



УДК 340.13:004.738

[https://doi.org/10.52058/2786-5274-2025-12\(52\)-2903-2912](https://doi.org/10.52058/2786-5274-2025-12(52)-2903-2912)

Скоморовський Віталій Богданович доктор юридичних наук, професор, професор кафедри теорії та історії держави і права Університету економіки та права «КРОК», м. Київ, <https://orcid.org/0000-0002-1020-2322>

Корольова Вікторія Вікторівна кандидат юридичних наук, доцент, завідувач кафедри державно-правових дисциплін Університету економіки та права «КРОК», м. Київ, <https://orcid.org/0000-0003-2998-6144>

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ СКЛАДУ ПРАВОПОРУШЕНЬ У МЕРЕЖІ ІНТЕРНЕТ

Анотація. У статті здійснено комплексне теоретико-правове дослідження формування складу правопорушень у мережі Інтернет, що зумовлено стрімким розвитком цифрових технологій і зростанням кількості протиправних діянь, які відбуваються у віртуальному середовищі. Показано, що сучасна правова доктрина оперує широким спектром термінологічних конструкцій – інформаційні, комп'ютерні, кібернетичні правопорушення, делікти у сфері інформаційних технологій – однак їх змістова неоднорідність створює методологічні труднощі у формуванні єдиного підходу до правового аналізу цифрових правопорушень. Послідовно розкрито вплив історичного розвитку мережі Інтернет на формування правових підходів до її регулювання та окреслено ключові напрями наукових досліджень, що стали підґрунтям для становлення інформаційного та цифрового права в Україні.

Особливу увагу приділено концептуальним засадам, запропонованим О.Марценюком, який адаптує традиційну чотирикомпонентну модель складу правопорушення до особливостей цифрового середовища. Показано, що в Інтернет-просторі кожен елемент складу набуває нового змісту: об'єктом посягання стають інформація, інформаційні ресурси та телекомунікаційні системи; об'єктивна сторона реалізується через технічно опосередковані дії, пов'язані з доступом, модифікацією, блокуванням чи знищенням даних; суб'єкт характеризується наявністю спеціальних знань у сфері ІТ та здатністю до анонімізації; суб'єктивна сторона найчастіше проявляється як умисна форма вини. Проаналізовано подальший розвиток доктринального підходу, який призвів до формування концепції інформаційних правопорушень як міжгалузевої категорії, водночас підкреслено неприпустимість ототожнення цієї категорії з усім комплексом Інтернет-правопорушень.

Доведено, що відсутність усталеного понятійного апарату та належної систематизації складів правопорушень у цифровій сфері ускладнює ефективне



застосування норм юридичної відповідальності. Обґрунтовано необхідність розроблення цілісної теоретико-методологічної моделі цифрових деліктів, яка б враховувала особливості віртуального середовища, технічну природу діянь та специфