаційному світі з притаманною йому віртуалізацією суспільних відносин.

Інтернет-технології дозволяють завантажувати, зберігати, поширювати різні види інформації, в тому числі об'єкти, які охороняються правом інтелектуальної власності. Але часто об'єкти права інтелектуальної власності потрапляють до мережі Інтернет без згоди й навіть поза межами обізнаності автора. Це призводить не тільки до порушення права автора на отримання винагороди за свій інтелектуальний труд, а й на 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 інтелектуальних прав авторів та інших правоволодільців⁴⁰. Тому, враховуючи особливості правової природи об'єктів права інтелектуальної власності та особливості Інтернету, який має глобальні та цифрові характеристики, пріоритетним завданням законодавця є адаптація національного законодавства до реалій цифрової епохи. Правове регулювання відносин інтелектуальної власності має враховувати їх віртуалізацію, в тому числі і через використання мережі Інтернет та забезпечувати ефективну охорону інтелектуальних прав суб'єктів відповідних відносин.

4.2. Комп'ютерна програма як об'єкт правової охорони

Комп'ютерна програма (далі – КП) 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

⁴⁰ Новосельська І. В., Бобровник А. С. Теоретико-правові питання охорони авторського права в мережі інтернет. URL: <https://dilegal.ua/teoretiko-pravovi-pitannya-oxoroni-avtorskogoprava-v-merezhi-internet/>

судової практики показує, що вона зазнає найбільшого впливу від правопорушень, що обумовлено суттєвою різницею між витратами ресурсів на створення КП та витратами на їх незаконне копіювання та розповсюдження. Крім того, комп'ютерним програмам, поряд з доменним іменем та веб-сайтом, притаманно використання тільки через Інтернет-ресурс, що передбачає особливості її правової охорони як об'єкта права інтелектуальної власності.

Інтеграція програмного забезпечення (КП) 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.

Відповідно до положень Бернської конвенції про охорону літературних та художніх творів, **комп'ютерна програма** визначається об'єктом авторського права. Тому всі країни-учасниці цієї конвенції мали внести відповідні положення про правовий статус КП у національне законодавство.

Згідно з п. 26 ч.1 і ст.1 Законом України «Про авторське право і суміжні права» **Комп'ютерна програма (КП)** – це набір інструкцій у вигляді слів, цифр, кодів, схем, символів або у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером (настільним комп'ютером, ноутбуком, смартфоном, ігровою приставкою, смарт-телевізором тощо), які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражену у вихідному або об'єктному коді). У ст. 18 Закону прописано, що комп'ютерні програми охороняються як літературні твори. Така охорона поширюється на КП незалежно від способу або форми її вираження.

Вибір ефективної системи правової охорони КП в Україні є дискусійним питанням у зв'язку з тим, що вона є складним комплексним об'єктом.

Постає цікаве питання: чому законодавець поєднав охорону літературних творів та комп'ютерних програм? Існує кілька неофіційних пояснень, одне з яких свідчить про те, що відповідно до норм авторського права захищається форма, в якій втілені ідеї автора⁴¹.

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), аудіовізуального, твору

⁴¹ Водорезова С. Р. Особливості правової охорони комп'ютерної програми як об'єкта інформаційних відносин. Право та інновації. № 3 (7) 2014. С. 69-76.

образотворчого мистецтва, твору, виконаного способами, подібними до фотографії, художнього твору, що також дає підстави віднести їх до творів у галузі мистецтва⁴².

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 впливає 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 погодитися⁴³.

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.

⁴² Філік Н. В., Омельченко Г. В. Комп'ютерна програма як об'єкт авторського права: проблеми правової охорони. Юридичний вісник. №2 (39). 2016. С. 130-137.

⁴³ Жуванов Д. Яку форму правової охорони обрати для комп'ютерної програми. URL:http://www.romanenko.biz/ua/library/article_program.html.

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 коду, об'єктного коду, 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, алгоритми⁴⁴.

Також є важливим питання щодо використання для правової охорони КП принципу «презумпції авторства», який використовується в сфері авторського права, зокрема, щодо автоматичного визнання інтелектуальних прав на комп'ютерну програму як об'єкта авторського права без обов'язкової державної реєстрації у Національному органі інтелектуальної власності (далі – НОІВ). Практика підтверджує, що однієї «презумпції авторства» для потужного захисту КП 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.

⁴⁴ Водорезова С. Р. Особливості правової охорони комп'ютерної програми як об'єкта інформаційних відносин. Право та інновації. № 3 (7) 2014. С. 69-76.

Разом з тим велика кількість авторів комп'ютерних програм не звертаються до НОІВ 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 вказують науковці, комп'ютерна програма нерідко створюється колективом авторів (співавторів), 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 програми⁴⁵.

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 як відтворення екранних заставок (screen displays). Суттєвий недолік авторської охорони полягає в неможливості запобігти створенню конкуруючої комп'ютерної програми з використанням ідеї наявної програми.

З урахуванням всіх переваг та недоліків щодо здійснення правової охорони КП інститутом авторського права, на думку фахівців слід реєструвати окремі елементи комп'ютерних програм та захищати її не тільки авторським правом, а також певними інститутами права промислової власності, що забезпечуватиме комплексний підхід до правової охорони КП, який передбачає:

- реєстрацію самого коду КП як об'єкта авторського права;
- реєстрацію алгоритму роботи КП шляхом отримання патенту України на корисну модель або патенту на винахід як на спосіб (процес);
- реєстрацію назви КП – як торговельної марки;
- реєстрації графічного інтерфейсу КП – як промислового зразка;

Отже, на сьогодні 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

⁴⁵ Тарасенко Л. Л. Комп'ютерна програма як об'єкт інтелектуального права // Матеріали Міжнародної наукової конференції (круглий стіл) на тему «ІТ-право: проблеми і перспективи розвитку в Україні» у м. Львів, 18 листопада 2016 р. URL: <http://aphd.ua/it-pravo-problemy-i-perspektyvy-rozvytku-vukrani-14/>

визнана об'єктом патентної охорони). 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, яка передбачає видачу програмних патентів як охоронних документів інтелектуальних прав на КП. 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. Правознавці вважають такий підхід цілком обґрунтованим, оскільки, якщо розглядати КП як частину винаходу (корисної моделі), патентне право захищає її функціональну сутність, а не кінцевий результат, як у випадку захисту авторським правом.

Фахівці вважають, що у сфері патентних відносин КП як самостійний об'єкт права інтелектуальної власності не є технічним рішенням та не відповідає умовам патентоспроможності, які притаманні винаходу (корисній моделі) (ст. 7 Закону «Про охорону прав на винаходи і корисні моделі»), але зазначений об'єкт може отримати патентну охорону у складі технічних рішень, в яких використовується. За певних обставин алгоритм роботи КП може отримати патентну охорону шляхом отримання патенту, як невід'ємна частина винаходу (корисної моделі), запатентована як спосіб (процес) (ч. 1 ст. 6 Закону України «Про охорону прав на винаходи і корисні моделі»).

Патент на винахід дає змогу захистити змістовий бік програмного забезпечення, патентна охорона поширюється на сутність, що є основною ідеєю програми, втіленою в алгоритмі. Таким чином, 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. 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.

Реєстрація назв програм і сайтів, як торговельних марок у НОІВ може стати дієвим механізмом уникнення повного або ж часткового копіювання вже наявного якісного продукту у вигляді КП. 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. Як знак для товарів і послуг можуть охоронятися КП або їх окремі модулі і в цьому випадку назва КП або її модулів можуть бути зареєстровані відповідно до Закону України «Про охорону прав на знаки для товарів і послуг».

Коли ж йдеться про зовнішній вигляд програми, її **графічний інтерфейс**, то додаткову правову охорону КП може отримати як промисловий зразок, порядок державної реєстрації якого визначається Законом України «Про охорону прав на промислові зразки».

Слід також зазначити, що робочі матеріали стосовно КП, що застосовуються під час її розроблення, сам код КП можуть зберігатися певною юридичною особою як

комерційна таємниця та підлягати правовій охороні, що відповідає правовому режиму охорони інтелектуальних прав на комерційну таємницю (глава 46 ЦКУ).

Таким чином, можна дійти до висновку, що норми інституту авторського права у недостатньому ступені здатні забезпечувати потужну правову охорону інтелектуальних прав на КП. Доцільно використовувати можливість охорони цих прав з боку різних інститутів системи права інтелектуальної власності. На думку фахівців, віднесення комп'ютерних програм до об'єктів промислової власності буде сприяти розвитку ІТ-індустрії і поширенню програмного забезпечення⁴⁶.

Унікальним явищем у сфері комп'ютерних технологій на сьогодні визнається **штучний інтелект** (далі – ШІ) (Artificial Intelligence), який по суті є програмним продуктом (тобто КП). Деякі фахівці у сфері ІТ вважають його вдосконаленим форматом Комп'ютерної програми. Мова йде про робототехніку, перспективи її розвитку та значення для людства. Тому актуальним на сьогодні є питання правової регламентації у цій сфері.

Місце ШІ у правовій площині є важливою темою юридичного дискурсу. Перші дослідження та заходи, присвячені різним аспектам ШІ, розпочалися ще у 1970–1980 рр., але на офіційному рівні здійснюються лише перші кроки у цьому напрямку. Розроблення правових стандартів щодо ШІ провадиться в країнах Східної Азії та США, а також Європейським Союзом. Так, Європейський Парламент ухвалив 16 лютого 2017 р. Резолюцію 2015/2103 (INL) щодо цивільно-правового регулювання робототехніки з рекомендаціями для Європейської Комісії⁴⁷. Цей документ має назву «Норми цивільного права про робототехніку» і є одним із перших реальних кроків на шляху до законодавчого закріплення стандартів розроблення та використання штучного інтелекту, але Резолюція має винятково рекомендаційний характер, її положення дають можливість сформулювати уявлення про те, що буде лежати в основі норм, які регламентують відповідну діяльність у найближчій перспективі.

Для України аналіз змісту цієї Резолюції є важливим з урахуванням того, що курс нашої держави спрямований на європейську інтеграцію, тому вочевидь, що саме стандарти Європейського Союзу в цій сфері будуть покладені в основу відповідних норм українського законодавства у майбутньому.

Так, 2 грудня 2020 р. Кабінет Міністрів України видав розпорядження «Про схвалення Концепції розвитку штучного інтелекту в Україні», де термін «штучний інтелект» використовується в такому значенні: **штучний інтелект** – організована сукупність інформаційних технологій, із застосуванням якої можна виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань. Галуззю штучного інтелекту у зазначеній Концепції визначається напрям діяльності у сфері інформаційних технологій, який забезпечує створення, впровадження та використання технологій штучного інтелекту.

⁴⁶ Там же.

⁴⁷ European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. Режим доступу: URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>.

Важливою світовою подією, пов'язаною з розвитком та можливими наслідками активного використання ШІ, було підписання у листопаді 2023 року так званої «Декларації Блетчлі» (Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023), яка визначила принципові положення щодо безпеки та етики подальшого створення та використання технологій ШІ⁴⁸. Для підписання зазначеного документу на Саміті безпеки ШІ, що відбувся у Великій Британії, зібралися представники 28 країн світу. У заході взяли участь представники урядів США, Японії, Австралії, країн ЄС, КНР, Бразилії, Ізраїлю, Південної Кореї, Туреччини, України та інші. «Декларація Блетчлі» символізує спільні зусилля між націями для створення рамок, які гарантуватимуть, що технології ШІ розроблятимуться та використовуватимуться відповідально та безпечно по всьому світу. «Декларація Блетчлі» не є нормативним актом, вона пропонує співпрацю країн щодо регламентації безпеки використання ШІ. Тобто створення підвищених глобальних стандартів безпеки щодо управління ризиками ШІ. Так, в цьому документі визначаються основні принципи, що є результатом колективного консенсусу 28 країн, які окреслюють спільне бачення сприяння безпеці та етичним міркуванням у розробці та розгортанні ШІ, а саме:

- сприяння міжнародній співпраці для навігації в складному ландшафті безпеки ШІ. Необхідність створення єдиного фронту для вирішення проблем і використання можливостей, які надає ШІ на глобальній арені;
- визначення спільних зобов'язань щодо зниження ризиків, пов'язаних із ШІ, і забезпечення того, щоб ці технології розроблялися з підходом до безпеки;
- дотримуватися моральних засад (етики використання ШІ), що передбачає ставлення з повагою до прав людини, сприяння орієнтованому на людину підходу до ШІ;
- прозорість та підзвітність щодо створення і використання ШІ;
- заохочення та обмін знаннями з приводу досягнення технологій ШІ, що спрямовано на прискорення глобального розуміння та пом'якшення ризиків, пов'язаних зі ШІ, сприянню культурі спільного навчання та постійному вдосконаленню практик безпеки ШІ.

Слід зазначити, що прем'єр-міністр Великої Британії, що була ініціатором Саміту, назвав декларацію «знаковим досягненням», яке свідчить про готовність найбільших світових держав в галузі ШІ до спільної відповідальності за майбутнє людства. Водночас вони прагнуть використовувати потенціал ШІ для покращення життя людей, економічного зростання та соціального прогресу.

Враховуючи участь України в Саміті та підписанні Декларації, перед національним законодавцем постала необхідність в правовому регулюванні використання ШІ. Так вперше було врегульовано авторські права на результати використання ШІ. Національний Закон «Про авторське право і суміжні права» не наділив авторськими правами Штучний Інтелект. Однак, на неоригінальні об'єкти згенеровані ШІ, відповідно до ст. 33 Закону, поширюється правовий режим так званого права «*sui generis*» - своєрідний, єдиний у своєму роді Цей термін походить

⁴⁸ . Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 Published 1 November 2023. URL: The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 – GOV.UK (www.gov.uk)

від латинської та означає унікальність правової конструкції (акту, статусу, закону тощо), яка, незважаючи на наявність схожості з іншими подібними конструкціями, в цілому не має прецедентів. Формула «*sui generis*» використовується у різноманітних дисциплінах для позначення всього унікального у своєму роді, що не входить у звичайні параметри речей цього виду. *Sui generis у праві* – це юридичне поняття, яке застосовується до будь-якої справи, яка через свою унікальність вимагає особливого та унікального тлумачення органом влади. Так, у ст. 3 Закону «Про авторське право і суміжні права» вказано, що його положення «спрямовані на охорону та захист особистих немайнових і майнових прав інтелектуальної власності, в тому числі суб'єктів права особливого роду (*sui generis*) на неоригінальний об'єкт, згенерований комп'ютерною програмою».

Отже, ч. 1 ст. 33 Закону «Про авторське право і суміжні права» визначає, що неоригінальним об'єктом, згенерованим КП, є об'єкт, який відрізняється від існуючих подібних об'єктів та утворений в результаті функціонування КП без посередньої участі фізичної особи в утворенні цього об'єкта. Твори, створені фізичними особами з використанням комп'ютерних технологій, не вважаються неоригінальними об'єктами, згенерованими КП. Відповідно до ч. 3 ст. 33 Закону «Про авторське право і суміжні права» у результаті утворення неоригінального об'єкта, згенерованого КП, особисті немайнові права не виникають, а згідно з ч. 4 ст. 33 цього нормативного акту обсяг майнових прав суб'єкта права особливого роду (*sui generis*) на неоригінальний об'єкт, згенерований КП, визначається ст. 12 Закону, в якій прописані майнові права інтелектуальної власності на твір. Тобто зміст цієї норми поширюється на авторів та інших правовласників КП, яка згенерувала неоригінальний об'єкт і передбачає, що вони можуть використовувати, створений ШІ твір, надавати дозвіл на його використання, передавати права на використання, продавати тощо. Таким чином, зазначені суб'єкти, мають такі самі майнові права інтелектуальної власності як і автор будь-якого, створеного особисто ним твору або правовласник, який отримав майнові інтелектуальні права за правочином (договором) або законом. Право особливого роду (*sui generis*) на неоригінальний об'єкт, згенерований КП, спливає через 25 років, що обчислюються з 1 січня року, наступного за роком, в якому згенеровано неоригінальний об'єкт (ч. 5 ст. 33 Закону). Строк чинності права особливого роду (*sui generis*) на неоригінальний об'єкт, згенерований КП, спливає через 25 років, що обчислюються з 1 січня року, наступного за роком, в якому згенеровано неоригінальний об'єкт (ч. 6 ст. 33 Закону).

4.3. 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 законодавець затвердив значно пізніше, і на сьогодні у новому Законі «Про авторське право і суміжні права» в п. 5. ч. 1 ст.1 зазначається, що **веб-сайт – це сукупність даних, електронної (цифрової) інформації, зокрема об'єктів авторського права і (або) суміжних прав тощо, пов'язаних між собою і структурованих у межах адреси веб-сайту та (або) облікового запису власника такого веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики та (або) числової адреси за Інтернет-протоколом.** З аналізу цього визначення стає зрозумілим, що у новому Законі розширено поняття веб-сайту як на складного структурного об'єкта, що містить невизначену кількість елементів (кожен з яких є об'єктом 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 зокрема об'єктів авторського права і (або) суміжних прав тощо;
- 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»⁴⁹.

В чинному законодавстві на сьогодні відсутня пряма вказівка на приналежність веб-сайту до об'єктів права інтелектуальної власності. Зокрема, у ст. 6 Закону «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. 6 Закону «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 власності⁵⁰.

Більшість фахівців з інтелектуальної власності згодні з тим, що веб-сайт це об'єкт права інтелектуальної власності. Однак питання, до якого правового інституту

⁴⁹ Ю. Атаманова. Захист прав інтелектуальної власності у мережі Інтернет: світовий досвід та вітчизняні перспективи. Право та інновації. 2014 (3).

⁵⁰ В. Борівська, Т. Михайліна. Правовий режим вебсайту та його складників як об'єктів інтелектуальної власності. Підприємництво, господарство і право. №4, 2021. С.5-9.

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, веб-сайт як об'єкт ІТ-права та права інтелектуальної власності – складне явище, яке містить елементи різних правових понять. Його розробка потребує інтелектуальної творчої праці від творця, а функціонування не можливе поза межами Інтернету.

Таким чином, веб-сайт (Інтернет-сайт) може позиціонуватися як 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.

Інформаційне наповнення веб-сайту (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. Інтернет-сайт має доменне ім'я, яке є унікальним. У багатьох випадках використання домену (як назви Інтернет-сайту) є формою 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, насамперед у сфері авторського права і суміжних прав**, 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. Поєднуючи різnorідні за своїм характером об'єкти, веб-сайт має ознаки, що не є

сукупністю ознак його складових частин. За змістом веб-сайт є сукупністю даних, електронної (цифрової) інформації, зокрема об'єктів авторського права і (або) суміжних прав тощо, 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.

4.4. Авторські права на службовий твір та твори, створені за замовленням

Актуальним у сучасних реаліях є питання правової регламентації об'єктів права інтелектуальної власності, створених за трудовим договором та об'єктів створених за замовленням (тобто за умовами цивільно-правового договору). З метою виконання положень Угоди про асоціацію з Європейським Союзом від 16.09.2014 року, правовий режим службових творів та творів, створених на замовлення був оновлений в Законі України «Про авторське право і суміжні права», що вступив в дію з 01.01.2023 р. Угода була важливою не лише в ракурсі європейської інтеграції України, вона містить важливі питання правового регулювання різних правовідносин. зокрема щодо правового регулювання інтелектуальної власності. Так, ч. 4 ст. 181 розділу 9 Угоди містить положення щодо належності виключних майнових прав працівників при створенні службових творів. Зокрема, чітко вказано, що *права на комп'ютерну програму, створену найманим працівником належать роботодавцю*. Питання визначення виключних майнових авторських прав (ВМАП) на службовий твір є дуже важливим, оскільки багато творів, зокрема в сфері ІТ- технологій, створюються як службові твори. Проте роботодавець не завжди добросовісно підходить до визначення належності ВМАП на службовий твір, а це може породжувати багато проблем в майбутньому щодо розпорядження цими правами.

Отже, у ст. 14 Закону «Про авторське право і суміжні права» визначено, що особисті *немайнові авторські права* на службовий твір належать працівникові, творчою працею якого створено такий твір, а *майнові права* на службовий твір переходять до роботодавця з моменту створення службового твору у повному складі, якщо інше не передбачено Законом, трудовим договором (контрактом) або іншим договором щодо майнових прав на твір, укладеним між працівником (автором) і роботодавцем.

Аналогічні правила поширюються і на твори, створені за договором замовлення (тобто за умовами цивільно-правового договору). При цьому, Закон не забороняє сторонам домовлятися про умови розподілу інших інтелектуальних майнових прав (ст. 14 «Авторське право на службовий твір», ст. 15 «Авторське право на твір, створений за замовленням»).

Автор службового твору має право на винагороду (ч. 2 ст. 14 Закону) якщо інтелектуальні майнові права на твір переходять до роботодавця. Але, якщо посадові обов'язки працівника прямо передбачають створення службових творів відповідних видів, авторська винагорода може бути включена до заробітної плати працівника згідно із договором між працівником і роботодавцем. Відповідно до ч. 3 ст. 15 Закону автор твору, створеного за замовленням також має право на винагороду, якщо інтелектуальні майнові права переходять до замовника.

Закон не є категоричним щодо недоторканості службового твору та твору, створеного за замовленням. Так у ч. 3 ст. 14 Закону визначається, що роботодавець

має право доручити іншій особі завершити незавершений службовий твір, вносити зміни у завершений службовий твір, супроводжувати службовий твір ілюстраціями, передмовами, післямовами тощо, якщо інше не передбачено трудовим договором (контрактом) або іншим договором щодо майнових прав на службовий твір. Згідно з ч. 4 ст. 15 Закону замовник має право вносити зміни до твору, створеного за замовленням, супроводжувати його ілюстраціями, передмовами, післямовами тощо, якщо інше не передбачено договором замовлення.

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: «Про архітектурну діяльність», «Про медіа», «Про вищу освіту», «Про кінематографію».

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 з інтелектуальної власності особисті немайнові права інтелектуальної власності на твір, як вже було зазначено вище, створений у зв'язку з виконанням трудового договору, належать працівникові, який створив цей об'єкт. До особистих немайнових прав авторів творів, 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 (ст. 423 ЦКУ, ст. 11 Закону «Про авторське право і суміжні права»).

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 (ч. 2 ст. 439 ЦК України).

Частиною 1 ст. 429 ЦКУ 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 не встановлюють таких випадків належності особистих немайнових прав іншим особам, у тому числі роботодавцю.

Майнові права інтелектуальної власності на службові твори

Відповідно до законодавства, майновими правами інтелектуальної власності на твір, в тому числі й на службовий 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 (ч. 1 ст. 440 ЦКУ, ст. 12 Закону «Про авторське право і суміжні права»).

На відміну від особистих немайнових прав, майнові права на службовий твір можуть відчужуватися шляхом укладання цивільно-правових договорів та передаватися правонаступникам (наприклад у випадку реорганізації юридичної особи, яка у трудових відносинах виступала роботодавцем).

4.5. Захист авторського права і суміжних прав

Використання об'єктів авторського права і суміжних прав може бути правомірним та неправомірним.

Правомірне використання об'єктів авторського права передбачає передання майнових прав на твір іншій особі (фізичній або юридичній) на підставі закону чи правочину повністю (на всі способи використання твору на території всіх держав світу) або частково (на окремі способи використання твору на території всіх держав світу або на окремі способи використання твору на території окремих держав світу, або на всі способи використання твору на території окремих держав світу). Особа, до якої перейшли майнові права на твір у повному складі або частково, є суб'єктом авторського права у межах набутих права. Суб'єкт авторського права має право надати дозвіл на використання твору або розпоряджатися майновими правами на твір в іншій спосіб, що не суперечить закону (ч. 2 ст. 12 Закону «Про авторське право і суміжні права»).

Аналогічний правовий режим передбачається Законом щодо правомірного використання об'єктів суміжних прав шляхом передання (відчуження) майнових прав на виконання, фонограму, відеограму, програму організації мовлення на підставі закону або правочину (договору) (ст. 38-41 Закону «Про авторське право і суміжні права»).

Здійснення майнових прав на об'єкти авторського права і об'єкти суміжних прав передбачається у розділі IV Закону «Про авторське право і суміжні права». Так, у ч.1 ст.48 цього Закону прописано, що розпорядження майновими правами на об'єкти авторського права і об'єкти суміжних прав може здійснюватися на підставі: трудового договору (контракту); договору про створення за замовленням і використання об'єкта авторського права або об'єкта суміжних прав; договору про передання (відчуження) майнових прав на об'єкт авторського права або об'єкт суміжних прав; ліцензійного

договору на використання об'єкта авторського права або об'єкта суміжних прав; публічної ліцензії на використання об'єкта авторського права або об'єкта суміжних прав; іншого правочину щодо розпорядження майновими правами на об'єкт авторського права або суміжних прав.

Без дозволу суб'єктів авторського права передбачається «вільне» використання творів. Так, ст. 25 Закону визначає випадки вільного використання комп'ютерної програми без дозволу власника: 1) виготовити резервну копію, якщо це необхідно для використання цієї КП; 2) декомпілювати КП (перетворити її з об'єктивного коду вихідній текст) з метою одержання інформації, необхідної для досягнення її взаємодії з іншою незалежно розробленою КП. При умові, що: інформація необхідна для досягнення здатності до взаємодії, раніше не була доступною цій особі з інших джерел; зазначена декомпіляція здійснюється виключно щодо тих частин КП, які необхідні для досягнення здатності до взаємодії; інформація, одержана в результаті декомпіляції, може використовуватися лише для досягнення здатності до її взаємодії з іншими програмами, але не може передаватися іншим особам, крім випадків, якщо це необхідно для досягнення здатності до взаємодії з іншими КП, а також не може використовуватися для розроблення, виготовлення чи продажу КП, суттєво подібної за своїм вираженням до декомпільованої КП, або для вчинення будь-якої іншої дії, що порушує авторське право; 3) спостерігати, вивчати, досліджувати функціонування КП з метою визначення ідей і принципів, що лежать в її основі, за умови, що це робиться в процесі виконання будь-якої дії із завантаження, показу, функціонування, передачі чи записування в пам'ять (збереження) КП.

Без дозволу суб'єктів авторського права на КП, якщо договором не передбачене інше та якщо певні дії необхідні виключно для належного використання копії КП за призначенням, у тому числі для виправлення помилок, законний користувач КП має право: 1) здійснювати відтворення КП в цілому або частково, будь-яким способом та в будь-якій формі; 2) здійснювати переклад, адаптацію або будь-яку іншу зміну (модифікацію) КП і відтворення результатів таких дій.

Без дозволу суб'єктів суміжних прав законодавством передбачається вільне використання об'єктів суміжних прав (ст. 43 Закону).

Неправомірне використання об'єктів авторського права і суміжних прав – це їх використання без дозволу суб'єктів авторського права і суміжних прав, що пов'язане з порушенням як особистих немайнових, так і майнових авторських і суміжних прав.

Стаття 53 Закону «Про авторське право і суміжні права» визначає підстави для захисту авторського права і суміжних прав як будь-яке порушення, невизнання або оспорування таких прав, а також створення загрози порушення таких прав.

Порушенням особистих немайнових та/або майнових авторських і суміжних прав відповідно до ч. 2 ст. 53 Закону є:

1) плагіат – це опублікування твору або його частини у незмінному або видозміненому вигляді, включаючи опублікування перекладу іншомовного твору або його частини під іменем особи, яка не є автором цього твору;

2) використання об'єкта авторського права або об'єкта суміжних прав, якщо такі дії не підпадають під передбачені Законом випадки вільного використання об'єктів авторського права або суміжних прав, без дозволу суб'єкта таких прав, у тому числі:

- *піратство* у сфері авторського права і суміжних прав – відтворення, ввезення на митну територію України, вивезення з митної території України і розповсюдження піратських примірників творів (у тому числі КП і баз даних), фонограм, відеограм, незаконне використання програм організації мовлення, *камкординг*, а також *Інтернет-піратство*, тобто незаконне використання об'єктів авторського права та/або об'єктів суміжних прав із застосуванням мережі Інтернет;

- ввезення на митну територію України без дозволу суб'єктів авторського права та/або суб'єктів суміжних прав примірників творів (у тому числі КП і баз даних), фонограм, відеограм, записів передач організації мовлення;

- управління веб-сайтом, який шляхом індексації метаданих твору або об'єкта суміжних прав та надання пошукової системи, дозволяє користувачам цього веб-сайту знаходити та поширювати твір або об'єкт суміжних прав у межах однорангової мережі без дотримання майнових прав суб'єктів авторського права та/або суб'єктів суміжних прав тощо.

Згідно з ч. 3 ст. 53 Закону «Про авторське право і суміжні права» діями, що створюють загрозу порушення особистих немайнових та майнових авторських і суміжних прав, є, зокрема:

1) розповсюдження ввезення на митну територію України технічних пристроїв, обладнання, що включає КП та надає доступ користувачам до об'єктів авторського права та/або об'єктів суміжних прав без дозволу відповідних суб'єктів суміжних прав (у тому числі, коли КП, застосунки та додатки до неї, технології або технічні пристрої використовують сигнали інших Інтернет-ресурсів);

2) налаштування КП, застосунків, додатків до них, технологій, технічних пристроїв, які надають доступ до об'єктів авторського права та/або об'єктів суміжних прав без дозволу відповідних суб'єктів авторського права або суб'єктів суміжних прав таких об'єктів (у тому числі, коли КП, застосунки та додатки до неї, технології або технічні пристрої використовують сигнали інших Інтернет-ресурсів);

3) надання інструкцій щодо налаштування КП, застосунків та додатків до неї, технологій, технічних пристроїв для отримання доступу до об'єктів авторського права та/або об'єктів суміжних прав без дозволу відповідних суб'єктів авторського права або суб'єктів суміжних прав таких об'єктів у будь-якій формі з метою отримання винагороди від надання таких інструкцій.

Захист особистих немайнових і майнових прав суб'єктів авторського права і суміжних прав здійснюється в порядку встановленому адміністративним, цивільним і кримінальним законодавством. Цивільно-правовий захист авторського права і суміжних прав передбачений ст. 55 Закону «Про авторське право і суміжні права» шляхом звернення зацікавлених суб'єктів до суду з будь-якими вимогами, не забороненими законом. Зокрема про: 1) визнання авторського права або суміжних прав; 2) відновлення становища, яке існувало до порушення; 3) припинення та/або заборону вчиняти дії, що порушують авторське право та/або суміжні права чи створюють загрозу їх порушення; 4) стягнення винагороди, передбаченої законодавством про авторське право і суміжні права; 5) відшкодування моральної шкоди; 6) відшкодування збитків, завданих порушенням авторського права або суміжних прав, включаючи упущену вигоду, або стягнення доходу, отриманого порушником внаслідок порушення ним авторського права або суміжних прав, або

стягнення компенсації; 7) припинення підготовчих дій до порушення авторського права та/або суміжних прав, у тому числі шляхом призупинення митних процедур, якщо є підстави вважати, що на митну територію України чи з митної території України можуть бути пропущені піратські примірники творів, фонограм, відеограм, засоби обходу технологічного засобу захисту об'єктів авторського права та/або об'єктів суміжних прав тощо; 8) опублікування за рахунок порушника в ЗМІ даних про порушення авторського права та/або суміжних прав та судові рішення щодо цих порушень; 9) вжиття інших передбачених законодавством заходів, пов'язаних із захистом авторського права та/або суміжних прав.

Порушення інтелектуальних прав у мережі Інтернет часте явище у сьогодишньому світі. Для їх захисту у мережі Інтернет, наприклад, на англomовних доменах передбачається чітко розвинена процедура «takedown notice» як вимога видалення нелегального контенту. Створені типові форми-скарги на незаконний твір, після їх заповнення, вони відправляються адміністратором цифрових ресурсів і негайно блокується контент для перевірки. У соціальних мережах тоді сповіщається про обмежений доступ до контенту з коментарем «Даний контент порушує авторське право».

В Україні процедура «takedown notice» передбачена ст. 56 Закону «Про авторське право і суміжні права» де визначається **порядок припинення порушень авторського права і суміжних прав з використанням мережі Інтернет**. Відповідно до цієї норми особа право, якої порушено, має право звернутися із заявою про припинення порушення авторського права.

Із заявою можна звернутися до власника веб-сайту чи веб-сторінки (в залежності від того, де було порушення авторського права та/або суміжних прав), одночасно копія заяви відправляється постачальнику послуг хостингу (компанія, яка надає послуги розміщення сайтів у мережі Інтернет). Можна звернутися і безпосередньо до постачальника послуг хостингу в тому випадку, якщо власник веб-сайту чи веб-сторінки, після отримання заяви, не вчинив жодних дій або, якщо неможливо встановити власника веб-сайту чи веб-сторінки. Якщо неможливо знайти дані про власника веб-сайту чи постачальника послуг хостингу, то можна звернутися до Українського національного офісу інтелектуальної власності та інновацій для того, щоб отримати допомогу у пошуку зазначених суб'єктів.

Форма заяви має бути письмовою, складена у паперовій чи електронній формі. Відправити її можна електронною поштою або рекомендованим листом. Якщо заява складається в електронній формі, у ній мають бути дотриманні усі вимоги законодавства у сфері електронних документів та електронного документообігу. При цьому обов'язково накладається електронний підпис адвоката або представника у справі з інтелектуальною власністю (патентного повіреного). Відправлено має бути дві обов'язково однакові за змістом заяви: з накладанням кваліфікованого електронного підпису і її копія у звичайній електронній формі. Заяву у паперовій формі підписує адвокат чи патентний повірений і відправляє її рекомендованим листом з повідомленням про вручення.

У заяві слід зазначити:

- відомості про заявника: (ім'я фізичної особи (найменування юридичної особи); місце проживання (перебування або місцезнаходження, адреса електронної пошти, а

для заявників-юридичних осіб – ідентифікаційні дані про реєстрацію юридичної особи у країні місцезнаходження, зокрема в торговельному, банківському, судовому або державному реєстрі, у тому числі реквізити реєстру, реєстраційний номер;

- вид і назву об'єктів авторського права та/або об'єктів суміжних прав, іншу інформацію, що дає можливість ідентифікувати об'єкти щодо яких порушуються права;

- вмотивоване твердження про наявність у заявника майнових прав на об'єкт авторського права та/або об'єкт суміжних прав чи виключних прав на використання такого об'єкта з посиланням на підстави виникнення таких прав та строк їх чинності (підстави не вказуються, якщо заявник є первинним суб'єктом відповідних майнових прав);

- гіперпосилання на електронну (цифрову) інформацію, розміщену або в іншій спосіб використану на веб-сайті, або гіперпосилання на веб-сторінку, до якої здійснювалося інтерактивне надання доступу об'єкта авторського права або об'єкта суміжних прав, про порушення майнових прав, про який йдеться у заяві;

- про вимогу до власника веб-сайту щодо унеможливлення доступу до цифрового контенту на веб-сайті або вимогу до власника веб-сайту і провайдера послуг обміну контентом щодо недопущення ними подальшого розміщення на веб-сайті зазначеного цифрового контенту;

- відомості про постачальника послуг хостингу, який надає послуги та/або ресурси для розміщення відповідного веб-сайту у мережі Інтернет. Тут слід вказати: найменування, адресу електронної пошти або поштову адресу, на яку, в передбачених законом випадках, власник веб-сайту або інші особи мають надсилати інформацію.

Адвокат чи патентний повірений має перевірити достовірність інформації у заяві і підтвердити наявність права інтелектуальної власності у заявника. До заяви слід додати копію документів, що посвідчують повноваження адвоката чи патентного повіреного. Заява має бути складена максимально коректно, тобто відповідно вимог Закону, оскільки власник веб-сайту чи постачальник послуг хостингу має право відмовити у задоволенні заяви, якщо вона складена з порушеннями.

Власник веб-сайту чи веб-сторінки має обмежити доступ до цифрового контенту не пізніше 48 годин з моменту отримання заяви. Про вжиті заходи він повинен повідомити заявника та постачальника послуг хостингу. Слід звернути увагу на те, що обмежується доступ тільки до цифрової інформації, зазначеної в заяві про порушення авторського права і суміжних, а не всієї веб-сторінки чи веб-сайту.

Власник веб-сторінки або веб-сайту може відмовити у задоволенні заяви, тоді про відмову надсилається повідомлення заявнику та постачальнику послуг хостингу протягом 48 годин з моменту отримання заяви. Причинами відмови заяви у задоволенні можуть бути: документальне підтвердження наявності права на використання цифрового контенту; оформлення заяви про припинення порушення авторського права та/або суміжних прав з порушенням вимог законодавства.

Якщо заяву відправлено власнику веб-сайту, який не є власником веб-сторінки, на якій розміщено цифровий контент, зазначений у заяві, тоді власник веб-сайту невідкладно, але не пізніше 24 годин з моменту отримання заяви, зобов'язаний направити її копію власнику веб-сторінки. Одночасно надсилається повідомлення

заявнику про те, що він не є власником веб-сторінки. У повідомленні потрібно вказати час відправлення копій власнику веб-сторінки та надати гіперпосилання на умови публічного правочину, який визначає правила користування веб-сайтом для третіх осіб. У свою чергу, власник веб-сторінки протягом 48 годин розглядає заяву та надсилає відповідь власнику веб-сайту, а протягом 24 годин власником веб-сайту відповідь відправляється заявнику та постачальнику послуг хостингу. Якщо жодної відповіді від власника веб-сторінки не отримано, тоді власник веб-сайту самостійно унеможливорює доступ до цифрового контенту, зазначеного в заяві.

Якщо ж заява направляється постачальнику послуг хостингу, протягом 24 годин її відправляють власнику веб-сайту з роз'ясненням прав та обов'язків, пов'язаних з такою заявою, а також правових наслідків бездіяльності. Власник веб-сайту розглядає заяву протягом 24 годин і надсилає відповідь постачальнику послуг хостингу. Останній, у свою чергу, надсилає відповідь заявнику. Якщо заявник своєчасно не отримав відповідної відповіді, то тоді він має право звернутися до Українського національного офісу інтелектуальної власності та інновацій з ініціюванням притягнення власника веб-сайту чи постачальника послуг хостингу до відповідальності.

Стаття 57 Закону «Про авторське право і суміжні права» визначає зобов'язання постачальників послуг хостингу щодо забезпечення захисту авторського права і суміжних прав з використанням мережі Інтернет. Відповідно до ч. 1 цієї норми постачальники послуг хостингу зобов'язані передбачити у договорах про надання послуг хостингу умови і правила, що забороняють замовникам послуг вчиняти дії з розміщення цифрового контенту з порушенням авторського права та/або суміжних прав третіх осіб, а також зобов'язують замовників послуг зазначити достовірну і коректну інформацію про себе, у тому числі контактні дані, а в разі їх зміни – невідкладно інформувати про це в порядку, визначеному законодавством.

Стаття 58 Закону «Про авторське право і суміжні права» передбачає відповідальність провайдерів послуг обміну контентом за порушення авторського права та/або суміжних прав та випадки звільнення їх від відповідальності.

Запитання для самоконтролю і самостійного опрацювання

1. Розкрийте зміст Договору BOIB з авторського права.
2. У чому полягає основний зміст Договору BOIB про виконання і фонограми?
3. У чому полягає суть понять «творча діяльність» і «інтелектуальна діяльність»?
4. Визначте основний статус Інтернет-договорів BOIB.
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?

РОЗДІЛ 5. ДОГОВОРИ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (ІТ)

5.1. Загальні положення щодо договірних відносин в цифровому середовищі та їх види

У сфері інформаційних технологій (ІТ) договори є фундаментальним інструментом для регулювання правовідносин між сторонами. Вони визначають обсяг робіт (послуг), права та обов'язки сторін, фінансові умови, а також регулюють питання захисту інтелектуальної власності та конфіденційності.

Договори у сфері ІТ – це юридичні угоди, що регулюють надання, використання, розробку, підтримку та обслуговування програмного забезпечення, апаратного забезпечення та ІТ-послуг. Такі договори охоплюють широке коло правових питань, пов'язаних із захистом даних, інтелектуальною власністю та забезпеченням конфіденційності.

Значення договорів у сфері ІТ є багатограним та важливим для забезпечення стабільності та ефективності взаємодії між сторонами. Одним з ключових аспектів є правова визначеність. Чітке визначення прав та обов'язків кожної сторони у договорі допомагає уникнути непорозумінь та суперечок, забезпечуючи зрозумілу та передбачувану правову базу для всіх учасників. Наприклад, *у договорі на розробку програмного забезпечення чітко прописуються етапи роботи, строки виконання та вимоги до кінцевого продукту, що дозволяє обом сторонам мати чітке уявлення про свої обов'язки.*

Ще одним важливим аспектом є захист інтелектуальної власності. Договори регулюють питання використання та захисту програмного забезпечення, захищаючи права власника на інтелектуальну власність. Наприклад, *ліцензійні угоди встановлюють, як і в яких умовах можна використовувати програмне забезпечення, обмежуючи несанкціоноване копіювання чи розповсюдження.*

Фінансові умови в договорах також грають важливу роль. Визначення порядку оплати та фінансових зобов'язань сприяє фінансовій стабільності та плануванню. Для прикладу, *у договорі на надання ІТ-послуг може бути прописаний порядок оплати за кожний етап робіт або надання послуг, що дозволяє компаніям чітко планувати свої витрати та доходи.*

Крім того, договори встановлюють стандарти якості наданих послуг або продуктів, що забезпечує високу якість та задоволеність клієнтів. Наприклад, *в угодах про технічну підтримку можуть бути визначені часи реакції на запити та обов'язки постачальника щодо усунення неполадок.*

Важливою функцією договорів є також сприяння ефективному вирішенню спорів. Чітко прописані умови та процедури врегулювання конфліктів допомагають швидко вирішувати спірні питання, що можуть виникати під час виконання договору.

Нарешті, договори сприяють підтримці довгострокових відносин між компаніями. Вони створюють правову основу для тривалого співробітництва, встановлюючи правила та обов'язки, які є зрозумілими для обох сторін. Наприклад, *довгострокові контракти на обслуговування ІТ-систем можуть включати регулярні огляди та оновлення, що підтримує постійний зв'язок між постачальником та клієнтом.*

У сфері ІТ існує декілька видів договорів, кожен з яких має своє призначення та нормативно-правове регулювання.

Ліцензійні договори надають ліцензіату право на використання програмного забезпечення або інтелектуальної власності ліцензіара. Згідно зі статтею 1109 Цивільного кодексу України⁵¹, такі договори визначають вид ліцензії (ексклюзивна або невиключна), умови використання, обмеження, а також розмір і порядок оплати.

Договори на розробку програмного забезпечення регулюють процес створення програмного забезпечення, охоплюючи всі етапи розробки. Відповідно до статей 837-838 Цивільного кодексу України, основні положення таких договорів включають технічне завдання, терміни виконання, права на результати роботи та порядок прийому і здачі робіт.

Договори на надання ІТ-послуг охоплюють надання різноманітних послуг, таких як аутсорсинг, консалтинг та хмарні послуги. Згідно зі статтею 901 Цивільного кодексу України, такі договори містять опис послуг, рівень сервісу (SLA)⁵², безпеку даних, конфіденційність та відповідальність за порушення умов договору.

Договори на технічну підтримку та обслуговування регулюють надання технічної підтримки та обслуговування ІТ-інфраструктури. Нормативною базою для таких договорів є статті 901-907 Цивільного кодексу України, і вони визначають умови технічної підтримки, рівні підтримки та порядок вирішення технічних проблем.

Вищезазначені договори регулюються основними нормативно-правовими актами, серед яких Цивільний кодекс України, який є основним документом, що регулює договірні відносини. Також важливими є закони України «Про захист прав споживачів»⁵³, «Про електронну комерцію»⁵⁴, який регулює правові відносини в сфері електронної комерції, включаючи електронні договори, та «Про авторське право і суміжні права»⁵⁵, який захищає права інтелектуальної власності.

Таким чином, договори у сфері ІТ є ключовим інструментом для регулювання взаємовідносин між сторонами, забезпечуючи правову визначеність, захист інтелектуальної власності, фінансову стабільність та високу якість наданих послуг. Нормативно-правова база України забезпечує ефективне правове регулювання цих відносин, що сприяє розвитку ІТ-сектору в країні.

Основні умови ІТ договорів у контексті положень Цивільного кодексу України охоплюють ключові аспекти, що забезпечують правову визначеність і ефективність взаємодії між сторонами. Одним із основних елементів є визначення сторін, що передбачає чітке зазначення найменувань, адрес і контактних даних сторін договору. Це є необхідним для встановлення правових відносин відповідно до статті 638 Цивільного кодексу України, яка регулює загальні положення щодо укладання договорів.

Предмет договору має містити опис послуг або робіт, що виконуються. Це може включати, наприклад, надання технічної підтримки, аутсорсинг, розробку програмного

⁵¹ Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV.

⁵² SLA (Service Level Agreement) – це угода між постачальником послуг і клієнтом, яка визначає очікуваний рівень обслуговування. Вона описує конкретні показники та стандарти, яких повинні дотримуватися постачальники послуг, а також наслідки та компенсації у випадку недотримання цих стандартів.

⁵³ Про захист прав споживачів: Закон України від 12.05.1991 № 1023-XII.

⁵⁴ Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII.

⁵⁵ Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX.

забезпечення та інші IT-послуги. Чіткий опис предмета договору є критично важливим для уникнення непорозумінь під час його виконання.

Технічне завдання (Statement of Work, SOW)* є важливим компонентом, що містить специфікації вимог і очікуваних результатів. Це включає функціональні та нефункціональні характеристики, що допомагає визначити конкретні роботи, які будуть виконані в рамках договору.

Фінансові умови, що визначають порядок оплати та фінансові зобов'язання, також є важливими для забезпечення фінансової стабільності. Усі платежі мають бути чітко визначені, що сприяє ефективному фінансовому плануванню. Питання про ціну договору (договірну ціну) є досить цікавим: з одного боку, ціноутворення залежить виключно від волі контрагентів за договором, тобто є вільним, а з іншого – не завжди є таким, оскільки підпадає під державне регулювання. Наприклад, в Україні є певні категорії товарів і послуг, на які держава встановлює граничні ціни або тарифні ставки. Це стосується, зокрема, комунальних послуг, ліків, енергоносіїв та інших товарів, що мають соціальне значення (Закон України «Про ціни і ціноутворення»). Держава може впливати на ціни на певні IT-послуги через регуляції, які встановлюють вимоги до тарифів на послуги, особливо якщо вони надаються державними підприємствами або в рамках держзамовлень. Наприклад, в рамках державних закупівель можуть встановлюватися граничні ціни на IT-послуги, що фінансуються з державного бюджету. Закон України «Про електронну комерцію» визначає основні принципи, які регулюють електронну комерцію, включаючи аспекти ціноутворення в сфері IT. Це включає правила про формування цін на електронні товари та послуги, а також вимоги до інформації, яку постачальники повинні надавати споживачам. Згідно з Законом України «Про захист прав споживачів», постачальники IT-послуг зобов'язані надавати споживачам прозору інформацію про ціни та умови надання послуг, що також регулює питання ціноутворення.

Умови конфіденційності та захисту даних регулюють обробку та захист конфіденційної інформації клієнта, що є важливим у контексті сучасних інформаційних технологій. Це узгоджується з вимогами законодавства про захист персональних даних, що також підкреслює важливість дотримання норм щодо конфіденційності.

Умови, що регулюють інтелектуальну власність і визначають права сторін на результати виконаних робіт, є надзвичайно важливими для забезпечення належного захисту інтелектуальної власності. Правові основи для охорони авторських та суміжних прав у сфері IT закріплені в статтях 422-432 Цивільного кодексу України. Ці положення формують рамки для правової охорони інтелектуальної власності, що має важливе значення для бізнесу та інновацій у цій галузі.

Умови вирішення спорів, що регулюють процедури для розв'язання конфліктів, є суттєвими для підтримки гармонійних відносин між сторонами. Це можуть бути такі заходи, як медіація, арбітраж або судові розгляди. Ці механізми дозволяють швидко і ефективно вирішувати спірні питання, запобігаючи ескалації конфліктів і сприяючи збереженню професійних зв'язків.

* Statement of Work (SOW) – це документ, який визначає конкретні деталі проекту, включаючи обсяг робіт, терміни, вимоги, ресурси та інші ключові аспекти. SOW є важливою складовою IT-договорів, оскільки він встановлює очікування та стандарти для всіх учасників проекту.

Отже, основні елементи ІТ-договорів створюють правову основу, яка забезпечує ефективне управління відносинами між сторонами, надаючи правову визначеність і захищаючи інтереси учасників. Ця структура сприяє зниженню ризиків і конфліктів, дозволяючи сторонам зосередитися на виконанні своїх зобов'язань і досягненні спільних цілей.

5.2. Ліцензійні угоди в сфері ІТ

Ліцензійний договір є ключовим договором в сфері ІТ, та широко використовується з метою розповсюдження та дистрибуції програмного забезпечення. У сфері ІТ-бізнесу існує безліч ліцензій. Ці договори є одними з найбільш поширених і необхідні для реалізації проектів різного рівня складності та масштабу. Вони варіюються від ліцензій на фотографії на фотостоках до рішень white-label⁵⁶ для конкретного програмного забезпечення, яке використовується у великих ІТ-продуктах.

Цивільний кодекс України (ЦК) 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).

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**.

⁵⁶ **White-label пішення** – це продукти або послуги, які розробляються однією компанією, але продаються під брендом іншої компанії. В ІТ-сфері це часто стосується програмного забезпечення, яке може бути адаптоване та перепродане з використанням фірмового стилю клієнта.

Укладений договір породжує взаємні права та обов'язки для його сторін, тому це договір є **взаємнозобов'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. В свою чергу, презумпція відплатності договору, виходячи з положень частини 5 статті 626 ЦК не спростована, а у частині 3 статті 1109 ЦК 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 **носить строковий характер**. Строк є істотною умовою договору, виходячи з положень статті 1110 ЦК. 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 урахувати правила статті 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 частини 2 статті 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.

Ліцензіат має право:

- 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.

Ліцензіар має право:

1) на отримання винагороди за ліцензійним договором, як- що така встановлена умовами договору;

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

3) на інформацію про межі і 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 частині 4 статті 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).

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 порівняно зі становищем, передбаченим законом або типовим договором, є нікчемними і замінюються умовами, встановленими типовим договором або законом (ст. 1111 ЦК).

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

1) вид ліцензії;

2) 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);

3) розмір, порядок і строки виплати винагороди за використання об'єкта права інтелектуальної власності;

4) 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).

Однак деякі із вищезазначених умов ліцензійного договору, закріплених у ч. 3 ст. 1109 ЦК (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). 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).

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 із сторін не повідомить письмово іншу сторону про відмову від договору, договір вважається продовженим на невизначений строк. У цьому випадку кожна із 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 (частини 1,3 ст. 1110 ЦК).

Положення ЦК 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).

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).

Винагорода за наданий дозвіл може бути встановлена у вигляді фіксованої грошової суми (паушальний платіж⁵⁷), періодичних платежів (роялті) чи їх поєднання (комбінованих платежів).

⁵⁷ Про затвердження Національного стандарту № 4 «Оцінка майнових прав інтелектуальної власності»: Постанова Кабінету Міністрів України; Стандарт від 03.10.2007 № 1185 (п. 3)

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 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 апаратною мікросхем комп'ютера, а програмне забезпечення, у свою чергу, здатне виконувати функції електронної апаратури.

На відміну від прикладного програмного забезпечення, системне не вирішує конкретні прикладні задачі, а лише забезпечує роботу інших програм, управляє апаратними ресурсами обчислювальної системи і 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 і профілактики апаратури комп'ютера та обчислювальних мереж; виконання допоміжних технологічних процесів (копіювання, архівування, відновлення файлів програм і баз даних і т. д.).⁵⁸

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

⁵⁸ 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>.

команд, які, якщо їх записати на машинозчитуваному носіїві, 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 власності⁵⁹.

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»).

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 копіювання⁶⁰.

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 і ціна програмного забезпечення.

⁵⁹ 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.

⁶⁰ Там же. С.133.

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 користуванням: 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 в ЦК України, ні в 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 договірної права.

5.3. Договори 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. Договори на розробку ПЗ є ключовими елементами правових відносин у сфері інформаційних технологій. Вони визначають умови, обов'язки і права сторін, а також регулюють процес створення, тестування, впровадження і підтримки програмних продуктів. У цьому розділі розглянемо основні аспекти, пов'язані з такими договорами, включаючи їх правову природу, структуру та специфічні вимоги.

Відповідно до українського законодавства програмне забезпечення є твором. Зокрема, положення ЦК 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. Договори на розробку програмного забезпечення підпадають під регулювання Цивільного кодексу України, зокрема статей 837-838. Вони є двосторонніми угодами, в яких одна сторона (розробник) зобов'язується створити певний програмний продукт відповідно до технічного завдання, а інша сторона (замовник) - оплатити його. Важливо, щоб у договорі були чітко прописані умови виконання робіт, терміни, а також права на результати розробки.

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

Договір **Time & Materials (оплата за фактом)**. Зазвичай такі договори використовують у разі, коли об'єм 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, проектування, 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.

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 проектування, у ході якого створюються документи, що детально описують для програмістів спосіб і план реалізації зазначених вимог. Після того, як проектування повністю виконане, програмістами за договором виконується реалізація отриманого проекту. На наступній стадії процесу відбувається інтеграція окремих компонентів, що розробляються різними командами програмістів. Після того, як реалізація і 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 і усунення помилок.

Перехід від однієї фази до іншої відбувається тільки після повного і успішного завершення попередньої. Таким чином, каскадна модель має на увазі, що перехід від однієї фази розробки до іншої відбувається тільки після повного і 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 і вирішальним спорах про неякісне надання послуг стосовно розробки програмного забезпечення⁶¹.

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 навиків 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

⁶¹ Фасій, Богдан Володимирович. Agile waterfall та out staff договір або договори на розробку програмного забезпечення.// Часопис цивілістики 26 (2017): 98-102.

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 розорявалися, 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» (аутсорсінг), проте це абсолютно різні поняття. Аутсорсінг являє собою передачу компанією тих чи інших непрофільних для неї функцій стороннім організаціям за договором (наприклад, ІТ-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 представляє собою типовий outsourcing. Для розробки передових моделей або нових пристроїв беруться в найм дизайнери і вузькі фахівці в тій чи іншій області. Зокрема, до роботи над iWatch (годинник від «яблучної» компанії) було залучено близько сотні тимчасових фахівців з провідних годинних фірм Швейцарії.

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 увагу 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).

Особисті немайнові права автора 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-передання). 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-передання).

5.4. Договори на надання ІТ-послуг

Договори на надання ІТ-послуг є невід'ємною частиною сучасного бізнес-середовища, оскільки вони регулюють широкий спектр відносин між постачальниками послуг і замовниками. Ці угоди сприяють встановленню прав і обов'язків, а також визначенню умов співпраці, що є критично важливим для ефективного функціонування підприємств у сфері інформаційних технологій.

Згідно з українським законодавством, основними нормативно-правовими актами, які регулюють договори на надання ІТ-послуг, є Цивільний кодекс України та спеціалізовані закони, такі як Закон України «Про електронну комерцію» та Закон України «Про авторське право і суміжні права». Цивільний кодекс, зокрема, статті 901-906, визначає загальні правила для договорів про надання послуг, включаючи умови укладання, виконання та припинення договорів.

Види договорів на надання ІТ-послуг різноманітні, зокрема:

1. Договори на технічну підтримку. Угода, що регулює умови надання технічної підтримки, включаючи підтримку програмного забезпечення, системного адміністрування, усунення несправностей та оновлення систем. Цей тип договору часто містить рівні обслуговування (Service Level Agreement, SLA), які визначають терміни реагування на запити клієнта, обсяги послуг та відповідальність сторін. Як різновид, це **договір на обслуговування ІТ-інфраструктури**, який охоплює всі аспекти обслуговування комп'ютерних мереж, серверів та інших ІТ-ресурсів. Наприклад, угода може містити положення про регулярні огляди систем, оновлення обладнання та забезпечення безпеки даних. Також до даного договірному типу можна віднести **договір на технічну підтримку для хостингових послуг**, в рамках якого хостинг-провайдер* може зобов'язуватися надавати клієнту підтримку, включаючи налаштування серверів, управління доменами та реагування на запити щодо безпеки веб-сайтів. У таких угодах зазвичай визначаються часи реагування на технічні запити та обсяги послуг.

2. Аутсорсингові договори. Аутсорсинг ІТ-послуг став популярним рішенням для компаній, які прагнуть зосередитися на своїх основних бізнес-процесах. Ці угоди можуть охоплювати передачу функцій, таких як обслуговування ІТ-інфраструктури, обробка даних, розробка програмного забезпечення, підтримка систем та інше. Аутсорсинг ІТ-послуг є практикою, коли компанії передають певні завдання або функції стороннім постачальникам. Це дозволяє зосередитися на основних бізнес-процесах, знижуючи витрати та підвищуючи ефективність. Багато компаній аутсорсять створення програмних рішень стороннім розробникам. Наприклад, стартап може замовити розробку мобільного додатку в аутсорсинговій компанії, яка спеціалізується на цій сфері.

3. Договори про електронну комерцію. В умовах зростання електронної комерції важливими є договори, що регулюють угоди між продавцями та споживачами, а також між бізнесами в електронному середовищі. Договори про електронну комерцію в ІТ є важливим елементом правового регулювання відносин, що виникають у сфері онлайн-торгівлі та послуг. Ці договори охоплюють різноманітні аспекти, такі як купівля-продаж товарів і послуг через Інтернет, умови використання веб-сайтів, а також захист прав споживачів.

4. Договори на надання консалтингових послуг. Цей тип договорів регулює надання послуг, пов'язаних з консалтингом у сфері ІТ. Це може включати стратегічне планування, аналіз бізнес-процесів, розробку технологічних рішень та оцінку ефективності ІТ-систем.

5.5. Договори на технічну підтримку та обслуговування

Договори на технічну підтримку та обслуговування та договори на надання ІТ-послуг схожі між собою, але мають кілька ключових відмінностей, які визначають їх правову природу та функціональні аспекти.

* Хостинг-провайдер – це компанія або організація, яка надає послуги з розміщення веб-сайтів, додатків або даних на своїх серверах. Основні функції хостинг-провайдера включають забезпечення доступу до веб-сайтів через Інтернет, зберігання файлів та даних, а також управління серверами, які підтримують ці послуги.

Договори на технічну підтримку та обслуговування зосереджуються на забезпеченні підтримки вже існуючих систем, їх функціонування та усунення неполадок. Вони регулюють специфічні аспекти обслуговування та моніторингу. В свою чергу, договори на надання ІТ-послуг охоплюють широкий спектр послуг, включаючи розробку програмного забезпечення, консалтинг, аутсорсинг та інші послуги. Ці угоди можуть включати створення нових систем чи їх компонентів, що не є частиною технічної підтримки. Договори на технічну підтримку часто укладаються на тривалий термін, який забезпечує постійний доступ до підтримки. Вони можуть бути розраховані на рік або більше. В свою чергу, договори на надання ІТ-послуг можуть бути укладені на обмежений період, наприклад, на виконання конкретного проекту, з можливістю продовження, якщо це необхідно.

Так, договори на технічну підтримку та обслуговування є важливими елементами у сфері ІТ, оскільки вони визначають умови, за яких постачальники послуг зобов'язуються надавати підтримку для ІТ-систем, програмного забезпечення або апаратних засобів. Ці угоди допомагають забезпечити стабільну роботу технологічних систем та захистити інтереси як постачальників, так і клієнтів.

Договори на технічну підтримку регулюються нормами Цивільного кодексу України, що визначає основи зобов'язань сторін у рамках цих угод. Зокрема, статті 901-907 Цивільного кодексу визначають загальні умови укладання таких угод, а також права та обов'язки сторін. Згідно зі статтею 901 Цивільного кодексу, за договором про надання послуг одна сторона (виконавець) зобов'язується за завданням другої сторони (замовника) надати послугу, яка споживається в процесі вчинення певної дії або здійснення певної діяльності, а замовник зобов'язується оплатити виконавцеві зазначену послугу, якщо інше не встановлено договором. Це означає, що договір на технічну підтримку повинен чітко визначати, які саме послуги надаються, а також їх вартість. Важливо, щоб сторони узгодили деталі щодо обсягу робіт, термінів виконання та вимог до якості послуг.

Також слід врахувати, що Закон України «Про захист прав споживачів» має значний вплив на технічну підтримку. Цей закон встановлює права споживачів, які мають бути дотримані постачальниками послуг. Зокрема, він передбачає вимоги щодо якості послуг, що надаються, а також можливості повернення або усунення дефектів у разі неналежного виконання зобов'язань. Наприклад, споживач має право на отримання інформації про послуги, а також може вимагати усунення недоліків або повернення грошей у разі невиконання умов договору.

Цей договір визначає, які саме послуги з технічної підтримки будуть надаватись, включаючи допомогу у вирішенні технічних проблем, оновлення програмного забезпечення, моніторинг систем та обслуговування апаратного забезпечення. Важливим є врегулювання в договорі рівень сервісу (Service Level Agreement, SLA), включаючи час реагування на запити, порядок усунення неполадок та графік обслуговування.

Стосовно прав та обов'язків сторін договір визначає, які обов'язки має постачальник послуг (наприклад, забезпечення підтримки в певні години) і які зобов'язання має клієнт (наприклад, надання доступу до системи). У договорі на технічну підтримку може бути вказано, що постачальник зобов'язується надавати підтримку для програмного забезпечення протягом 24 годин на добу, а також

включати регулярні перевірки системи для запобігання можливих проблем. Важливо також вказати, що у разі серйозних збоїв постачальник має реагувати в межах, наприклад, однієї години.

Отже, в умовах швидкого розвитку технологій та інновацій, договірні відносини в ІТ набувають особливого значення, оскільки вони формують правову основу для співпраці між розробниками програмного забезпечення, постачальниками послуг та споживачами.

Договори в сфері ІТ можуть охоплювати різні види угод, такі як ліцензійні договори, договори на розробку програмного забезпечення, договори на надання ІТ-послуг, а також договори на технічну підтримку. Кожен із цих договорів має свої особливості та вимоги, що регулюються відповідними нормами Цивільного кодексу України та іншими нормативно-правовими актами, такими як Закон України «Про електронну комерцію» та Закон України «Про авторське право і суміжні права». Ключовими аспектами, які слід враховувати при укладанні договорів у сфері ІТ, є захист інтелектуальної власності, умови щодо конфіденційності, а також вимоги до якості послуг. Правова визначеність та чіткість у формулюванні умов договору є важливими для запобігання суперечкам і забезпечення стабільності відносин між сторонами.

Запитання для самоконтролю і самостійного опрацювання:

1. Визначення та значення договорів у сфері ІТ.
2. Види договорів у сфері ІТ, їх правова характеристика.
3. Зміст та основні умови договорів у сфері ІТ.
4. Поняття ліцензійного договору, його правова характеристика.
5. Поняття договору на розробку програмного забезпечення, його правова характеристика, та види.
6. Поняття договору на надання ІТ-послуг, його правова характеристика та види.
7. Поняття договору на технічну підтримку та обслуговування, його правова характеристика та види.

РОЗДІЛ 6.

ГОСПОДАРСЬКА ДІЯЛЬНІСТЬ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ. ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ

6.1. Електронна комерція

Розвиток сучасного світу та економіки ознаменувався переходом на новий етап розвитку людського суспільства і появою «інформаційної» або «цифрової» економіки, яка пов'язана із всебічним використанням ІКТ. Головною складовою інформаційної економіки є глобальна мережа Інтернет, яка в свою чергу є елементом інфраструктури інформаційного суспільства. Доступ до мережі Інтернет дає необмежені можливості роботи з інформацією в електронному середовищі, що в свою чергу приводить до зміни правил гри між учасниками бізнесу. Застосування інформаційних технологій у різних сферах бізнесу, зокрема маркетинг, менеджмент, фінанси сприяють появі нових підходів до організації бізнесу, зокрема появі так званого «електронного бізнесу»⁶². Правові норми, статuti чи правила здійснення комерційних операцій сьогодні потребують вдосконалення, а Інтернет-споживачі – захисту.

В літературі е-бізнес поділяють на чотири основні види, кожен з яких працює по-своєму. Всі ці види мають свої правила співпраці, різні способи оплати та рівні довіри між учасниками.

B2B (бізнес для бізнесу). Це співпраця компаній між собою, наприклад, виробник меблів продає свою продукцію меблевим магазинам. Тут ідеться про великі замовлення за оптовими цінами. Такі угоди часто укладають на довгий термін, а популярні платформи для такої торгівлі – це Alibaba та IndustryBuying.

B2C (бізнес для споживача). Це найбільш звичний для нас формат, коли компанії продають товари звичайним покупцям через інтернет-магазини. Rozetka чи Amazon – типові приклади. Тут все просто: обрав товар, оплатив, отримав доставку додому, покупці можуть читати відгуки, порівнювати ціни та обирати зручний спосіб оплати.

C2C (споживач для споживача). Така електронна торгівля це коли звичайні люди продають речі іншим людям, найчастіше на таких майданчиках, як OLX чи Facebook Marketplace. Тут часто продають вживані речі за нижчими цінами, ніж у магазинах. Продавці та покупці можуть спілкуватися нап'яму та домовлятися про ціну.

C2B (споживач для бізнесу). Це коли звичайні люди пропонують свої послуги компаніям. Сюди входять фрілансери, які працюють через платформу Upwork, фотографи, які продають свої роботи на фотобанках, блогери, які рекламують товари компаній. Також це можуть бути експерти, які надають консультації бізнесу, або люди, які заробляють на платних опитуваннях від компаній.

Сучасний е-бізнес – це якісно нові технології, які дозволяють компанії досягти конкурентної переваги завдяки поліпшенню обслуговування своїх клієнтів та оптимізації бізнес-стосунків з партнерами. Інтернет-технології є одним з основних, але не єдиним ключовим аспектом в е-бізнесі.

⁶² Садчикова, І., Тарасенко, А., & Дубина, М. (2023). Теоретичне обґрунтування сутності поняття «електронна комерція». *Економіка та суспільство*, (53). <https://doi.org/10.32782/2524-0072/2023-53-36>.

Електронний бізнес – це вид економічної діяльності суб'єктів господарювання через комп'ютерні мережі, зокрема Інтернет, з метою отримання прибутку. Це електронна економічна діяльність, яка здійснюється за допомогою інформаційно-комунікаційних технологій (ІКТ) з метою отримання прибутку.

Е-бізнес – це більше ніж проста електронна покупка або продаж товарів. Він потребує використання мережних комунікаційних технологій для проведення дій з метою отримання прибутків всередині і поза підприємством.⁶³

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 терміну⁶⁴:

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.

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.

ЮНСІТРАЛ (UNCITRAL, United Nations Commission on International Trade Law) – це Комісія Організації Об'єднаних Націй з права міжнародної торгівлі. Її було створено в 1966 році Генеральною Асамблеєю ООН для сприяння гармонізації та уніфікації міжнародного торгового права. ЮНСІТРАЛ підготувала набір законодавчих актів, які дозволили та полегшили використання електронних засобів для участі в комерційній діяльності.

ЮНСІТРАЛ розробила ряд важливих документів, які широко застосовуються в міжнародній торгівлі, серед яких: Типовий закон ЮНСІТРАЛ про електронну комерцію (1996 р.), який встановлює правила рівного ставлення до електронної та паперової інформації, а також юридичне визнання електронних транзакцій і процесів на основі фундаментальних принципів відсутність дискримінації щодо використання електронних засобів, функціональна еквівалентність і технологічна нейтральність. Типовий закон ЮНСІТРАЛ про електронні підписи (2001) містить додаткові правила щодо використання електронних підписів.

⁶³ Краус К.М., Краус Н.М., Маньзура О.В. Електронна комерція та Інтернет-торгівля: навчально-методичний посібник. – Київ: Аграр Медіа Груп, 2021. – 454 с.

⁶⁴ Маловичко С. В. Тенденції та перспективи розвитку електронної торгівлі в Україні. Економіка і регіон. 2015. № 4. С. 67-73.

Конвенція Організації Об'єднаних Націй про використання електронних комунікацій у міжнародних контрактах (Нью-Йорк, 2005) спирається на вже існуючі тексти ЮНСІТРАЛ і забезпечує юридичну визначеність для електронних контрактів у міжнародній торгівлі. Типовий закон ЮНСІТРАЛ про електронні переказні записи (2017) застосовує ті самі принципи, щоб дозволити та полегшити використання в електронній формі переказних документів та інструментів, таких як коносаменти, переказні векселі, чеки, векселі та складські розписки.

У 2019 році ЮНСІТРАЛ схвалила публікацію Приміток щодо основних питань контрактів на хмарні обчислення, а в 2022 році прийняла Типовий закон ЮНСІТРАЛ про використання та транскордонне визнання послуг керування ідентифікацією та довірчих послуг, який забезпечує першу глобально узгоджену уніфіковану правову структуру для ідентифікації фізичних і юридичних осіб в Інтернеті, а також для надання гарантій щодо якості даних в електронній формі, в тому числі через кордонів. У 2022 році ЮНСІТРАЛ схвалила публікацію таксономії правових питань, пов'язаних із цифровою економікою, яка фіксує дослідницьку роботу секретаріату ЮНСІТРАЛ за темами штучного інтелекту, даних, онлайн-платформ, цифрових активів і децентралізованих систем, і яка призначена керувати пропозиціями щодо майбутньої законодавчої роботи щодо електронної комерції (цифрової торгівлі) та в інших сферах роботи.

Правове регулювання комерційної діяльності в українському цифровому просторі започатковано ухваленням Закону України «Про Національну програму інформатизації» у 1998 році⁶⁵. 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 році⁶⁶. 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.

Черговим документом, який відіграє не менш важливу роль є Закон України «Про захист правспоживачів». Так, даним Законом закріплюється правспоживачів на якісні товари та послуги, а також визначаються умови повернення товарів, в тому числі придбаних в електронній формі. Акт також передбачає обов'язок продавця надати покупцеві повну та достовірну інформацію про товар або послугу, що продається через Інтернет. Відтак, дані закони створюють правову основу для розвитку електронної комерції, забезпечуючи належне регулювання правовідносин між суб'єктами господарювання та споживачами, а також захист прав учасників в умовах цифрової економіки.

⁶⁵ Про Національну програму інформатизації : Закон України. Відомості Верховної Ради України (ВВР), 1998, № 27-28, ст.181.

⁶⁶ Про електронну комерцію : Закон України. URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text>

При теоретичному вивченні поняття «електронна комерція» варто виділити предмет, об'єкт, суб'єкт та рівні її функціонування. Щодо предмету електронної комерції – це будь-яка форма проведення комерційних операцій, таких як: торгівля, комерційне представництво й агентські відносини, факторинг, лізинг, будівництво промислових об'єктів, надання консультативних послуг, інжиніринг, купівля/продаж ліцензій, інвестування, фінансування, банківські послуги, страхування й інші форми промислової або підприємницької співпраці. Всі процеси, які складають зміст електронної угоди, наприклад, дослідження ринку, пошук комерційного партнера, платіжні операції, страхування ризиків тощо також є предметом е-комерції.

Об'єктом електронної комерції виступають певні товари, послуги та інформація, а також процес пошуку, замовлення, доставка та оплата, яка здійснюється виключно електронним способом.

Серед ключових елементів електронної комерції можна виділити наступні: 1) суб'єкти-учасники (виробники, постачальники, продавці, споживачі та уряд); 2) бізнес-процеси (продаж, оплата, логістика, виконання, маркетинг, підтримка, логістика, замовлення); 3) мережі та мережеві технології (Інтернет, Екстранет, Інтранет, програмне забезпечення корпоративні інформаційні системи щодо). Електронна комерція може функціонувати на трьох рівнях: перший рівень – Інтернет-комерція; другий рівень – електронна комерція; третій рівень – електронний бізнес.

Електронний бізнес – дуже динамічна галузь. Зараз технології е-бізнесу – один із важливих інструментів сучасної конкурентної боротьби. Впровадження інформаційних технологій в управління економікою на макро- та мікрорівнях є одним з головних чинників підвищення ефективності виробництва та забезпечення розвитку економіки. Впровадження комп'ютерних технологій і автоматизація управління підприємством робить можливим виникнення нових форм організації виробництва, що дає базис для функціонування віртуальних підприємств та електронної комерції. 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.

Отже, електронна комерція продовжує стрімко розвиватися, вимагаючи ефективного правового регулювання як на національному, так і на міжнародному рівнях. Міжнародний характер електронної комерції піднімає питання про гармонізацію законодавства різних держав, що є необхідним для забезпечення правової визначеності та захисту прав усіх учасників ринку. Неоднорідність правового регулювання, яка існує на рівні національних юрисдикцій, ускладнює функціонування суб'єктів електронної комерції, особливо в аспекті захисту прав споживачів, безпеки даних та забезпечення виконання електронних договорів⁶⁷.

⁶⁷ Берч В.В. Правове регулювання електронної комерції: міжнародні та національні стандарти // Науковий вісник Ужгородського Національного Університету, 2024. 2(85). С.11-16.

6.2. Електронний документообіг

Актуальність електронних документів для використання у господарській діяльності, взаємодії з державними органами та суді збільшується щодня. Документообіг є у кожному бізнесі. Це сукупність інформації, яка створюється та циркулює на підприємстві чи поступає ззовні або створюється для надання за межі компанії. Очевидно, що електронний документообіг в порівнянні з паперовим дозволяє вивести планування діяльності підприємства, облік та контроль на всіх етапах управління на новий рівень – комплексного підходу, системного аналізу та прогнозування. А це, в свою чергу, підвищує стійкість підприємства в умовах частих криз та знижує ризики в умовах невизначеності. Питання електронного документообігу та його впровадження на підприємствах та установах України можна назвати питанням загальнодержавного значення.

Документообіг буває внутрішній та зовнішній. **Внутрішній документообіг** (його ще іноді називають корпоративним) – це рух документів всередині компанії, тобто обмін документами між різними підрозділами та співробітниками однієї організації.

В межах однієї компанії відбувається створення, узгодження та підписання великої кількості документів – наказів, службових записок, заяв, інструкцій, статутів і багато іншого. Все це можна вести в електронному вигляді та автоматизувати. ЕДО дозволяє не лише перевести документи в електронний формат, а налаштувати процеси та організувати роботу з документами максимально зручно і швидко.

Внутрішній електронний документообіг дозволяє значно оперативніше створювати, узгоджувати та шукати документи, мати історію всіх файлів, організувати легкий доступ відповідальних співробітників до документів, контролювати, де знаходяться документи та на якому етапі виконання завдань із ними тощо.

Зовнішній документообіг – це рух документів за межами компанії, тобто обмін документами із контрагентами, клієнтами, партнерами, державними органами та іншими зовнішніми організаціями.

Зазавичай зовнішній документообіг передбачає погодження рахунків, актів виконаних робіт, звітів, накладних тощо. Електронний зовнішній документообіг дозволяє миттєво передавати документи контрагентам, не витрачаючи часу й коштів на друк та пересилку. А також ЕДО підвищує захист документів, тож обмін стає значно безпечнішим.

Надійний «фундамент» для розвитку ЕДО в Україні був побудований завдяки наступним етапам:

1. Затвердження організаційно-правових основ ЕДО та правил його використання. У 2003 році Верховна Рада ухвалила закон «Про електронні документи та електронний документообіг». Іншими словами, важливість ЕДО в Україні держава підтвердила на законодавчому рівні. Відтак, е-документ повинен мати обов'язкові реквізити, а також електронний підпис або підпис, прирівняний до власноручного, для ідентифікації власника.

2. Е-документу надали юридичної сили. У цьому ж 2003 році парламент ухвалив закон «Про електронний цифровий підпис». Тобто якщо документ з відповідними

реквізитами на ньому та електронним цифровим підписом (ЕЦП) має і паперовий, і електронний варіант, то обидва формати вважаються оригіналами й мають однакову юридичну силу.

3. Податкові звіти в електронному вигляді. Згодом у 2017 році держава затвердила Положення про застосування електронного підпису та електронної печатки банками України. Саме тоді згідно з Податковим кодексом України підприємці отримали можливість відправляти звітність онлайн в електронному вигляді.

4. Електронний документообіг для державних установ. Постанова Кабінету Міністрів № 55 від 17 січня 2018 року «Деякі питання документування управлінської діяльності» – це свого роду рекомендації для виконавчої влади перейти на електронний документообіг. У Постанові також було зафіксовано формат ЕДО для державних організацій.

5. З'явився кваліфікований електронний підпис. Також у 2018 році набрав чинності Закон України «Про електронні довірчі послуги», а Закон України «Про електронний цифровий підпис» відповідно втратив свою силу. Новий Закон роз'яснював поняття кваліфікованого електронного підпису (КЕП) замість ЕЦП. Тобто надав можливість користуватися сучасними електронними методами ідентифікації особи, зокрема MobileID або BankID.

Тож, завдяки цим законодавчим діям держави та появі хмарних технологій кожна з компаній може оптимізувати свої бізнес-процеси та функціонувати віддалено попри пандемії, кризи й воєнні умови. Технології допомагають працювати з електронними документами з будь-якого гаджета, підключеного до інтернету.

Компанія має право самостійно розробляти порядок електронного документообігу та обирати програмне забезпечення для його функціонування. Єдиною обов'язковою умовою є дотримання норм діючого законодавства в сфері електронного документообігу. Проте два головних документи, що регулюють ЕДО на підприємстві, це: *положення про ЕДО* та *наказ про ЕДО*: У положенні про ЕДО зазначаються умови ведення електронного документообігу (як створювати, хто приймає та перевіряє документ, як зберігає, як змінює чи знищує тощо). За допомогою наказу затверджується наявність ЕДО в компанії та список співробітників, які будуть працювати з е-документообігом. Створювати та оформлювати ці документи зазвичай допомагає юридичний відділ⁶⁸.

6. 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.

Етапи роботи з електронним документообігом зазвичай передбачають такі дії з документами:

- створення;

⁶⁸ Ганна Сухорукова Етапи розвитку ЕДО в Україні: від минулого до сучасності. Електронний ресурс. [//hub.kyivstar.ua/author/ganna-suhorukova](https://hub.kyivstar.ua/author/ganna-suhorukova).

- оброблення;
- відправлення / передавання;
- одержання /підтвердження факту одержання (при потребі);
- використання;
- зберігання;
- знищення.

Система електронного документообігу – це програмне рішення, яке дозволяє організувати роботу з е-документами та обмін ними всередині компанії чи з зовнішніми отримувачами. В системі ЕДО можна створювати документи, відправляти та отримувати їх на узгодження, підписувати, керувати рухом документів, розмежовувати доступ до них, зберігати та відправляти в архів тощо. Залежно від виду документообігу системи теж діляться на внутрішні (корпоративні) та зовнішні. Системи внутрішнього (корпоративного) документообігу дозволяють обмінюватися документами всередині компанії. А системи зовнішнього електронного документообігу – це рішення для обміну та підписання документів з контрагентами, клієнтами та іншими користувачами поза межами компанії. Обмінюватись документами з державою можливо через офіційні ресурси. Багато сервісів надають можливість відправити звіт до податкової служби. Також це можна зробити на сайті cabinet.sfs.gov.ua, маючи лише ЕЦП. На сайтах інших державних установ теж можна замовити електронний документ. Наприклад, запит до ЄДР здійснюється на порталі minjust.gov.ua, а до інших державних органів на сайті kmu.gov.ua.

Ринок програмних продуктів України пропонує різноманітні програмні рішення для підприємств щодо впровадження або вдосконалення електронного документообігу – як внутрішнього, так і зовнішнього. Існують безкоштовні сервіси, створені з урахуванням всіх вимог українського законодавства. До таких відноситься Paperless – сервіс для компаній та підприємців по обміну документами між собою в електронній формі. Серед платних сервісів найбільш популярними в Україні є сервіси електронного документообігу M.E.Doc (від компанії Укрзвіт), ВЧАСНО, Document.Online, Арт-Офіс, Comarch EDI, FossDoc та інші.

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 форму⁶⁹.

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

⁶⁹ 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>

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 кільком 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»⁷⁰ 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

⁷⁰ 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>

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. II 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 господарської та правильність її оформлення; особистий підпис або інші дані, які дозволяють ідентифікувати особу, яка взяла участь у господарській операції. 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.

Переваги та недоліки електронного документообігу

Електронний документообіг зручніший за паперовий, адже не потрібно друкувати документи та відправляти їх чи носити по кабінетах на підпис. Крім цього, фахівці виділяють наступні переваги ЕДО:

- документи відправляються миттєво, навіть якщо контрагент знаходиться в іншій країні. Процес узгодження та підписання документів не зупиняється, навіть якщо керівник у від'їзді. До того ж деякі вендори пропонують системи, що мають мобільні застосунки;

- можна відправити документи кільком адресатам одночасно. Узгоджувати документи можна послідовно чи паралельно, ви можете легко зробити такі маршрути погодження, як вам потрібно;

– доступні шаблони документів, які ви робите один раз, і потім всі співробітники ними користуються, щоб швидко і без помилок створювати документи. Шаблони вже мають обов'язкові поля, тому неможливо забути внести важливу інформацію – система не збереже документ без неї;

– економія коштів на друці та пересилці документів;

– кращий рівень конфіденційності, адже доступ до документів в системі контролюється адміністратором. Це гарантує, що документ побачать тільки ті співробітники/відділи, які мають на це право. До того ж, система дозволяє вести аудит всіх дій з кожним документом та контролювати, хто й коли саме щось змінював;

– для зберігання електронних документів не потрібен фізичний архів, що дуже зручно для великих компаній, яким потрібні великі приміщення, щоб вмістити всі документи й організувати роботу з ними. Електронний документообіг в архіві дозволяє зберігати безліч документів в е-форматі, миттєво їх вивантажувати та шукати.

Якщо говорити про недоліки електронного документообігу, до них можна віднести небезпеку проникнення вірусів в документи. Але зазвичай ця проблема вирішується завдяки надійним системам документообігу. Наприклад, Megapolis.DocNet має вбудований антивірус, який автоматично перевіряє всі вхідні документи та поміщає небезпечні в карантин⁷¹.

Також до недоліків можна віднести небажання співробітників переходити на нові технології; додаткові фінансові витрати, витрати часу на впровадження та адаптацію; неможливість працювати з усіма контрагентами в електронному середовищі через те, що вони ще не перейшли на електронний документообіг.

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 та електронний підпис?

⁷¹ Електронний документообіг: системи, види, особливості впровадження та як він працює в Україні. Електронний ресурс. <https://inbase.com.ua/elektronnyj-dokumentobig-sistemy-vydy-osoblyvosti-vprovadzhennya-ta-yak-vin-praczuuye-v-ukrayini/>

РОЗДІЛ 7.

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

Електронні гроші як інноваційний фінансовий інструмент з'явилися на початку 90-х років минулого століття, коли Інтернет почав розповсюджуватися по всьому світу і охоплювати широкі маси користувачів. Саме розвиток Інтернет, як глобального інтерактивного засобу комунікації, сприяв подальшій еволюції грошей, створивши умови для винаходу, створення і розвитку їх нової форми – електронних грошей. Винахідником і першим розробником електронних грошей є американський вчений-інформатик, кріптограф Девід Чаум, який результати своїх досліджень виклав у опублікованій в 1981 році статті «Невідстежувана електронна пошта, зворотні адреси та цифрові псевдоніми» де обґрунтував ідеї «сліпого підпису», «цифрового конверта» і описав технологію використання електронних грошей, яка дозволяла здійснювати фінансові транзакції анонімно. Свій науковий задум Девід Чаум реалізував на практиці, створивши комерційну компанію DigiCash, яка розробила платіжну систему e-Cash для безпечної оплати товарів і послуг в Інтернеті електронними грошима і у 1994 році провела перший електронний платіж. У цьому ж році робочою групою з платіжних систем ЄС, яка складалася із представників європейських банків, уперше було використано термін «електронні гроші», існування електронних грошей було визнане на офіційному рівні⁷². 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 грошах⁷³. 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»⁷⁴. У вітчизняному законодавстві застосування і використання електронних грошей регламентується окремим законодавчим нормативним актом – Законом України «Про

⁷² О. В. Поштаренко До питання зародження електронних грошей // Прикарпатський юридичний вісник. Випуск 6 (53), 2023. С.95-99. http://pjuv.nuoua.od.ua/v6_2023/19.pdf

⁷³ Б. Дучак Електронні гроші в Україні третього світу / URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ000975

⁷⁴ 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

платіжні послуги» (далі – Закон)⁷⁵, а також Положенням Про випуск електронних грошей та здійснення платіжних операцій з ними, затвердженим Постановою правління Національного Банку України від 29.09.2022 № 210⁷⁶. Відповідно до Закону «**електронні гроші**» – одиниці вартості, що зберігаються в електронному вигляді, випущені емітентом електронних грошей для виконання платіжних операцій (у тому числі з використанням наперед оплачених платіжних карток багатоцільового використання), які приймаються як засіб платежу іншими особами, ніж їх емітент, та є грошовим зобов'язанням такого емітента електронних грошей. Крім цього, Закон вводить новий для нашого законодавства термін – «цифрові гроші Національного банку України» (далі - **цифрові гроші**) - електронна форма грошової одиниці України, емітентом якої є Національний банк України. Ширше за змістом поняття цифрових грошей передбачене ч. 2 ст. 35 Закону України «Про Національний банк України», зокрема: «Цифрові гроші Національного банку як електронна форма грошової одиниці України є законним платіжним засобом на території України, приймається фізичними і юридичними особами для проведення платіжних операцій та розрахунків виключно у випадках, передбачених законодавством України». Можна виділити наступні істотні ознаки цифрових грошей:

- цифрові гроші є різновидом коштів у безготівковій формі;
- цифрові гроші є електронною формою грошової одиниці України;
- цифрові гроші є законним платіжним засобом на території України;
- цифрові гроші використовуються для проведення платіжних операцій та розрахунків виключно у випадках передбачених законом;
- емітентом цифрових грошей є Національний банк України;
- цифрові гроші підлягають погашенню.

Сьогодні нормативний матеріал щодо Е-гривні обмежується лише загальними положеннями, що визначають її поняття. Е-гривня – це електронна форма грошової одиниці України, емітентом якої є Національний банк. Ключове призначення е-гривні, на думку регулятора, – ефективно виконувати всі функції грошей, доповнюючи готівкову та безготівкову форми гривні. Національний банк у вересні 2021 року відкрив проєкт «Е-гривня», метою якого є визначення потреби широкомасштабного випуску в Україні цифрової форми гривні. У жовтні 2022 року ДП «УКРАЇНСЬКИЙ ІНСТИТУТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ» (УКРПАТЕНТ) зареєструвало торговельну марку «е-гривня» та «e-hryvnia», яка належить Національному банку.

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 грішима⁷⁷. Для

⁷⁵ Про платіжні послуги : Закон України від 30.06. 2021 № 1591-ІХ. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#n1249>

⁷⁶ Про випуск електронних грошей та здійснення платіжних операцій з ними. URL: <https://zakon.rada.gov.ua/laws/show/v0210500-22#Text>

⁷⁷ В. Кравчук, Д. Науменко, А. Глибовець. Електронні гроші в Україні. Аналітичний звіт. – К. : Альфа ПІК, 2012. – 64с.

проведення платіжних операцій використовуються кошти в готівковій або безготівковій формі. Електронні гроші та цифрові гроші існують лише в безготівковій формі.

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*», розширено поняття «*емітентів електронних грошей*». Насьогодні, **емітентом електронних грошей** вважається установа електронних грошей або інша визначена Законом юридична особа, яка надає платіжні послуги з випуску електронних грошей та виконання платіжних операцій з ними, у тому числі відкриття та обслуговування електронних гаманців, та має право на надання такої платіжної послуги відповідно до Закону.

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

- зобов'язаний перед укладенням договору з користувачем інформувати його про створення електронного гаманця та отримати його згоду; електронний гаманець не поповнюється електронними грошима, що надходять від неідентифікованих споживачів; електронний гаманець поповнюється та використовується на загальну максимальну суму платежів не більше ніж 5000 гривень;
 - фіксувати та зберігати інформацію про всі операції/транзакції з електронними грошима;
 - надавати кредит електронними грошима;
 - 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:

1. Емітент електронних грошей. Емітентами електронних грошей в Україні можуть бути виключно такі особи: банки; установи електронних грошей; філії іноземних платіжних установ; оператори поштового зв'язку; Національний банк України; органи державної влади, органи місцевого самоврядування.

Для набуття статусу емітента електронних грошей та отримання права на надання послуги з випуску та виконання платіжних операцій з електронними грошима, у тому числі відкриття та обслуговування електронних гаманців, особа (крім Національного банку України, банків, органів державної влади, органів місцевого самоврядування) має отримати ліцензію на надання фінансових платіжних послуг у порядку, визначеному Законом та нормативно-правовими актами Національного банку України (ст. 57 Закону «Про платіжні послуги»). Мінімальний розмір статутного капіталу юридичної особи (крім юридичної особи, що має намір надавати платіжні послуги у статусі малої платіжної установи), яка надає або має намір надавати платіжні послуги з випуску та виконання платіжних операцій з електронними грошима, у будь-який час не може становити менше 10 мільйонів гривень (ст.16 Закону).

2. Іноземна платіжна установа/іноземна установа електронних грошей (далі - іноземна платіжна установа) - юридична особа - нерезидент, яка відповідно до законодавства держави, в якій вона зареєстрована, має право надавати платіжні послуги;

1. Комерційний агент (агент) - юридична особа або фізична особа-підприємець, яка діє від імені, в інтересах, під контролем і за рахунок особи, яку вона представляє під час надання платіжних послуг на підставі відповідного договору;

2. Користувач платіжних послуг (далі - користувач) - фізична особа або юридична особа, яка отримує чи має намір отримати платіжну послугу як платник або отримувач (або обидва одночасно) та/або є власником електронних грошей (цифрових грошей Національного банку України), а в разі надання послуг банком - клієнт банку.

Закон виділяє користувачів-споживачів, користувачів - суб'єктів господарювання та користувачів, які є органами державної влади або органами місцевого самоврядування. Їх права регламентуються ст. 60 Закону «Про платіжні послуги».

Випуск електронних грошей здійснюється емітентом електронних грошей шляхом їх надання користувачам відповідно до умов договору. Споживачі мають право отримувати електронні гроші в обмін на готівкові кошти або кошти, перераховані з поточних або платіжних рахунків. Електронні гроші вважаються випущеними з моменту отримання емітентом (комерційним агентом) коштів 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, що здійснює випуск електронних грошей, зобов'язаний погашати випущені ним електронні гроші на вимогу користувача. Негайно після пред'явлення

користувачем електронних грошей до погашення (у тому числі через комерційного агента) емітент електронних грошей зобов'язаний здійснити погашення електронних грошей та забезпечити виплату користувачу відповідної суми коштів в обмін на вилучені з обігу електронні гроші.

Значущі зміни в сферу електронних платежів вніс Закон України «Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг»⁷⁸: Ці новації можна класифікувати на три групи, що:

1) розширюють спектр розрахунків: – передбачена можливість здійснення розрахунків за відвантажені товари (виконані роботи, надані послуги) з використанням електронних грошей платниками єдиного податку I-III групи; – передбачена можливість сплати податків і зборів електронними грошима;

2) регулюють режим оподаткування: – віднесення до поняття "дохід з джерелом їх походження з України" дохід надавачів платіжних послуг від здійснення діяльності на платіжному ринку і при цьому не вважається доходами кошти, що отримуються надавачами платіжних послуг від користувачів платіжних послуг для здійснення платіжних операцій; – віднесено до операцій, що не є об'єктом оподаткування ПДВ, випуск та погашення електронних грошей, а також надання послуг, пов'язаних з виконанням платіжних операцій, що надаються надавачами платіжних послуг, операторами платіжних систем, розрахунково-касовим обслуговуванням;

3) адмініструють діяльність: – поширені вимоги щодо можливості відкриття і ведення рахунків клієнтам виключно за умови взяття таких клієнтів на облік у контролюючих органах; – поширена відповідальність за порушення строку та порядку подання інформації про відкриття або закриття рахунків на небанківських надавачів платіжних послуг.

Окремо варто зосередити увагу, що згаданий Закон, окрім того, що легалізує електронні гроші, фактично прирівнює рахунки електронних гаманців до рахунків банків⁷⁹.

Види електронних грошей

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

1. За типом носія:

а) *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);

б) *на базі програмного забезпечення* (англ. Network-based чи software-based), або їх ще називають онлайн-грошима. В цьому випадку електронні гроші зберігаються на накопичувачах інформації у формі файлів бази даних/масиву

⁷⁸ Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг: Закон України від 12.01.2023 № 2888–ІХ. <https://zakon.rada.gov.ua/go/2888-20>

⁷⁹ Грицай С.О. Електронні гроші: поняття та нові аспекти використання// Forum Prava, 2023. 74(1). С. 141–150. http://forumprava.pp.ua/files/141-150-2023-1-FP-Hrytsai_15.pdf

інформації. А при здійсненні транзакції запит до оператора електронних грошей є обов'язковим для завершення операції.

2. За типом технології зберігання:

а) із *централізованим веденням рахунків* (англ. account-based): всі транзакції записуються та ідентифікуються через централізовану систему рахунків, управління якою здійснює система електронних грошей;

б) 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).

3. За ступенем анонімності:

а) *повністю анонімні* системи електронних грошей: ідентифікація користувача не вимагається ані при придбанні ним електронних грошей, ні при здійсненні ним транзакцій. Таким чином, ідентифікація та відстеження здійснених операцій між платником та отримувачем платежу є неможливою;

б) 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;

в) 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.

4. За розміром платежу:

а) системи *пікоплатежів* (англ. micropayments): можуть здійснюватись платежі розміром від менш ніж 1 євроценту до 1 євро;

б) 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;

в) системи макрорплатежів: можуть здійснюватись транзакції більшого розміру⁸⁰.

Запитання для самоконтролю і самостійного опрацювання

1. Що таке електронні гроші?
2. Хто може випускати електронні гроші в Україні?
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?
5. Що таке е-гривня?
6. В чому полягає різниця між е-грошима і безготівковими грошима?
7. В чому різниця між е-грошима і національною валютою?

⁸⁰ В.Кравчук, Д.Науменко, А.Глибовець. Електронні гроші в Україні. Аналітичний звіт. – К.: Альфа ПІК, 2012. – 64 с.

РОЗДІЛ 8. ПРАВОВИЙ РЕЖИМ ВІРТУАЛЬНОЇ ВАЛЮТИ (КРИПТОВАЛЮТИ)

8.1. Зміст та юридична природа криптовалюти

Розвиток цифрової економіки був надзвичайно швидким у другому десятилітті 21-го століття, спричинивши значні прориви на всіх ринках. Сучасні технологічні інновації більше не розглядаються як питання додаткової ефективності, а радше як необхідність для довголіття бізнесу. Розрив між традиційними економічними процесами та цифровими економічними процесами скорочується швидше, ніж будь-коли раніше. Центральні банки в усьому світі серйозно розглядають впровадження цифрових валют центральних банків (CBDC) і запроваджують інноваційні блокчейн-стратегії для стимулювання економічного зростання. В Україні активно продовжується інформатизація економіки, важливим елементом якої є використання цифрових валют. За даними щорічного звіту аналітичної компанії Chainalysis «Глобальний індекс впровадження криптовалют» – українці є активними користувачами криптовалюти в світі. Країна у 2020 році займала першу сходинку цього рейтингу. У 2021 році Україна мала вже 4-е місце, пропустивши вперед В'єтнам, Індію і Пакистан, у 2022-третє, а у 2023 стала п'ятою. У 2024 році Україна залишається в TOP-10 і займає 6-е місце в цьому рейтингу⁸¹. В свою чергу Triple A, фінтех-компанія, яка дозволяє компаніям обробляти платежі та виплати в цифровій валюті, нещодавно опублікувала звіт «Стан глобального володіння криптовалютою у 2024 році», в якому зазначає, що 562 мільйони людей у світі зараз володіють цифровими валютами, що більше за 420 мільйонів у 2023 році, і становить 6,8% населення планети. За їх оцінками, приблизно 6,5 мільйонів українців, або 15,72% від загальної кількості населення, володіють криптовалютою⁸². Капіталізація світового ринку криптовалют станом на початок 2025 року становила 3,45 трильйона доларів США⁸³. 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 криптовалют 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».

⁸¹ The 2024 Global Adoption Index: Central & Southern Asia and Oceania (CSAO) Region Leads the World in Terms of Global Cryptocurrency Adoption. September 11, 2024. <https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/>

⁸² Triple A. The State of Global Cryptocurrency Ownership in 2024. <https://www.triple-a.io/cryptocurrency-ownership-data>

⁸³ Ціни на криптовалюту за ринковою капіталізацією. <https://www.coingecko.com/>

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. Вказана концепція була викладена у його програмній статті «Bitcoin: A Peer-to-Peer Electronic Cash System»⁸⁴, яка була оприлюднена в мережі (на веб-сайті <https://bitcoin.org/>) і в якій було обґрунтовано з технічної точки зору можливість використання інформаційних технологій для електронних готівкових (однорівневих) розрахунків. 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. Саму назву «криптовалюта» (з огляду на криптографічну філософію створення даного продукту та платіжну ідею, що лежала в основі її створення) запропонував оглядач журналу «Forbes» Енді Грінберг у статті, опублікованій ним у 2011 році⁸⁵. Пропозиція виявилася вдалою і термін став загальнопоширеним.

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 виражений у їх власній розрахунковій одиниці.

Вперше в Україні рекомендаційні роз'яснювальні документи, якими намагались врегулювати сферу криптовалюти, з'явилися ще в 2014 році. НБУ опублікував Роз'яснення «Щодо правомірності використання в Україні «віртуальної

⁸⁴ «Біткоїн: електронна пірінгова система готівки». URL: https://bitcoin.org/files/bitcoin-paper/bitcoin_uk.pdf

⁸⁵ Andy Greenberg. Crypto Currency. URL: <https://www.forbes.com/forbes/2011/0509/technologypsilocybinbitcoins-gavinandresencryptocurrency.html#718ca248353e>

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 135 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»⁸⁶ (Закон № 2074), 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.

⁸⁶ Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>

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 (відмивання) 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 правильним⁸⁷. Саме тому, в подальшому було прийнято Закон України «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав» від 10.08.2023 №3320-IX, відповідно до якого ЦКУ було доповнено новою статтею 179-1 «Поняття цифрової речі». Так, цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність. Цифровою річчю є віртуальні активи, цифровий контент та інші блага, щодо яких застосовуються положення частини першої цієї статті.

Частина 3 статті 179-1 ЦКУ передбачила, що до цифрових речей застосовуються положення про речі, якщо інше не встановлено цим Кодексом, законом або не впливає із сутності цифрової речі. Однак, ці зміни до ЦКУ викликали потребу в уточненні, а як саме на віртуальні активи має поширюватись режим речей: наприклад, чи вони є подільними чи неподільними, чи можна якісь токени визначати похідними речами до інших токенів тощо. І поки тривали дискусії щодо змін до ЦКУ та класифікації, в червні 2023 року було оприлюднено Регламент (ЄС) 2023/1114 Європейського парламенту та Ради від 31 травня 2023 року про ринки криптоактивів (Markets in Crypto-Assets Regulation або Регламент MiCA), який передбачає регулювання віртуальних активів у ЄС. Зокрема, Регламентом MiCA надано чітке визначення основних термінологічних понять на ринку віртуальних активів, класифікацію віртуальних активів та послуг щодо віртуальних активів, які надаються професійними постачальниками таких послуг, а також визначено чітке розмежування повноважень щодо регулювання ринку віртуальних активів між компетентними органами, з одночасним врегулюванням питання боротьби із зловживаннями на ринку віртуальних активів, через встановлення вимог до публічної пропозиції окремих видів віртуальних активів, а також допуску до торгів.

А, зважаючи на отримання Україною статусу кандидата на членство в ЄС, та, що норми українського законодавства щодо віртуальних активів мають відповідати європейським стандартам, вже стало очевидним та безапелюсним, що запуск ринку

⁸⁷ Іван Лясківський. Новий закон про віртуальні активи – нові можливості для бізнесу. URL: <https://ain.ua/2021/09/13/novij-zakon-pro-virtualni-aktivi-novimozhливosti-dlya-biznesu-kolonka-yurista/>

віртуальних активів в Україні не може відбутись без попереднього оновлення редакції Закону №2074-IX⁸⁸.

Таким чином, при правовій неузгодженості термінології ми звертаємось до наукових досліджень юридичної природи і змісту криптовалюти. Так, Логойда В.М. пропонує таке визначення: «*Криптовалюта* – це віртуальний актив (різновид цифрових приватних грошей) з відкритим вихідним кодом, заснований на технології розподіленого реєстру або подібній технології, який не має центрального адміністратора, захищається засобами криптографії та використовується в однорангових (децентралізованих) віртуальних мережах між їх учасниками та за їх згодою в якості міри вартості та засобів обігу, платежу і збереження вартості»⁸⁹. В свою чергу В. Д. Іванюк запропонувала своє авторське визначення поняття криптовалюта: «*Криптовалюта* – це альтернативний засіб платежу, номінований у власній розрахунковій одиниці, врегульований фінансово-правовими нормами, використання якого базується на криптографічних методах для забезпечення фінансових транзакцій з метою погашення боргових зобов'язань»⁹⁰. В дисертаційному дослідженні Могил Людмили сформульовано визначення *криптовалюти* як економіко-правової фікції, що є взаємозамінним різновидом віртуального активу у формі шифрованого електронного запису, емісія та облік якого виконується децентралізовано на основі технології розподіленого реєстру та криптографічних алгоритмів, який є об'єктом речових прав та здатен виконувати обігові і накопичувальні функції⁹¹.

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: грошовими коштами; грошовим сурогатом; товаром (майно, актив); майновим правом; формою платіжної послуги⁹².

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

⁸⁸ Форсюк В. Чому в Україні так і не запрацював Закон України «Про віртуальні активи». URL: <https://rates.fm/ua-uk/expert-opinion/chomu-v-ukrayini-tak-i-ne-zaprasyuvav-zakon-ukrayini-pro-virtualni-aktivy/>

⁸⁹ Логойда В. М. Криптовалюти як об'єкт цивільних прав: порівняльно-правовий аналіз. Дисертація на здобуття вченого ступеня доктора філософії у галузі права. Ужгород: УНУ, 2022. URL: [file:///C:/Users/pagin/Downloads/%D0%B4%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F%20\(%D0%9B%D0%BE%D0%B3%D0%BE%D0%B9%D0%B4%D0%B0%20%D0%92.%D0%9C.\).pdf](file:///C:/Users/pagin/Downloads/%D0%B4%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F%20(%D0%9B%D0%BE%D0%B3%D0%BE%D0%B9%D0%B4%D0%B0%20%D0%92.%D0%9C.).pdf).

⁹⁰ Іванюк В.Д. Фінансово-правове регулювання ринку криптовалют в Україні. Дисертація на здобуття вченого ступеня доктора філософії у галузі права. Тернопіль: ЗНУ, 2021. URL: <https://www.wunu.edu.ua/svr/disertacia/ivanuk/dusertacia.pdf>

⁹¹ Могил Л. С. Правове забезпечення використання криптовалют в господарському обігу : дис...доктора філос. / Могил, Людмила Сергіївна ; Національний університет «Одеська юридична академія» – Одеса, 2023. – 223 с. URL: <https://dspace.onua.edu.ua/items/ca9af90b-a30f-454d-b28e-da1b842aa4cc>.

⁹² Кремінський, О. Правовий режим віртуальної валюти (криптовалюти) в Україні. Path of Science. 2020. Vol.6, №4. С. 1001-1008. URL: <https://cyberleninka.ru/article/n/pravoviy-rezhim-virtualnoyi-valyuti-kriptovalyuti-v-ukrayini/viewer>.

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)⁹³. Але багато компаній декларують, що їхня криптовалюта чимось підкріплена і забезпечена. Аналітики Worldscore склали рейтинг ТОП-10 криптовалют із найоригінальнішим забезпеченням (рис. 1)⁹⁴.

№	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. 1. ТОП-10 криптовалют із найнезвичайнішим забезпеченням, заявлені до випуску у світі

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 тільки 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

⁹³ 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%20rehulivannia_Kaznachieieva_Dorosh_2020.pdf?sequence=1&isAllowed=y.

⁹⁴ Урожай перцю та нафта: опубліковано ТОП-10 незвичайних підкріплень для криптовалют. <https://minprom.ua/opinion/242993.html>.

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.

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 адміністратора⁹⁵. 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 криптовалют, 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 криптовалют і по-різному вирішують спори щодо її обігу⁹⁶:

8.2. Правовий режим криптовалют у світі: підходи до регулювання

На думку експертів визнання на державному рівні технології блокчейн і одного з продуктів її реалізації – криптовалют, 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. На сьогодні серед регуляторів провідних країн світу, зокрема країн Європейського Союзу, немає єдиного підходу до визначення правового статусу криптовалют та регулювання операцій з ними. Оподаткування криптовалют і операцій з ними здійснюється відповідно до

⁹⁵ Олег Кременський Правовий режим віртуальної валюти (криптовалюти) в Україні. Path of Science. 2020. Vol.6, №4. С.1001-1008. <https://cyberleninka.ru/article/n/pravoviy-rezhim-virtualnoyi-valyuti-kriptovalyuti-v-ukrayini/viewer>.

⁹⁶ Сергій Лисенко Правовий захист операцій із криптовалютами: примарний чи реальний? <https://unba.org.ua/publications/6558-pravovij->

національного законодавства державчленів Європейського союзу, наприклад, в Норвегії, Фінляндії і Німеччині криптовалюта оподатковується податком на приріст капіталу (Capital Gains Tax) і податком на багатство (Wealth Tax). В Австрії криптовалюта розглядається податковими органами як нематеріальний актив, а її майнінг – як операційна діяльність. А дохід, що одержано в результаті її відчуження, обкладається податком на прибуток (Income Tax).

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 засобом⁹⁷.

У Болгарії криптовалюта визнана фінансовим активом та обкладається відповідними податками.

У Фінляндії криптовалюта визначається як фінансовий інструмент, операції з ними вважаються приватними угодами й звільнені від ПДВ. У Швейцарії криптовалюта прирівняна до іноземних валют – операції з нею звільнені від ПДВ, але оподатковуються як майно.

Уряд Естонії не визнає криптовалюту законним платіжним засобом, а розглядає її як «вартість, представлену в цифровій формі», тому класифікує криптовалюти як цифрові активи для оподаткування, але не обкладає їх ПДВ. Проте криптовалютні біржі вважаються законними, якщо зареєстровані згідно вимог. В Естонії діють правила щодо фінансових прогнозів та складання бізнеспланів, а підрозділ фінансової розвідки може відмовити в ліцензії, якщо суб'єкт господарювання не проводить бізнес-операції в Естонії та не має жодного явного зв'язку з країною. Також є вимога аудиту компанії та підтвердження професійних навичок й несудимості засновників компанії.⁹⁸

⁹⁷ 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/publications/65.pdf>

⁹⁸ Івахно В. Криптовалюта в Україні: регулювати чи дозволити згоріти? URL: <https://loyer.com.ua/uk/kryptovalyuta-v-ukrayini-regulyuvaty-chy-dozvolity-zgority/>

У Хорватії, Киргизстані, Індонезії та Литві криптовалюта не визнана легальним засобом платежу, а в Болівії та Бангладеш її обіг взагалі заборонений.

На сьогодні однією з найбільш сприятливих і комфортних країн для ведення криптовалютного бізнесу вважається Великобританія. На сьогодні цифрова валюта у Великобританії вважається унікальною комбінацією цифр, яка отримана в результаті складних математичних обчислень і алгоритмів. Дохід, отриманий в результаті майнінга цифрових грошей і їх обміну на фунт стерлінгів або іншу валюту, не повинен обкладатися податком на додану вартість (Value Added Tax).

В США існують великі хеджфонди, біржі та інші компанії, пов'язані з криптовалютами, а за деякі товари можна розрахуватися не тільки фіатними, а і цифровими грошима, але правове регулювання криптовалютних операцій залишається не менш складним, ніж в Європі. В основному це обумовлено наявністю як федерального права, так і права штатів і відсутністю єдиної позиції серед регуляторів щодо правового статусу криптовалют. Наприклад, Штат Каліфорнія першим з усіх штатів США на законодавчому рівні дозволив використовувати криптовалюту. А в штаті Нью Йорк ведення бізнесу пов'язаного з криптовалютами було врегульовано в серпні 2015 року, коли була введена BitLicense – ліцензія на ведення криптовалютного бізнесу. Треба зазначити, що через рік після введення ліцензії її отримали лише Bitcoin гаманець «Circle» і Фінансово-технічний стартап «Ripple», а такі гравці ринку, як «Poloniex», «ShapeShift» та «Kraken» припинили діяльність у цьому штаті. При цьому ведення криптовалютного бізнесу в штаті залишилось не врегульованим. Треба зазначити, що в Сполучених Штатах Америки цифрова валюта розглядається одночасно як гроші (їх аналог), як власність і як біржовий товар⁹⁹.

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,

⁹⁹ Ткачук І.І. Статус криптовалют в Україні та інших країнах світу. Економіка і суспільство. Випуск № 16 / 2018. С.521-526. https://economyandsociety.in.ua/journals/16_ukr/79.pdf.

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 криптобінники 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 заборонаю 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 згорання інноваційних проєктів у цій сфері і перенесення їх у прозорішу регулятивну юрисдикцію¹⁰⁰.

Запитання для самоконтролю і самостійного опрацювання

1. Що таке криптовалюта і чим вона відрізняється від електронних грошей?
2. Назвіть основні ознаки кріптавалюти.
3. В чому полягає державний нагляд криптовалютного бізнесу?
4. Статус криптовалют в Україні.

¹⁰⁰ Шинкаренко О. М., Рогова Н. В., Панівнік І. А. Особливості нормативного регулювання криптовалют: світовий досвід. Фінансовий простір. 2018 № 3 (31). С. 139-144.

РОЗДІЛ 9.

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

Сучасний етап розвитку України безпосередньо впливає на стан її інформаційної безпеки. При цьому інформаційні відносини є ключовим компонентом діяльності органів державної влади, державного управління та інститутів громадянського суспільства, пов'язаних зі створенням, перетворенням і споживанням інформації. 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 15-й національний індекс кібербезпеки; 76-й глобальний індекс кібербезпеки та 43-й індекс мережевої готовності (рис. 2)¹⁰¹.

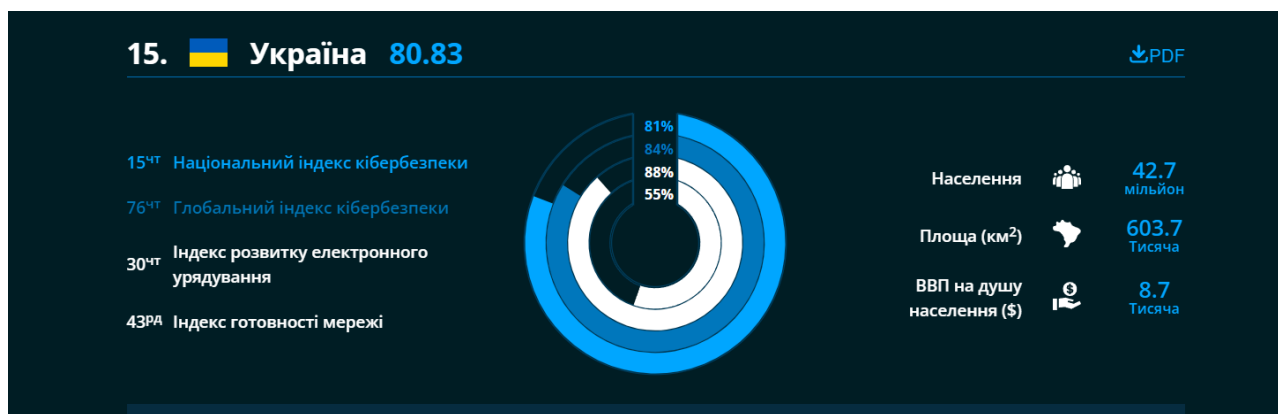


Рис. 2. Національні індекси кібербезпеки

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 груп¹⁰². Істотну проблему становить поширення інформаційної злочинності (кіберзлочинності), в тому числі діяльність організованих

¹⁰¹ Офіційний сайт Академії електронного управління Естонії. URL: <https://ncsi.ega.ee/country/ua/>

¹⁰² 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. 216 ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). URL: <https://doi.org/10.1007/978-3-030-66717-7>.

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 додатків¹⁰³. Тому не випадково питання забезпечення інформаційної безпеки включені практично в усі розділи, присвячені реалізації стратегічних національних пріоритетів Стратегії національної безпеки України¹⁰⁴. Окреслені в Стратегії положення отримали свій розвиток і в Стратегії воєнної безпеки України¹⁰⁵. 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.

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.

9.1. Загальні відомості про юридичну відповідальність в ІТ-сфері

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

¹⁰³ Спіціна 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.

¹⁰⁴ Стратегія національної безпеки України: Указ Президента України №121/2021. URL: <https://www.president.gov.ua/documents/3922020-35037>.

¹⁰⁵ Стратегія воєнної безпеки України: Указ Президента України № 392/2020. URL: <https://www.president.gov.ua/documents/1212021-37661>.

оперуємо надалі. 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 правопорушення¹⁰⁶. Основними відмінними 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) 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;

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. Насамперед це обумовлено відсутністю визначення цього поняття у нормативно-правових актах України. 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.

¹⁰⁶ Каленіченко 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.

68 Конституції: «Кожен зобов'язаний неухильно дотримуватися Конституції України та законів України, не посягати на права і свободи, честь і гідність інших людей. Незнання законів не звільняє від юридичної відповідальності»¹⁰⁷.

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. 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. 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. 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.¹⁰⁸ 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.

¹⁰⁷ Конституція України. Відомості Верховної Ради України (ВВР), 1996, № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>

¹⁰⁸ 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. Белякова. Київ : КВІЦ, 2019. С 108.

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.

Чинне законодавство не містить положень щодо визначення категорії **«інформаційно-правова відповідальність»**. Незважаючи на це, інформаційно-правова відповідальність існує об'єктивно. Про існування такої відповідальності свідчить наявність Закону України «Про інформацію», Закону України «Про телебачення і радіомовлення», Закону України «Про захист персональних даних», Закону України «Про доступ до публічної інформації», у яких не передбачаються санкції за правопорушення в інформаційній сфері, однак містяться переліки правопорушень. Наприклад, ст. 37 Закону України «Про інформацію» заборонено розголошувати зміст документів, які становлять внутрішньовідомчу службову кореспонденцію (довідних записок, переписки між підрозділами тощо), якщо вони пов'язані з розробкою напряму діяльності установи, процесом прийняття рішень і передують їх прийняттю; також заборонено розголошувати інформацію фінансових установ, підготовлену для контрольно-фінансових відомств. В інформаційних

правопорушеннях інформаційна складова є невід'ємною від предмета правопорушення. Предметом необхідно розуміти інформацію як документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі й навколишньому середовищі. Тобто предметом інформаційного правопорушення є конкретні об'єкти матеріального світу, щодо яких учинено правопорушення. Отже, інформаційне правопорушення – це протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на врегульовані законом суспільні відносини, що виникають під час здійснення інформаційної діяльності (отримання, використання, поширення та зберігання учасниками інформаційних правовідносин інформації), і за яку законом передбачено інформаційну відповідальність¹⁰⁹.

Варто також підкреслити, що порушення норм інформаційного права зумовлює не лише власне інформаційно-правову відповідальність, а й відповідальність, передбачену іншими галузями права. Інформаційна відповідальність може реалізовуватись паралельно з адміністративною, кримінальною, цивільною й дисциплінарною. При цьому в різних випадках інформація може відігравати як головну, так і другорядну роль. За висновками фахівців, на сьогодні найбільш поширеними правопорушеннями в інформаційній сфері є проступки. Вони характеризуються незначною небезпекою (шкідливістю для суспільства), вчиняються в різних галузях інформаційної діяльності, спрямовані на різні об'єкти і мають різні юридичні наслідки. Насамперед це: цивільні, дисциплінарні та адміністративні правопорушення в сфері інформаційно-майнових відносини та що порушують інтереси інформаційних відомств, організацій та структур, фірм та тощо.

1. *Цивільне правопорушення* – це протиправне діяння, що завдає шкоди майновим і пов'язаним з ними особистим немайновим інтересам суб'єкта. Об'єкт цього правопорушення – майнові або пов'язані з ними немайнові цінності. Залежно від характеру цивільно-правового порушення розрізняють:

- договірні правопорушення, які пов'язані з порушенням обов'язків сторін цивільно-правового договору;
- позадоговірні правопорушення, які пов'язані з недотриманням чи невиконанням вимог цивільно-правових норм.

До громадян, інформаційних відомств, структур тощо можуть бути в суді пред'явлені претензії і вони зобов'язані відшкодувати завдані збитки чи шкоду або відновити порушені інформаційні права. Наприклад, ч. 2 ст. 1076 ЦК говорить: «У разі розголошення банком відомостей, що становлять банківську таємницю, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди». Суб'єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями (ч. 2 ст. 200 ЦК). Стаття 862 ЦК «Конфіденційність одержаної сторонами інформації» - якщо сторона у договорі підряду внаслідок виконання договору одержала від другої сторони інформацію про нові рішення і технічні знання, у тому числі й такі, що не захищаються законом, а також відомості, що можуть розглядатися як комерційна таємниця, вона не має права повідомляти їх іншим особам без згоди другої сторони.

¹⁰⁹Писаренко Г.М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення // Науковий вісник Ужгородського національного університету, 2016. Серія ПРАВО. Випуск 36. Том 2. С.55-58.

Цивільно-правова відповідальність настає в тих випадках, коли в результаті недотримання відповідних норм інформаційного права заподіюється шкода підприємствам, установам, організаціям і громадянам. Так, у Цивільному кодексі України вказано, що якщо відомості, які порочать честь, гідність або ділову репутацію громадянина, поширені в засобах масової інформації, то вони мають бути спростовані в тих же засобах масової інформації.

2. *Дисциплінарне правопорушення* – це протиправне діяння суб'єкта, що завдає шкоди внутрішньому трудовому розпорядку підприємств, установ та організацій. Дисциплінарні проступки в інформаційній сфері - це правопорушення, вчинені суб'єктами інформаційного права у зв'язку з виконанням ними своїх трудових прав і обов'язків. До посадової особи чи працівника, який вчинив дисциплінарний проступок, застосовуються заходи загальної (догана, звільнення) або спеціальної (зауваження, попередження, пониження в посаді, тимчасове усунення від виконання службових обов'язків у зв'язку з проведенням службового розслідування тощо) дисциплінарної відповідальності. Дисциплінарна відповідальність найманого працівника/посадової особи передбачається в трудовому договорі (контракті) або в законі.

3. *Адміністративним проступком* в інформаційній сфері називається правопорушення, вчинене громадянином і яке виражається в порушенні встановлених правил поведінки в зазначеній сфері. До громадянина, який вчинив адміністративний проступок, можуть бути застосовані також різноманітні заходи покарання: штраф, конфіскація, попередження та інш.

9.2. 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, 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. 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 відповідальності¹¹⁰. 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.

- 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.

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. 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 відповідальність¹¹¹.

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,*

¹¹⁰ 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. Белякова. Київ : КВІЦ, 2019. 344 с.

¹¹¹ Настюк В. Я., Білевцева В. В. Загальноправова характеристика адміністративної відповідальності за інформаційні правопорушення. Інформація і право. 2013. № 1. С. 151–157.

об'єктом в яких виступають інформаційні права, свободи особи, правові режими інформації чи гарантований державою публічний інформаційний правопорядок¹¹².

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.

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. 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. 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

¹¹² Заярний О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія. Київ : Видавничий дім «Гельветика», 2017. 700 с.

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) будучи 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.

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 правопорушень¹¹³. 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. Що є характерною особливістю адміністративних інформаційних правопорушень?
4. Що є ознаками адміністративної відповідальності?
5. Що є національними інтересами України в інформаційній сфері?

¹¹³ Там же.

РОЗДІЛ 10.

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Посилення суттєвого впливу інформаційної сфери на життя людини, на діяльність держави та суспільства перетворилось на одну з особливостей соціального розвитку XX ст. та початку XXI ст. В той же час, розвиток інформаційних технологій не тільки ознаменував кардинально інший еволюційний розвиток людства та початок масового поширення та споживання інформації, але й виявив вразливість суспільства до зловживань в інформаційній сфері та технології. Так, 12 грудня 2023 року Україна зазнала однієї з найбільш небезпечних кібератак за всі роки незалежності. Незважаючи на те що об'єктом впливу стала приватна компанія Приватне акціонерне товариство «КІЇВСТАР», яка надає послуги у забезпеченні безпроводного електронного зв'язку, його наслідки відчула вся країна. Протягом двох днів був відсутній мобільний та інтернет-зв'язок. В результаті таких дій конфіденційна інформація абонентів стала не лише загальнодоступною, але й об'єктом кримінального впливу. Зафіксовано порушення роботи банків, банкоматів і торгових терміналів. Загальні матеріальні збитки уточнюються до цього часу. За кібератаку на одного із національних операторів мобільного зв'язку ПРАТ "КІЇВСТАР" Службою Безпеки України порушено кримінальні провадження за 8-ма статтями КК України. Однією з цих статей у повідомленні прес-служби СБУ вказано несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України). Зрозуміло, що реакцією держави на порушення у зазначеній сфері стало посилення охорони в інформаційній сфері, в тому числі кримінально-правовими засобами.

З моменту прийняття Кримінального кодексу України у 2001 році¹¹⁴ і до цього часу відбуваються суттєві зрушення в питаннях кримінальної відповідальності за зловживання у сфері інформаційних технологій. Зокрема, у 2004 році кримінальний кодекс був доповнений статтями 361-1 - Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; 361-2 - Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; 363-1 - Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку. Це підтверджує ту особливу увагу, яку приділяє держава проблемам функціонування інформації та її захисту в сучасному цифровому середовищі.

Викладене вимагає потребу висвітлення підстав притягнення до кримінальної відповідальності за порушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

¹¹⁴ Кримінальний кодекс України: Закон. (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131

10.1. Підстави кримінальної відповідальності за порушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Кримінальна відповідальність є одним з видів юридичної відповідальності. Вона полягає у вимушеному перетерпіванні особою, винною у вчиненні кримінального правопорушення державного осуду та певних обмежень особистого, майнового та іншого характеру.

Зміст кримінальної відповідальності полягає у взаємозв'язку її двох основних елементів. Державного осуду та обмежень особистого, майнового та іншого характеру.

Державний осуд означає негативну оцінку з боку суспільства суспільно небезпечного діяння вчиненого злочинцем. Ця оцінка міститься в обвинувальному вирокі суду, який проголошується від імені держави Україна, в якому визнаються винність особи у вчиненому кримінальному правопорушенні.

Обмеження особистого, майнового та іншого характеру представляють собою кримінальне покарання, яке призначається особі у випадку визнання її винною у вчиненні злочину або проступку. В залежності від характеру обмежень вони можуть бути особистими (позбавлення волі, обмеження волі тощо), майновими (штраф, конфіскація майна), мати інший характер (позбавлення права займати певні посади або займатися певною діяльністю, позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу).

Кримінальний кодекс України, який набрав чинності з 1 вересня 2001 р. встановлює відповідальність тільки у випадку вчинення особою кримінального правопорушення. Кримінальні правопорушення поділяються на кримінальні проступки і злочини.

Відповідно до ч.1 ст. 11 КК України кримінальним правопорушенням є передбачене Кримінальним кодексом суспільно небезпечне винне діяння (дія або бездіяльність), вчинене суб'єктом кримінального правопорушення.

Це означає, що кримінальним правопорушення визнається тільки протиправне (прямо передбачене кримінальним законом як злочин або проступок), суспільно небезпечне (таке що спричинює або створює реальну загрозу спричинення шкоди охоронюваним правам і свободам людини, власності, громадському порядку та громадській безпеці, довкіллю, конституційному устрою України, миру і безпеці людства) діяння.

Наявність вказаних у ст. 11 КК України ознак хоча і дає відповідь на питання які діяння і чому визнаються злочинними, але, в той же час, не дає можливості правозастосовнику встановити та обґрунтувати наявність в певних діях особи ознак конкретного кримінального правопорушення. У зв'язку з цим, теорія та практика кримінального права виробила поняття складу кримінального правопорушення. Відповідно до ч. 1 ст. 2 КК України єдиною і достатньою підставою кримінальної відповідальності є вчинення особою суспільно небезпечного діяння, яке містить склад кримінального правопорушення, передбаченого Кримінальним кодексом. Саме за допомогою складу кримінального правопорушення законодавець описує в законі протиправне діяння, а тому встановлення його в суспільно небезпечному діянні особи дає підстави визнавати останнього кримінальним правопорушенням.

Таким чином, підставою для притягнення до кримінальної відповідальності за порушення інформаційній сфері та сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є наявність в суспільно небезпечному діянні вчиненому особою складу кримінального правопорушення, пов'язаного з використанням інформаційних технологій.

10.2. Склад кримінального правопорушення як підстава притягнення до кримінальної відповідальності

Склад кримінального правопорушення представляє собою сукупність встановлених у законі об'єктивних та суб'єктивних ознак, при наявності яких суспільно небезпечне діяння визнається кримінальним правопорушенням.

Таким чином, якщо кримінальне правопорушення це явище реальної дійсності, то склад кримінального правопорушення це певне уявлення про нього закріплене в законі, за допомогою якого правоохоронні органи та суд визнають вчинене суспільно небезпечне діяння кримінальним правопорушенням. Так, створення програми-вірусу для проникнення в комп'ютерну мережу Приватного акціонерного товариства «КИЇВСТАР» є явищем реальної дійсності. Стаття ж 361 КК України містить ознаки складу за допомогою яких суд може встановити злочинність або незлочинність несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Як і явище реальної дійсності склад кримінального правопорушення характеризується з об'єктивної та суб'єктивної сторони. У рамках загального вчення про склад кримінального правопорушення прийнято виділяти елементи та ознаки складу.

До елементів складу відносять його об'єкт, об'єктивну сторону, суб'єкт та суб'єктивну сторону. Елементи складу кримінального правопорушення мають певні ознаки за допомогою яких розкривається їх зміст.

Об'єкт

Під об'єктом кримінального правопорушення розуміються ті суспільні відносини, яким внаслідок вчинення суспільно небезпечного посягання спричинюється шкода (або створюється реальна загроза її спричинення). У кримінальних правопорушеннях, пов'язаних з порушенням інформаційного законодавства об'єктом кримінального правопорушення виступають суспільні відносини що забезпечують захист інформації та безпечне функціонування електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

В залежності від обсягу охоронюваних суспільних відносин об'єкт кримінального правопорушення поділяється на: загальний, родовий та безпосередній.

Загальний об'єкт – це сукупність охоронюваних кримінальним законом суспільних відносин. Забезпеченням охороною за допомогою кримінального закону підлягають не всі існуючі у суспільстві суспільні відносини, а тільки найважливіші, посягання на які становить підвищену суспільну небезпеку. Приблизний перелік цих відносин міститься у ч. 1 ст. 1 КК України - це права та свободи людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України, мир і безпека людства.

Родовий об'єкт – це сукупність однорідних суспільних відносин, які охороняються єдиним комплексом кримінально-правових норм. Представлення про родовий об'єкт дає рубрикація Особливої частини КК України. Основні норми про відповідальність за порушення в інформаційній сфері містяться у розділі XVI Особливої частини КК, який має назву «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Під охороною кримінального закону в цьому розділі знаходиться інформаційна сфера, пов'язана з функціонуванням комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, а також захистом інформації, що обробляється за допомогою вказаних систем.

Під безпосереднім об'єктом розуміють ті конкретні суспільні відносини, які взяті під охорону певною кримінально-правовою нормою. Саме безпосередній об'єкт є складовим елементом конкретного складу кримінального правопорушення. Так, при несанкціонованих діях з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинених особою, яка має право доступу до неї безпосереднім об'єктом виступає встановлений порядок зберігання, передачі, обробки та використання інформації в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах уповноваженими особами (ст. 362 КК України).

Об'єктивна сторона

Об'єктивна сторона складу кримінального правопорушення це «зовнішня» сторона протиправного діяння. Ознаками, притаманними об'єктивній стороні кримінального правопорушення виступають суспільно небезпечне діяння (дія або бездіяльність), суспільно небезпечні наслідки, причинний зв'язок між суспільно небезпечним діянням і суспільно небезпечними наслідками, місце, час, спосіб, знаряддя й засоби, а також обстановка вчинення кримінального правопорушення. Ці ознаки виділяють як основні та найбільш загальні при характеристиці зовнішнього прояву суспільно небезпечного посягання. Як зазначається у науці кримінального права, конкретний прояв того чи іншого акту протиправної поведінки неоднозначний і дуже різноманітний, а вичерпний перелік його об'єктивних ознак просто неможливий через значну кількість. Виявлення і дослідження ознак об'єктивної сторони дозволяє установити наявність складу кримінального правопорушення в діях особи, правильно кваліфікувати вчинене, розмежувати скоєне від інших злочинних діянь. Саме ознаки об'єктивної сторони найбільш повно відображені в диспозиціях статей кримінального закону.

Об'єктивна сторона кримінальних правопорушень у сфері інформаційних відносин - це процес негативного впливу на ці суспільні відносини. Він починається дією або бездіяльністю особи, відбувається у конкретних умовах місця, часу, обстановки із застосуванням певних засобів або знарядь, способу його вчинення. Закінчується цей процес настанням суспільно небезпечних наслідків, тобто шкідливими змінами в об'єкті посягання, які повинні перебувати в необхідному причинному зв'язку з дією (бездіяльністю).

На відміну від об'єктивної сторони кримінального правопорушення, об'єктивну сторону складу кримінального правопорушення утворюють лише ті ознаки, які

характеризують зовнішній акт протиправної поведінки, і передбачені нормою кримінального права. Кримінально-правова норма не містить і не може містити всю масу різноманітних ознак, характерних для кожного конкретного злочину або проступку. Це не будь-які ознаки, а ті з них, які розкривають сутність явища, дають можливість виявити об'єктивні закономірності реальної дійсності, що криються за цим явищем. Суспільно небезпечне діяння (дія або бездіяльність) виступає обов'язковою ознакою об'єктивної сторони складу кримінального правопорушення. Інші ознаки – суспільно небезпечні наслідки, причинний зв'язок між суспільно небезпечним діянням і суспільно небезпечними наслідками, місце, час, обстановка, спосіб, засоби та знаряддя вчинення кримінального правопорушення – можуть бути як передбаченими, так і не передбаченими конкретною кримінально-правовою нормою, тобто вони виступають як факультативні ознаки об'єктивної сторони складу кримінального правопорушення.

Дія це активна форма поведінки людини, бездіяльність пасивна, тобто утримання особи від вчинення дій, які вона могла та повинна була вчинити. При вирішенні питання про притягнення до кримінальної відповідальності за бездіяльність слід обов'язково встановити, що особа не вчинила дії, які вона повинна була (на підставі закону, професійних, службових обов'язків тощо) і могла вчинити (виходячи з фізичних та інтелектуальних можливостей як самої особи, так і обставин, які склалися на цей момент). Протиправні порушення у сфері інформаційних відносин можуть вчинятися як шляхом дій, так і бездіяльності. Так, створення, використання, розповсюдження або збут, шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж скоюються лише активними діями (ст. 361-1 КК України). В той же час, порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку можуть вчинятися як шляхом дії, так і бездіяльності (ст. 363 КК України).

Суспільно небезпечні наслідки – це негативні зміни в об'єкті кримінально-правової охорони в результаті вчинення протиправного одіяння. Наслідки у кримінальному праві можна класифікувати на два вид: матеріальні та нематеріальні. До *матеріальних* слід відносити майнову та фізичну шкоду. До *нематеріальної* слід відносити шкоду політичного, ідеологічного, морального та іншого характеру. Суспільно небезпечні наслідки є факультативною ознакою об'єктивної сторони складу кримінального правопорушення. Тобто, для описання протиправного діяння законодавець не завжди вказує на наслідки, як обов'язкову ознаку складу кримінального правопорушення. В такому випадку для констатації факту вчинення кримінального правопорушення достатньо встановити сам факт вчинення протиправного діяння. Наприклад, несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України) є протиправним незалежно від наслідків його вчинення. Така законодавча конструкція має назву формального складу кримінального правопорушення. У матеріальних складах для визнання діяння кримінальним обов'язковим є встановлення, крім

суспільно небезпечного діяння, певних його наслідків, прямо визначених у законі. Протиправні порушення в інформаційній сфері в своїй більшості представляють собою правопорушення з формальним складом. Ступінь суспільної небезпеки цих протиправних діянь достатньо висока, а суспільно небезпечні наслідки настільки різноманітні, що сам факт втручання в комп'ютерну систему або електронних комунікаційних мереж є закінченим злочином. В той же час, суспільно небезпечні наслідки в кримінальних правопорушеннях в інформаційній сфері можуть виступати у якості обтяжуючих обставин. В такому разі, їх встановлення (значна шкода чи створення небезпеки тяжких технологічних аварій або екологічних катастроф, загибель або масове захворювання населення чи інші тяжкі наслідки) для правильної кваліфікації, зокрема в тій же частині 4 статті 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» є обов'язковим.

Причинний зв'язок це об'єктивно існуючий зв'язок між суспільно небезпечним діянням та суспільно небезпечними наслідками. Ставлення у вину особі суспільно небезпечних наслідків можливо тільки у випадку встановлення необхідного причинного зв'язку між вчиненим особою діянням та суспільно небезпечними наслідками. Це означає, що діяння є єдиною, достатньою та необхідною умовою настання суспільно небезпечних наслідків. У випадку наявності випадкового причинного зв'язку особа не може притягатися до кримінальної відповідальності за настання випадкових суспільно небезпечних наслідків.

Місце – це певна територія на якій вчинюється кримінальне правопорушення.

Час – це певний проміжок часу, протягом якого вчинюється кримінальне правопорушення. Так, шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки в умовах воєнного чи надзвичайного стану потребує обов'язкового встановлення вказаних термінів.

Обстановка – сукупність певних об'єктивних умов в яких відбувається подія кримінального правопорушення.

Засоби – речі матеріального світу за допомогою яких вчиняється або полегшується вчинення кримінального правопорушення.

Спосіб – це сукупність прийомів та методів за допомогою яких вчинюється кримінальне правопорушення. Наприклад, способом заволодіння чужим майном при шахрайстві з використанням електронно-обчислювальної техніки є оман або зловживання довірою.

Суб'єкт кримінального правопорушення

Ст. 18 КК визнає суб'єктом кримінального правопорушення фізичну, осудну особу, яка вчинила протиправне діяння у віці, з якого відповідно до Кримінального кодексу може наставати кримінальна відповідальність.

Фізичною особою визнається людина. *Юридичні особи до кримінальної відповідальності не притягаються.* Осудною визнається особа, яка під час вчинення кримінального правопорушення могла усвідомлювати свої дії (бездіяльність) і керувати ними (ч. 1 ст. 19 КК України). Загальний вік кримінальної відповідальності згідно із ч. 1 ст. 22 КК України становить 16 років.

Кримінальний закон і теорія кримінального права вирізняють два види суб'єктів кримінальних правопорушень – загальний і спеціальний. Як загальний, так і спеціальний суб'єкт кримінального правопорушення характеризується наявністю наступних обов'язкових ознак – це: 1) особа фізична; 2) особа осудна; 3) особа, яка вчинила протиправне діяння у віці, з якого може наставати кримінальна відповідальність. Для загального суб'єкта наявність таких ознак є достатньою, спеціальний же суб'єкт, крім зазначених, повинен мати й інші ознаки, передбачені кримінальним законом.

Відповідно до ч. 2 ст. 18 КК України спеціальним суб'єктом кримінального правопорушення є фізична осудна особа, яка вчинила у віці, з якого може наставати кримінальна відповідальність, кримінальне правопорушення, суб'єктом якого може бути лише певна особа.

В більшості випадків посягання у сфері інформаційних відносин може здійснюватися будь-якою особою, яка досягла 16 років (загальний суб'єкт). В окремих випадках відповідальність за втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж передбачена лише для осіб, які відповідальні за роботу зазначених мереж (ст. ст. 362-363 КК України).

Суб'єктивна сторона

Суб'єктивна сторона кримінального правопорушення являє собою відбиття психічних процесів, що проходять у свідомості особи, характеризують її волю й детермінують поведінку. На відміну від об'єктивної сторони, яка характеризує протиправне діяння із зовнішньої (фізичної) сторони, суб'єктивна виступає як внутрішня характеристика.

З точки зору більшості правників суб'єктивна сторона кримінального правопорушення – це психічна діяльність особи, що характеризує ставлення її свідомості й волі до вчинюваного нею суспільно небезпечного діяння та до його наслідків. *Елементами* суб'єктивної сторони є *вина, мотив і мета*, які хоча й тісно пов'язані між собою, однак мають самостійне юридичне значення. Вина – це обов'язкова ознака будь-якого кримінального правопорушення, відсутність якої виключає кримінальну відповідальність. На відміну від вини, мотив і мета становлять факультативні ознаки складу кримінального правопорушення. У передбачених законом випадках вони можуть виступати ознакою основного або кваліфікованого складів, а також впливати на кримінальну відповідальність, як обставини, що обтяжують або пом'якшують покарання.

Відповідно до ст. 23 КК України **виною** визнається психічне ставлення особи до вчинюваної дії чи бездіяльності, передбаченої цим Кодексом, та її наслідків, виражене у формі умислу або необережності. Таке законодавче визначення поняття вини вперше було закріплено в кримінальному законодавстві України в 2001 році.

Торкаючись проблеми форм вини у кримінальних правопорушеннях у сфері інформаційних технологій, слід зазначити, що КК установлює відповідальність лише за умисне їх вчинення. Разом із тим психічне відношення до настання суспільно небезпечних наслідків у вигляді тяжкої шкоди, технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення може мати ознаки як

умислу, так і необережності. В другому випадку зазначена форма вини у теорії кримінального права отримала назву складної (змішаної або подвійної).

Згідно ст. 24 КК України умисел поділяється на прямий і непрямий.

Прямим є умисел, якщо особа усвідомлювала суспільно небезпечний характер свого діяння (дії або бездіяльності), передбачала його суспільно небезпечні наслідки і бажала їх настання. *Непрямим є умисел*, якщо особа усвідомлювала суспільно небезпечний характер свого діяння (дії або бездіяльності), передбачала його суспільно небезпечні наслідки і хоча не бажала, але свідомо припускала їх настання. Як бачимо законодавець при визначенні умислу (як і вини в цілому) використовує зміст інтелектуального та вольового елементів психіки.

Інтелектуальний момент умислу (як прямого, так і непрямого) полягає: 1) в усвідомленні особою суспільно небезпечного характеру свого діяння (дії або бездіяльності); 2) у передбаченні його суспільно небезпечних наслідків.

Слід зазначити, що передбачення особою суспільно небезпечних наслідків діяння, що вона має намір учинити, як ознака інтелектуального моменту умислу, полягає в тому, що особа передбачає можливість або неминучість настання встановлених кримінальним законом суспільно небезпечних наслідків, розвиток (хоча б у загальних рисах) причинного зв'язку між суспільно небезпечним діянням і цими наслідками. Із цього випливає, що передбачення суспільно небезпечних наслідків, як ознака інтелектуального моменту умислу, має місце лише у кримінальних правопорушеннях із матеріальним складом.

Під час розгляду об'єктивної сторони кримінальних правопорушень у сфері інформаційних технологій нами було встановлено, що більшість вказаних протиправних діянь формулюються законодавцем як кримінальні правопорушення з формальним складом. А тому під час розгляду інтелектуального моменту умислу в кримінальних правопорушеннях у сфері інформаційних технологій встановлюється тільки усвідомлення особою суспільно небезпечного характеру свого діяння.

Усвідомлення особою суспільно небезпечного характеру свого діяння означає розуміння нею як його фактичних ознак, так і соціального характеру.

Усвідомлення особою фактичних ознак кримінальних правопорушень у сфері інформаційних технологій включає насамперед усвідомлення об'єктивних ознак складів цих протиправних діянь – об'єкта й об'єктивної сторони.

Поряд з усвідомленням фактичних ознак діяння необхідним складником інтелектуального моменту умислу виступає усвідомлення особою соціального характеру свого діяння, тобто усвідомлення його небезпечності для суспільства, шкідливості для суспільних відносин, які охороняються кримінальним законом.

Вольовий момент протиправних діянь з формальним складом визначається відносно самого суспільно небезпечного діяння, оскільки «саме в ньому сконцентрована соціальна шкідливість діяння». У таких складах предметом бажання є саме суспільно небезпечне діяння. Умисел в таких складах може бути лише прямим.

У теорії кримінального права мотив кримінального правопорушення визначають як зумовлене певними потребами й інтересами внутрішнє спонукання, яке викликає в особи бажання й рішучість вчинити суспільно небезпечне діяння. В більшості випадків мотив злочинних порушень в інформаційній сфері не впливає на

кваліфікацію. В той же час, шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки потребує обов'язкового встановлення корисливого мотиву.

Мета – це певний результат, що намагається досягти особа, яка скоює кримінальне правопорушення.

При формулюванні конкретного кримінального правопорушення законодавець не використовує усіх ознак елементів складу кримінального правопорушення перерахованих вище. Для визначення суспільно небезпечного діяння протиправним в законі вказуються тільки ті ознаки, які визначають суспільну небезпеку того чи іншого діяння. Так, для розголошення державної таємниці не має значення час його вчинення або обстановка в якій воно вчинялося. Крім того, не всі ознаки складу кримінального правопорушення містяться в статті Особливій частині КК України. Поняття суб'єкту кримінального правопорушення, умислу, стадій кримінального правопорушення містяться в нормах Загальної частини. Тому для вивчення ознак конкретного кримінального правопорушення необхідно звертатись до норм Особливої та Загальної частин КК. У випадку ж відсутності хоча б однієї з ознак складу кримінального правопорушення визначених в законі в конкретному суспільно небезпечному діянні особи виключає кримінальну відповідальність.

Таким чином, підставою для кримінальної відповідальності за кримінальні порушення в інформаційній сфері виступає вчинення особою суспільно небезпечного діяння, яке містить ознаки відповідних складів кримінальних правопорушень, передбачених КК України.

На сьогодні всі правопорушення у сфері інформаційних технологій, передбачені кримінальним законодавством умовно можна розділити на декілька груп.

Перша група норм стосується встановлених законодавством заборон щодо розповсюдження певного виду інформації. Згідно з Законом України «Про доступ до публічної інформації» публічна інформація поділяється на загальнодоступну та з обмеженим доступом.

Ст. 6 Закону України «Про доступ до публічної інформації» допускає обмеження доступу до інформації при дотриманні сукупності наступних вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Відсутність хоча б однієї із зазначених вимог унеможливорює обмеження доступу до інформації.

Згідно з Законом «Про доступ до публічної інформації» інформація з обмеженим доступом поділяється на:

- 1) конфіденційну інформацію;
- 2) таємну інформацію;
- 3) службову інформацію.

За порушення законодавства у сфері доступу, зберігання та поширення інформації з обмеженим доступом передбачено юридичну відповідальність, в тому числі кримінальну.

Чинне кримінальне законодавство України передбачає розгалужену систему кримінально-правових норм про відповідальність за порушення у сфері обігу інформації з обмеженим доступом. В залежності від виду інформації всі кримінально-правові норми зазначеної групи можна поділити на певні групи. Так, відповідальність за незаконне поводження з таємною інформацією передбачено ст. 111 КК «Державна зрада у формі шпигунства»; ст. 114 КК «Шпигунство»; ст. 159 КК «Порушення таємниці голосування»; ч. 3 ст. 160 КК «Порушення таємниці голосування, вчинені членом комісії з проведення референдуму або іншою службовою особою»; ст. 163 КК «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»; ст. 168 КК «Розголошення таємниці усиновлення (удочеріння)»; ст. 231 КК «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю»; ст. 232 КК «Розголошення комерційної або банківської таємниці»; ст. 328 КК «Розголошення державної таємниці»; ст. 330 КК «Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни»; ст. 381 КК «Розголошення відомостей про заходи безпеки щодо особи, взятої під захист»; ст. 387 КК «Розголошення даних оперативно-розшукової діяльності, досудового розслідування»; ст. 422 КК «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості».

Незаконне збирання, зберігання, отримання, розповсюдження службової інформації передбачено ст. 232-1 КК «Незаконне використання інсайдерської інформації»; ст. 361-2 КК «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації».

Незаконне поводження з конфіденційною інформацією передбачено ст. 182 КК «Порушення недоторканності приватного життя».

Судова практика

ОСОБА_4, 19.07.2023 о 06:25 год., перебуваючи у м. Калуш (точної адреси в ході досудового розслідування не встановлено), шляхом використання електронно-обчислювальної техніки та мобільного номеру телефону ОСОБА_6, авторизувався у мобільному додатку веб-банкінгу АТ КБ «ПриватБанк» та таким чином отримав доступ до особистого кабінету зареєстрованого та належного ОСОБА_6, отримавши тим самим над ним повний контроль, що призвело до витоку інформації, після чого усвідомлюючи суспільно небезпечний характер свого діяння, передбачаючи його суспільно-небезпечні наслідки та свідомо бажаючи їх настання, в порушенні вимог ст. 32 Конституції України, згідно якої «ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України, не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в

інтересах національної безпеки, економічного добробуту та прав людини»; ст. 14 Закону України «Про захист персональних даних» від 01.06.2010 №2297-VI, згідно якої «поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»; ст. 21 Закону України «Про інформацію» від 02.10.1992, згідно якої «інформація про фізичну особу є конфіденційною, конфіденційна інформація може поширюватись за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом»; а також усвідомлюючи, що згідно ст. 11 Закону України «Про інформацію» від 02.10.1992 «до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження», а отже, лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці, діючи умисно, усвідомлюючи суспільно небезпечний характер свого діяння, передбачаючи його суспільно-небезпечні наслідки та свідомо бажаючи їх настання, отримав та незаконно зберіг вказану конфіденційну інформацію відносно ОСОБА_6, а саме інформацію про паспорт громадянина України, реєстраційний номер облікової картки платника податків, адресу зареєстрованого місця проживання, дату народження.

Після вказаного, ОСОБА_4 19.07.2023 о 08:14 год. використав без належної згоди ОСОБА_6 інформацію, яка відповідно до ст. 11 Закону України «Про інформацію», відноситься до конфіденційної, зокрема щодо адреси, дати народження, номеру та дати видачі паспорта громадянина України та реєстраційного номеру облікової картки платника податків, для створення онлайн заявки на сайті з онлайн кредитування, а саме 1 БЕЗПЕЧНЕ АГЕНТСТВО НЕОБХІДНИХ КРЕДИТІВ - ТОВ «ШВИДКІ ГРОШІ», код ЄДРПОУ 37026878, від імені ОСОБА_6 , ІНФОРМАЦІЯ_2¹¹⁵.

Слід зазначити, що відповідальність за вказані дії безпосередньо пов'язана з порушенням встановлених чинним законодавством правил поведінки з інформацією з обмеженим доступом, зокрема законами України «Про інформацію», «Про доступ до публічної інформації», «Про оперативно-розшукову діяльність», «Про захист персональних даних». Обмеження, які встановлюються законодавством для певного виду інформації стосуються будь-яких учасників інформаційних відносин, а в окремих випадках тільки спеціальних суб'єктів, службових осіб або осіб, які мають доступ до певної інформації. Зокрема, за розголошення державної таємниці (ст. 328 КК України); комерційної або банківської таємниці (ст. 232 КК України); розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387 КК України); розголошення відомостей військового характеру, що становлять державну

¹¹⁵ Єдиний державний реєстр судових рішень Справа №345/1819/24. Проведення № 1-кп/345/201/2024. <https://youcontrol.com.ua/ru/catalog/court-document/119548591/>

таємницю, або втрата документів чи матеріалів, що містять такі відомості (ч. 2 ст. 422 КК України) несуть відповідальність особи, яким така інформація стала відома у зв'язку з їх службовою, професійною або іншою пов'язаною діяльністю.

Основною відмінністю між вказаними кримінально-правовими нормами є вид інформації (конфіденційна, таємна, службова), незаконне поводження з якою тягне кримінальну відповідальність для винного. Так, статті 111, 114 та 328 КК України передбачають відповідальність за незаконне поводження з інформацією, що містить державну таємницю. В той же час, стаття 232 КК України встановлює відповідальність за незаконне поводження з комерційною або банківською таємницею.

Більшість порушень у сфері обігу інформації з обмеженим доступом вчиняється лише умисно. Особа повинна усвідомлювати суспільно небезпечний характер свого діяння (дії або бездіяльності), передбачати його суспільно небезпечні наслідки і бажати їх настання або свідомо припускати такі наслідки.

В той же час, в окремих випадках закон передбачає кримінальну відповідальність і за необережні порушення у сфері неправомірного поводження з інформацією з обмеженим доступом. Наприклад, ст. 329 КК України передбачає відповідальність за втрату документів, що містять державну таємницю. Так, визнається караним втрата документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами,

Другу групу представляють норми, що стосуються посягань у різних сферах людської діяльності, однак з обов'язковим використанням інформаційних та комп'ютерних технологій. До таких злочинів слід віднести шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК України); домагання дитини для сексуальних цілей з використанням інформаційно-телекомунікаційних систем або технологій (ст. 156-1 КК України); одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження з використанням інформаційно-телекомунікаційних систем чи технологій (ст. 301-1 КК України); проведення видовищного заходу сексуального характеру за участю неповнолітньої особи з використанням інформаційно-телекомунікаційних систем чи технологій (ст. 301-2 КК України); домагання дитини для сексуальних цілей з використанням інформаційно-телекомунікаційних систем чи технологій (ст. 156-1 КК України). Як бачимо, більшість з вказаних порушень з'являються в кримінальному кодексі вже після прийняття у 2001 році нового закону України про кримінальну відповідальність і безпосередньо пов'язані з розвитком інформаційної галузі, електронно-обчислювальних систем та розширенням їхнього використання у злочинній діяльності. Основною відмінною ознакою вказаних злочинів від основних складів є засоби скоєння правопорушення. Так, заволодіння майном або правом на майно шляхом обману або зловживанням довірою (шахрайство) з використанням електронно-обчислювальної техніки означає здійснення таких видів обману, які

безпосередньо пов'язані з використанням комп'ютерної техніки, платіжних карток.

Судова практика

04.01.2024 до Стрийського міськрайонного суду Львівської області скеровано обвинувальний акт у кримінальному провадженні №1202314370000098 від 03.02.2023 про обвинувачення ОСОБА_3 у вчиненні кримінальних правопорушень, передбачених ч. 1 ст. 255, ч. 3 ст. 27 - ч. 4 ст. 28 - ч. 4 ст. 190 /в редакції Закону №2617-VIII від 22.11.2018/, ч. 3 ст. 27 - ч. 4 ст. 28 - ч. 5 ст. 361 КК України, тобто в організації заволодіння та заволодінні чужим майном шляхом обману (шахрайство), вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки у складі організованої групи, в організації несанкціонованого втручання та у несанкціонованому втручанні в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що призвело до витоку інформації, у складі злочинної організації, вчиненому повторно.

Відповідно до розробленого плану, завдань і мети існування злочинної організації, співорганізатор якої ОСОБА_3, було налагоджено створення веб-сайтів, що копіювали зовнішній вигляд справжніх сайтів банківських установ, підшукування соціальних мереж розсилки текстових повідомлень, створення телеграм ботів для подальшої оптимізації отриманої інформації, спрямованої на заволодіння грошовими коштами громадян по всій території України, з метою незаконного збагачення учасників групи.

Зокрема, 15.01.2023 о 05 годині 36 хвилин, ОСОБА_3, який в цей час перебував у місті Стрию Львівської області (більш точної адреси під час досудового розслідування не встановлено), маючи доступ до попередньо розробленого невідомою особою веб-ресурсу, що зовні копіює зміст та вигляд офіційного веб-сайту мобільного додатку «Приват24», отримав персональні дані ОСОБА_6, яка не ставлячи під сумнів побачене текстове повідомлення в мережі Інтернет, у вказаному посиланні зазначила свою особисту інформацію як клієнта АТ КБ «ПриватБанк», серед яких логін та пароль до облікового запису (акаунту) онлайн банкінгу, що є системою призначеною для дистанційного керування банківськими картками банку АТ КБ «ПриватБанк», який діє на підставі банківської ліцензії №22 від 05.10.2011, авторські права на який належать АТ КБ «ПриватБанк», та в цей час в нього виник умисел на несанкціоноване втручання в роботу інформаційної (автоматизованої) мережі.

В подальшому, ОСОБА_3, маючи персональні дані ОСОБА_6, без згоди та відома останньої, діючи від її імені, реалізуючи свій прямий злочинний умисел направлений на протиправне збагачення, маскуючи свої дійсні злочинні наміри, без відома учасників злочинної організації, в умовах воєнного стану, не санкціоновано втрутився в роботу інформаційної (автоматизованої) системи АТ КБ «ПриватБанк», увійшов у додаток «Приват24», через особистий акаунт клієнтки АТ КБ «ПриватБанк» ОСОБА_6, де знаходяться її персональні дані та реквізити офіційних документів, змінив прив'язаний до акаунту ОСОБА_6, фінансовий номер телефону НОМЕР_1, на свій фінансовий номер НОМЕР_2, який в цей час знаходився в мобільному терміналі IMEI: НОМЕР_3, НОМЕР_4, що призвело до витоку інформації та порушення порядку

її маршрутизації, яка є банківською таємницею, що надало можливість здійснювати транзакції від її імені.

Таким чином, ОСОБА_3 несанкціоновано втрутилась в роботу інформаційної (автоматизованої) мережі, що призвело до витоку інформації та порушення встановленого порядку її маршрутизації, в умовах воєнного стану, тобто вчинила кримінальне правопорушення, передбачене ч. 5 ст. 361 КК України.

Крім цього, 15.01.2023 в період з 06 години 08 хвилин по 06 годину 39 хвилин, ОСОБА_3, який в цей час перебував у місті Стрию Львівської області (більш точної адреси під час досудового розслідування не встановлено), через додаток «Приват 24» інформаційної (автоматизованої) системи АТ КБ «ПриватБанк», зайшов до облікового запису (акаунту) ОСОБА_6, та в цей час в нього виник умисел на заволодіння її коштами, які знаходились на банківському рахунку № НОМЕР_5 (картка № НОМЕР_6).

В подальшому, ОСОБА_3, реалізуючи свій злочинний умисел, спрямований на протиправне заволодіння чужим майном, шляхом незаконних операцій з використанням електронно-обчислювальної техніки, без відома учасників злочинної організації, повторно, через акаунт ОСОБА_6, здійснив переказ її коштів з рахунку № НОМЕР_5 (№ НОМЕР_6) в сумі 18 140 гривень, за покупку електронної валюти на ігрових сервісах ТОВ «Паріматч» (ЄДРПОУ:43363902, юридична адреса: Україна, 02140, м. Київ, проспект Миколи Бажана, 14А, офіс 26), якими в подальшому розпорядився на власний розсуд.

Своїми протиправними діями ОСОБА_3, завдав матеріальну шкоду потерпілій ОСОБА_6 на загальну суму 18 140 гривень.

Таким чином, ОСОБА_3 заволодів чужим майном шляхом обману (шахрайство), повторно, шляхом незаконних операцій з використанням електронно-обчислювальної техніки, тобто вчинив кримінальне правопорушення, передбачене ч. 3 ст. 190 КК України /в редакції Закону №2617-VIII від 22.11.2018/¹¹⁶.

Третя група норм стосується цілого розділу XVI Особливої частини кримінального кодексу України, який має назву «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Зазначений розділ КК України передбачає відповідальність за порушення, передбачені статтями 361-363-1 КК України і пов'язані з незаконним використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Судова практика

25.07.2018, точний час досудовим розслідуванням не встановлено, ОСОБА_1, перебуваючи за місцем свого проживання за адресою: АДРЕСА_1, з метою несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), які забезпечують функціонування електронного поштового серверу <https://www.bigmir.net/>, користуючись персональним комп'ютером із жорсткими дисками SAMSUNG HD753LJ s/n S13UJ1EQ202275 та SAMSUNG HD753LJ s/n

¹¹⁶ Єдиний державний реєстр судових рішень. Справа № 456/1727/24. <https://youcontrol.com.ua/ru/catalog/court-document/118536834/>

НОМЕР_1, який мав доступ до мережі Інтернет з наданою ІР-адресою ІНФОРМАЦІЯ_5, що обслуговується провайдером ТОВ «НашНет», (м. Київ, проспект Маяковського, 73А), діючи умисно, усвідомлюючи суспільно-небезпечний характер своїх дій, передбачаючи їх шкідливі наслідки та свідомо бажаючи настання таких наслідків, видаючи себе за авторизованого користувача електронної поштової скриньки з обліковим записом «ІНФОРМАЦІЯ_4», що належить ОСОБА_2 та є інформацією з обмеженим доступом, яка створена та захищена відповідно до вимог Законів України «Про захист персональних даних», «Про інформацію», «Про захист інформації в автоматизованих системах», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», звернувся до служби підтримки сервісу «ІНФОРМАЦІЯ_2 net» та вказав, що забув пароль до поштової скриньки і назвав попередні відомі йому авторизаційні дані ОСОБА_2. Таким чином, ОСОБА_1 отримав новий пароль до електронної поштової скриньки з обліковим записом «ІНФОРМАЦІЯ_4» та тим самим без згоди та відома ОСОБА_2 незаконно змінив пароль доступу до електронної поштової скриньки, чим здійснив несанкціоноване втручання в роботу облікового запису «ІНФОРМАЦІЯ_4» комп'ютерної мережі сервісу «ІНФОРМАЦІЯ_2.net», який належить ОСОБА_2 та на момент вчинення злочину використовувався нею в м. Рівне.

Внаслідок таких протиправних дій ОСОБА_1, процес зіставлення користувача ОСОБА_2 і наділених їй прав, який із використанням спеціалізованого програмного забезпечення автоматизовано здійснювався електронним поштовим сервером, був змінений та реєстраційні дані авторизованого на законних підставах користувача визнавалися недійсними, що призвело до наслідків у вигляді блокування та втрати інформації потерпілої ОСОБА_2, яка мала право доступу до неї, і витоку інформації, яку потерпіла не бажала розголошувати.

Своїми умисними діями, які виразилися у несанкціонованому втручанні в роботу електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж, що призвело до блокування, втрати та витоку інформації, ОСОБА_1 вчинив кримінальне правопорушення, передбачене ч.1 ст.361 КК України¹¹⁷.

В залежності від *предмету* кримінального правопорушення та *характеру* протиправної поведінки всі склади кримінальних правопорушень можна розділити на дві групи. Перша група норм стосується норм, пов'язаних з незаконним поводженням з інформацією, що розповсюджується за допомогою електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, *Стаття 361-2 КК України* визнає незаконним несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; *Стаття 362 КК України* визнає караним несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї).

¹¹⁷ Вирок від 13.09.2019 по справі № 569/12334/19 Рівненський міський суд Рівненської області // <https://zakononline.com.ua/court-decisions/show/84251500>

Друга група норм встановлює кримінальну відповідальність за перешкоджання діяльності інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж шляхом втручання або розповсюдження шкідливих програм, технічних засобів. Зокрема, *Стаття 361 КК України* передбачає відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; *Стаття 361-1 КК України* встановлює відповідальність за створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; *Стаття 363 КК України* передбачає порушення 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 оброблюється; *Стаття 363-1 КК України* встановлює відповідальність за перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку).

Родовим об'єктом кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є сукупність суспільних відносин, що виникають з приводу обробки (збирання, введення, запис, перетворення, зчитування, зберігання, знищення, реєстрація), захисту комп'ютерної інформації та експлуатації засобів, що їх забезпечують (ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку).

Предметом кримінальних правопорушень, відповідальність за які передбачена ст. ст. 361–363-1 КК України можуть виступати:

- електронно-обчислювальна машина (комп'ютер) – комплекс електронних пристроїв (складових елементів), що дозволяють здійснювати передбачені програмою або користувачем операції з інформацією, у тому числі здійснювати її введення або виведення, знищення, копіювання, модифікацію, автоматичну обробку, передачу інформації до комп'ютерних мереж та інші інформаційні процеси. ЕОМ може бути обладнана допоміжним устаткуванням (пристроями), що дозволяє яким-небудь образом змінювати або перезаписувати керуючі програми й (або) дані, необхідні для реалізації процесором його цільових функцій;

- автоматизовані системи – організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів;

- комп'ютерні мережі – комплекс (сукупність) з'єднаних лініями зв'язку комп'ютерів або комп'ютерних систем. В залежності від швидкості обміну даними між робочими комп'ютерами й розмірів охопленої території розрізняють локальні, регіональні та глобальні комп'ютерні мережі;

- мережі електрозв'язку – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

- носії комп'ютерної інформації – предмети, виготовлені з матеріалу з певними фізичними властивостями, що можуть бути використані для зберігання інформації та забезпечують сумісність із пристроями запису/зчитування інформації. До них слід відносити дискети, жорсткі магнітні диски, флеш накопичувачі, карти пам'яті, магнітні стрічки та ін.;

- комп'ютерна інформація (інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) – відомості у вигляді текстової, цифрової, графічної чи іншої інформації, знання або набір команд (програма), призначені для використання у ЕОМ або управління нею, що знаходиться у ЕОМ або на носіях комп'ютерної інформації, щодо режиму використання якої правила встановлює власник такої інформації. Основної ознакою комп'ютерної інформації є те, що вона повинна зберігатися чи оброблюватися в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах, мережах електрозв'язку або на носіях такої інформації.

Відповідно до ст. 21 Закону України «Про інформацію» та ст. 6 Закону України «Про доступ до публічної інформації», інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Відповідно до ст. 1 Закону України «Про державну таємницю», державна таємниця (секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом, державною таємницею і підлягають охороні державою.

До іншої передбаченої законом таємниці слід відносити комерційну, банківську, приватну таємницю та інші види таємниць, правовий режим доступу до якої та її використання регламентується чинним законодавством України.

До службової належить інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрішню службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

- шкідливі програмні чи технічні засоби – це комп'ютерні програми та пристрої (устаткування) призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

- повідомлення електрозв'язку – повідомлення, що передаються по радіо, дротових, оптичних або інших електромагнітних системах. Наприклад, це можуть бути листи електронної пошти, SMS, MMS.

Об'єктивна сторона переважної більшості цих кримінальних правопорушень виражається в активних діях, хоча деякі із протиправних діянь характеризуються злочинною бездіяльністю, наприклад, порушення 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 оброблюється (ст. 363 КК України).

Більшість складів кримінальних правопорушень, передбачених ст. ст. 361, 361-1, 361-2, 362, 363-1 КК України, сформульовані законодавцем як протиправні діяння з формальним складом. В той же час, склад кримінального правопорушення, передбаченого ст. 363 КК України та частини 2-4 ст. ст. 361, 361-1, 361-2, 362, 363-1 за ознакою значної шкоди та тяжких наслідків утворюють матеріальні склади, що вимагає для правильної кваліфікації встановлення відповідних наслідків. Відповідно до примітки ст. 361 КК України *значною шкодою* у статтях 361-363-1 вважається така шкода, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Суб'єкт кримінальних правопорушень загальний – фізична осудна особа, що досягла 16 річного віку, а у деяких випадках суб'єкт спеціальний: особа, яка має право доступу до інформації, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації (ст. 362 КК України), особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку або відповідальна за забезпечення порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України).

Суб'єктивна сторона кримінальних правопорушень зазначеної групи характеризується, як правило, умисною формою вини. Необережна форма вини може мати місце у випадку порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України).

Запитання для самоконтролю і самостійного опрацювання

1. Що може бути предметом кримінального правопорушення?
2. За якими критеріями розрізняється адміністративна та кримінальна відповідальність?
3. Надайте класифікацію кримінальних правопорушень в сфері ІКТ.
4. Хто не може бути суб'єктом кримінальної відповідальності в сфері ІТ?
5. Які елементи становлять склад кримінального правопорушення?

РОЗДІЛ 11.

ПРАКТИЧНІ ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

До розділу 1: IT-право як нова правова категорія

Завдання 1. Надайте характеристики 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 IT права як галузі законодавства. Порівняйте IT 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. Глобальне прагнення до контролю над великими технологіями». 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) Законі 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 Інтернетдоговори 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.

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) поійменовані та не поійменовані

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) поійменовані та не поійменовані
- e) строкові та безстрокові

Тестові завдання 2.

Питання 1. Який розділ договору визначає часові рамки, протягом яких повинні бути виконані роботи за договором?

- a) Предмет договору
- b) Терміни виконання робіт
- v) Вартість послуг та порядок оплати
- г) Відповідальність сторін за невиконання умов договору

Питання 2. Який розділ договору зазвичай містить умови щодо кількості сторінок веб-сайту та його функціональності?

- a) Терміни виконання робіт
- b) Основні вимоги до веб-сайту

- в) Вартість послуг та порядок оплати
- г) Відповідальність сторін за невиконання умов договору

Питання 3. В якому розділі договору зазначаються санкції за невиконання або неналежне виконання умов договору?

- а) Предмет договору
- б) Терміни виконання робіт
- в) Вартість послуг та порядок оплати
- г) Відповідальність сторін за невиконання умов договору

Питання 4. Які ключові відмінності між ексклюзивною та неексклюзивною ліцензією на програмне забезпечення повинні бути відображені в договорі ліцензування?

- а) Терміни дії ліцензії та вартість
- б) Кількість користувачів та обмеження на використання програмного забезпечення
- в) Права ліцензіара на передачу ліцензії третім особам та можливість надання ліцензій іншим користувачам
- г) Обов'язки щодо технічної підтримки та оновлення програмного забезпечення

Питання 5. Які основні елементи мають бути включені в розділ договору про надання ІТ-послуг, що стосується конфіденційності інформації?

- а) Опис послуг та терміни їх надання
- б) Права та обов'язки сторін щодо збереження конфіденційної інформації, умови використання та обмеження розкриття інформації третім особам
- в) Вартість послуг та порядок оплати
- г) Порядок врегулювання спорів та відповідальність сторін

Ситуаційне завдання:

Завдання 1. 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

Завдання 2. Складіть проект договору про надання ІТ-послуг між "TechSolutions" та "GreenEnergy". Врахуйте наступні аспекти: предмет договору, обов'язки сторін, терміни виконання робіт, вартість послуг та порядок оплати,

відповідальність сторін за невиконання або неналежне виконання зобов'язань, конфіденційність інформації.

Завдання 3. Фрілансер Іван домовився з місцевою кав'ярнею "CoffeeTime" про створення веб-сайту для їхнього бізнесу. Складіть договір на створення веб-сайту між фрілансером Іваном та кав'ярнею "CoffeeTime". Врахуйте наступні аспекти: предмет договору, терміни виконання робіт, вартість послуг та порядок оплати, основні вимоги до веб-сайту (наприклад, кількість сторінок, інтеграція з соцмережами), відповідальність сторін за невиконання умов договору.

До розділу 6: Господарська діяльність з використанням інформаційних технологій. Електронний документообіг

Тестові завдання 1.

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 мереж, які функціонують на основі єдиних принципів та загальних правил;

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 рачію 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-системою 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.

Тестові завдання 2.

1. За Законом електронним документом вважається:

- а) інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.
- б) відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.
- в) 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
- б) ні

3. Чи можна передати право підписання документів ключем ЕЦП від власника до іншої особи?

- а) так
- б) ні

4. Для ідентифікації повідомлення і перевірки його аутентифікації використовується ключ ЕЦП:

- а) відкритий
- б) закритий

5. Чи може підприємство використовувати електронну печатку якщо у нього немає традиційної печатки?

- а) так
- б) ні
- в) в залежності від виду підприємства

6. Ознаки електронного документа:

- а) є програмно-технічно залежним продуктом

b) має широкий спектр інформаційного відображення: текстові, графічні, електронні таблиці, бази даних, мультимедійні

c) документ може зберігатися 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 накладання 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 7-8: Електронні гроші: поняття, зміст та особливості правового регулювання в Україні. 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

с) комерційний агент

д) користувач

4. Емітенту забороняється:

а) надавати кредит з коштів, які є зобов'язанням цього емітента за випущеними ним електронними грошима;

б) залучати агентів для випуску електронних грошей.

с) здійснювати операції, пов'язані з використанням електронних грошей, через окремий поточний рахунок, відкритий в емітента;

д) 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:

а) списання електронних грошей на користь торговців для оплати товарів.

б) зарахування електронних грошей від емітента/агента з поповнення/агента з розповсюдження, які отримані в обмін на безготівкові кошти.

с) списання електронних грошей на користь агента з розрахунків для обміну на безготівкові кошти.

д) зарахування електронних грошей від користувачів за реалізовані товари.

6. Електронні гроші, це –

а) національна валюта України.

б) фіатні гроші.

с) валюта іноземної держави.

д) криптовалюта.

7. Емітент електронних грошей:

а) суб'єкт господарювання, що приймає електронні гроші як засіб платежу за товари законодавства України.

б) банківська установа.

с) 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.

д) розміщує інформацію про узгодження правил використання електронних грошей на сторінці Офіційного Інтернет-представництва Національного банку

До розділів 9-10: Юридична відповідальність за порушення законодавства у сфері використання інформаційно-комунікаційних технологій. 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 203 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 відшукування 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. Здійснить 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 ІТ сфері.

БІБЛІОГРАФІЧНИЙ СПИСОК

Нормативно-правові акти

1. Конституція України. Відомості Верховної Ради України (ВВР), 1996, № 30. Ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.
2. Цивільний кодекс України. Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>.
3. 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>.
4. 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.
5. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України (ВВР), 1992, № 48. Ст. 650.
6. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Відомості Верховної Ради України (ВВР), 2011, № 32. Ст. 314.
7. Про авторське право і суміжні права: Закон України від 1 грудня 2022 року № 2811-IX. Відомості Верховної Ради (ВВР), 2023, № 57. Ст. 166.
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 42.
9. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15.07.2021. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text>.
10. Про електронні комунікації: Закон України від 16.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.
11. Про Національну програму інформатизації: Закон України. Відомості Верховної Ради України (ВВР), 1998, № 27-28. Ст. 181.
12. Про електронну комерцію: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text>.
13. 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>
14. 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>
15. Про платіжні послуги: Закон України від 30.06.2021 № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#n1249> 215
16. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>
17. Про випуск електронних грошей та здійснення платіжних операцій з ними: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/v0210500-22#Text>
18. Про цифровий контент та цифрові послуги: Закон України від 10.08.2023р. URL: <https://zakon.rada.gov.ua/laws/show/3321-20#Text>

19. Про використання доменних імен у спеціальному публічному імені .gov.ua: Закон України від 28.07.2023 № 3284-IX. URL: <https://zakon.rada.gov.ua/laws/show/3284-IX#Text>
20. Про охорону прав на винаходи і корисні моделі: Закон України від 15 грудня 1993 року № 3687-XII. Відомості Верховної Ради України (ВВР), 1994, № 7. Ст. 32.
21. Про охорону прав на промислові зразки: Закон України від 15 грудня 1993 року.
22. № 3688-XII. Відомості Верховної Ради України (ВВР), 1994, № 7. Ст. 34.
23. Про внесення змін до Податкового кодексу України та інших законодавчих актів України щодо платіжних послуг: Закон України від 12.01.2023 № 2888-IX. URL: <https://zakon.rada.gov.ua/go/2888-20>.
24. Стратегія національної безпеки України: Указ Президента України №121/2021. URL: <https://www.president.gov.ua/documents/3922020-35037>.
25. Стратегія воєнної безпеки України: Указ Президента України № 392/2020. URL: <https://www.president.gov.ua/documents/1212021-37661>.
26. Доктрина інформаційної безпеки України: Указ Президента України від 25 лютого 2017 року № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374>
27. Про затвердження Національного стандарту № 4 «Оцінка майнових прав інтелектуальної власності»: Постанова Кабінету Міністрів України; Стандарт від 03.10.2007 № 1185 (п. 3).
28. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>.
29. 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
30. Polici pfper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 Published 1 November 2023. URL: The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 – GOV.UK (www.gov.uk).
31. Національна стратегія захисту дітей в цифровому середовищі на 2021 – 2026 роки. URL: <https://thedigital.gov.ua/regulations/natsionalna-strategiya-zakhistu-ditey-v-tsifrovomuseredovishchi-na-2021-2026-roki>.

Основна

32. Верба, І. І. Основи інтелектуальної власності: навчальний посібник / за ред. С. В. Чікін. 2-ге вид., перероб. і доп. К. : НТУУ «КПІ», 2013. 132 с.
33. Гуцу, С. Ф., Матвеєва, А. В., Спіцина, Г. О. та ін. ІТ-право : навч. посіб. Х. : Нац. аерокосм. ун-т імені М. Є. Жуковського «Харків. авіац. ін-т»; «Факт», 2022. 220 с.
34. ІТ право / за заг. ред. проф. О. С. Яворської. Львів: Видавництво «Левада», 2017. 470 с.

35. Краус, К. М., Краус, Н. М., Маньзура, О. В. Електронна комерція та Інтернет-торгівля: навчально-методичний посібник. Київ : Аграр Медіа Груп, 2021. 454 с.
36. Маєвська, А. А. Електронна комерція і право : навч.-метод. посібник. – Х., 2010. 256 с.
37. Плєскач, В. Л. Електронна комерція : підручник. К. : Знання, 2007. 535 с.
38. Гуцу, С. Ф. Правові основи інформаційної діяльності : навч. посіб. Х. : Нац. аерокосм. Ун-т, 2009. 48 с.
39. 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>.

Додаткова

40. Barlow, J. A Declaration of the Independence of Cyberspace. February 8, 1996 from Davos, Switzerland.
41. Digital 2024: Country Headlines Report. UCR: <https://datareportal.com/reports/digital-2024-local-country-headlines>.
42. Malgorzata Skorzewska-Amberg Impact of ICT. Technology, Society and Sustainability: Selected Concepts, Issues and Cases. 2017/03/03. UCR: https://www.researchgate.net/publication/314196632_Impact_of_ICT_on_the_law
43. Nechyporuk, M., Pavlikov, V., Filipenko, N., Spitsyna, H., Shynkarenko, I. Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering, pp. 206-220. 216 p. ISBN 978-3-030-66716-0, ISBN 978-3-030-66717-7 (eBook). URL: <https://doi.org/10.1007/978-3-030-66717-7>.
44. Postel, J. RFC1591: Domain Name System Structure and Delegation.: RFC Editor. United States. 1994. URL: <https://dl.acm.org/doi/10.17487/RFC1591#cited-by-sec>.
45. REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG&toc=OJ:L:2015:310:TOC.
46. UDRP спір та UDRP правила. Допоможе юрист? URL: https://legalitgroup.com/domenni-batli-212worldwide/?gclid=Cj0KCQiA8vSOBhCkARIsAGdp6RQnHZjnInvaep0Gk89OhsBVyEwzml5doJAEN18kOr8xRTLY4IBR6e8aAvtjEALw_wcB.
47. Арістова, І. В., Баранов, О. А., Дзьобань, О. П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія ; за заг. ред. проф. К. І. Бєлякова. Київ : КВІЦ, 2019. 108 с.
48. Атаманова, Ю. Захист прав інтелектуальної власності у мережі Інтернет: світовий досвід та вітчизняні перспективи. Право та інновації. 2014, № 3.
49. Берч, В. В. Правове регулювання електронної комерції: міжнародні та національні стандарти // Науковий вісник Ужгородського Національного Університету,

2024. № 2(85). С.11-16. URL: https://www.researchgate.net/publication/385971130_Legal_regulation_of_e-commerce_international_and_national_standards.

50. Бойко, Д. В. Правова природа доменних імен Інтернет : автореф. дис. ... канд. юрид. наук. Харків, 2005. 19 с.

51. Бонтлаб, В. В. Цивільно-правове регулювання доменних імен : автореф. дис. ... канд. юрид. наук. Київ, 2006. 20 с.

52. Борівська, В., Михайліна, Т. Правовий режим вебсайту та його складників як об'єктів інтелектуальної власності. Підприємництво, господарство і право. 2021, № 4. С. 5-9.

53. Булат, Н. М. Доменне ім'я як засіб індивідуалізації інтернет-ресурсів. Право і суспільство. 2020, № 2. С. 154-160.

54. Булат, Н. М. Основні напрями вдосконалення чинного законодавства щодо охорони доменних імен. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2020, Том 31 (70), Ч. 1, № 2. С. 74-78.

55. Булат, Н. М. Поняття та ознаки доменного імені. Development of modern technologies and scientific potential of the world : coll. of scientific papers «ööööö» with materials of the international scientific-practical conf., London, July 29, 2019. London : NGO «European Scientific Platform», 2019. Vol. 2. pp. 33–36. 118 p.

56. Водорезова, С. Р. Особливості правової охорони комп'ютерної програми як об'єкта інформаційних відносин. Право та інновації. 2014, № 3 (7). С. 69-76.

57. Грицай, С. О. Електронні гроші: поняття та нові аспекти використання// Forum Prava, 2023. № 74(1). С. 141–150. URL: http://forumprava.pp.ua/files/141-150-2023-1-FP-Hrytsai_15.pdf.

58. Гуцу, С. Впровадження штучного інтелекту у сферу безпеки праці на підприємствах критичної інфраструктури // Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану [Електронний ресурс] : тези доповідей науково-практичної конференції, 8 листопада 2023 р., Харків / Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут». Харків : ХАІ, 2023. С. 48-53.

59. Гуцу, С. Ф. Забезпечення інформаційної безпеки людини в цифровому медіа просторі України // Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи : тези доп. учасників міжн. наук.- практ. конф. (Харків, 12-13 груд. 2023р.); Наук.-дослід. ін-т публ. політики і соц. наук. Харків: НДІ ППСН, 2023.С.71-75.

60. Гуцу, С. Ф. Правове регулювання інформаційної безпеки в авіаційній сфері: міжнародно-правовий аспект//Міждисциплінарна науково-практична конференція «Сучасні проблеми розвитку авіаційно-космічної галузі України: інженерія, бізнес, право» [Електронний ресурс] : тези доповідей науково-практичної конференції, 5 листопада 2024 року, Харків / Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут».– Харків : ХАІ, 2024. С.93-98.

61. Гуцу, С. Ф., Спіцина, Г. О. Легалізація поняття інформаційної безпеки особистості в українському законодавстві // Пропілеї права та безпеки : наук. журнал / Ред. кол. Н. Є. Філіпенко, І. Р. Шинкаренко, С. Ю. Лукашевич, та ін. Національний

аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», 2023. № 2-3. С. 37-41.

62. Д а ц ю к , В. Б. ІТ-право та економічні свободи [Текст] // Правове регулювання та економічні свободи і права : монографія / Ужгород. нац. ун-т, НДІ порівнял. публіч. права та міжнар. права. Ужгород : Рік-У, 2020. Розд. 4. С. 110-141. ISBN 978-617-7692-74-3.

63. Доменні спори: українська й міжнародна актуальна практика. Юрист & Закон, 2019, № 38. Електронне видання. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013152.

64. Дучак, Б. Електронні гроші в Україні третього світу. URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ000975.

65. Електронний документообіг: системи, види, особливості впровадження та як він працює в Україні [Електронний ресурс]. URL: <https://inbase.com.ua/elektronnyj-dokumentobig-systemy-vydy-osoblyvosti-vprovadzhennya-ta-yak-vin-praczuuye-v-ukrayini/>

66. Еннан, Р. Поняття, ознаки, сутність, специфіка та види відносин у мережі Інтернет // Теорія і практика інтелектуальної власності. 2013. № 3. С. 10–19. URL: http://nbuv.gov.ua/UJRN/Tpiv_2013_3_3.

67. Харитонов, Є., Харитонova, О. Сутність ІТ-права: пошук парадигми // Право України, 2018, №1. С. 18-29.

68. Єдиний державний реєстр судових рішень Справа №345/1819/24. Проведення № 1-кп/345/201/2024. URL: <https://youcontrol.com.ua/ru/catalog/court-document/119548591/>

69. Єфремова, К. В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспект. Право та інноваційне суспільство. 2014. № 1. С. 5–11.

70. Жуванов, Д. Яку форму правової охорони обрати для комп'ютерної програми. URL: http://www.romanenko.biz.ua/library/article_program.html.

71. Заярний, О. А. Правове забезпечення розвитку інформаційної сфери України: адміністративно-деліктний аспект : монографія. Київ : Видавничий дім «Гельветика», 2017. 700 с.

72. Іванюк, В. Д. Фінансово-правове регулювання ринку криптовалют в Україні. Дисертація на здобуття вченого ступеня доктора філософії у галузі права. Тернопіль: ЗНУ, 2021. URL: <https://www.wunu.edu.ua/svr/disertacia/ivanuk/dusertacia.pdf>.

73. Івахно, В. Криптовалюта в Україні: регулювати чи дозволити згоріти? URL: <https://loyer.com.ua/uk/kryptovalyuta-v-ukrayini-regulyuvaty-chy-dozvolity-zgority/>.

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

75. Каленіченко, 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.

76. 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.
77. Кравчук В., Науменко Д., Глибовець А. Електронні гроші в Україні. Аналітичний звіт. К. : Альфа ПІК, 2012. 64 с.
78. Кремінський, О. Правовий режим віртуальної валюти (криптовалюти) в Україні. Path of Science. 2020. Vol. 6, №4. С. 1001-1008. URL: <https://cyberleninka.ru/article/n/pravoviy-rezhim-virtualnoyi-valyuti-kriptovalyuti-v-ukrayini/viewer>.
79. Логойда, В. М. Криптовалюти як об'єкт цивільних прав: порівняльно-правовий аналіз. Дисертація на здобуття вченого ступеня доктора філософії у галузі права. Ужгород: УНУ, 2022. URL: <https://uacademic.info/download/file/0823U100192/%D0%B4%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F%20%28%D0%9B%D0%BE%D0%B3%D0%BE%D0%B9%D0%B4%D0%B0%20%D0%92.%D0%9C.%29.pdf>
80. Маловичко, С. В. Тенденції та перспективи розвитку електронної торгівлі в Україні. Економіка і регіон. 2015. № 4. С. 67-73.
81. Марценюк, О. Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію : дис. ... канд. юрид. наук : 12.00.07. Київ, 2009. 266 с.
82. 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>.
83. Могил, Л. С. Правове забезпечення використання криптовалюти в господарському обігу : дис. ... д-ра філос. / Могил Людмила Сергіївна ; Національний університет «Одеська юридична академія» – Одеса, 2023. – 223 с. URL: <https://dspace.onua.edu.ua/items/ca9af90b-a30f-454d-b28e-da1b842aa4cc>.
84. Настюк, В. Я., Білевцева, В. В. Загальноправова характеристика адміністративної відповідальності за інформаційні правопорушення. Інформація і право. 2013. № 1. С. 151–157.
85. Некіт, К. Г. Доменне ім'я як об'єкт цивільних прав. Часопис цивілістики. 2017. Вип. 23. – С. 40-44.
86. Новицький Міжнародний досвід правового регулювання інтернет. Юридичний вісник. 2014, № 2 (31). С. 52-58.
87. Новосельська, І. В., Бобровник, А. С. Теоретико-правові питання охорони авторського права в мережі інтернет. URL: <https://dilegal.ua/teoretiko-pravovi-pitannya-oxoroni-avtorskogoprava-v-merezhi-internet/>
88. 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. URL: <http://aphd.ua/it-pravoproblemy-i-perspektyvy-rozvytku-v-ukrani-chetverta-mizhnarodnashchorichna-konferentsiia/>
89. Офіційний сайт ТОВ «Хостмастер». URL: <https://hostmaster.ua/policy/2ld.ua/>

90. Писаренко, Г. М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення // Науковий вісник Ужгородського національного університету, 2016. Серія ПРАВО. Випуск 36. Том 2. С. 55-58.

91. Пономарьов, М. Узагальнення судової практики розгляду судами справ у спорах, пов'язаних із використанням імен доменів. URL: <http://artimmer.com/ua/publicacii/uzagalnennyasudovoi-praktyky/269-uzagal%60nennya-sudovo%D1%97-praktikirozglyadu-sudami-sprav-u-sporax,-pov-yazanix-%D1%96zvikoristanniam-%D1%96men-domen%D1%96>.

92. Поштаренко, О. В. До питання зародження електронних грошей // Прикарпатський юридичний вісник. 2023, Випуск 6 (53). С. 95-99. URL: http://pjuv.nuoua.od.ua/v6_2023/19.pdf

93. Регламент публічного домену (версія 3.5), вступив у дію з 24 січня 2020 року. URL: https://www.hostmaster.ua/policy/Reglament2ld_3.5_UK.pdf

94. 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>.

95. Садчикова, І., Тарасенко, А., Дубина, М. Теоретичне обґрунтування сутності поняття «електронна комерція» // Економіка та суспільство, 2023, № 53. DOI: <https://doi.org/10.32782/2524-0072/2023-53-36>.

96. 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/>

97. Спіцина, Г. О., Гуцу, С. Ф. Щодо питання правового захисту персональних даних працівників // Науковий вісник Ужгородського національного університету. Серія ПРАВО, 2023. Випуск 76. Ч .1. С. 255-260.

98. 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.

99. Сухорукова, Г. Етапи розвитку ЕДО в Україні: від минулого до сучасності. [Електронний ресурс]. URL: <https://hub.kyivstar.ua/author/ganna-suhorukova>.

100. Тарасенко, Л. Л. Комп'ютерна програма як об'єкт інтелектуального права // Матеріали Міжнародної наукової конференції (круглий стіл) на тему «ІТ-право: проблеми і перспективи розвитку в Україні» у м. Львів, 18 листопада 2016 р. URL: <http://aphd.ua/it-pravo-problemy-i-perspektyvy-rozvytku-vukrani-14/>.

101. Тицька, Я. О., Поварчук, Н. С. Доктринальні підходи щодо визначення статусу права інформаційних технологій // Київський часопис права, 2023. № 1. С. 41-46. DOI: <https://doi.org/10.32782/kij/2023.1.6>.

102. Ткачук, І. І. Статус криптовалют в Україні та інших країнах світу. Економіка і суспільство. 2018, Випуск № 16. С. 521-526. URL: https://economyandsociety.in.ua/journals/16_ukr/79.pdf.

103. Фасій, Б. В. Agile waterfall та out staff договір або договори на розробку програмного забезпечення // Часопис цивілістики, 2017, № 26. С. 98-102.

104. Філик, Н. В., Омельченко, Г. В. Комп'ютерна програма як об'єкт авторського права: проблеми правової охорони. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник. «Повітряне і космічне право», 2016, № 2(39). С. 130-137. URL: <https://europub.co.uk/articles/-A-191808>.

105. Харитонов Є. О. Право інформаційних технологій // Енциклопедія соціогуманітарної інформології / коорд. проекту та заг. ред. проф. К. І. Беляков. Київ : Видавничий дім «Гельветика», 2020. Т. 1. С. 190-194.

106. Харитонов, Є., Харитонova, О. «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>

107. Харитонova, О. І. Проблемні питання визначення системи (структури) ІТ-права // ІТ-право: проблеми і перспективи розвитку в Україні. URL: <http://aphd.ua/publication-186/>

Навчальне видання

Гуцу Світлана Федорівна

Гордеюк Алла Олександрівна

Павликівський Віталій Іванович

Філіпенко Наталія Євгенівна

Федосенко Наталія Анатоліївна

ІТ-ПРАВО

Навчальний посібник

2-ге вид. доповн. і переробл.

Зв. план, 2025

Підписано до видання 10.01.2025

Ум. друк. арк. 17,3. Обл.-вид. арк. 16,5. Електронний ресурс

Видавець і виготовлювач

Національний аерокосмічний університет ім. М. Є. Жуковського

«Харківський авіаційний інститут»

61070, Харків-70, вул. Вадима Манька, 17

URL: <http://www.khai.edu>

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції сер. ДК № 391 від 30.03.2001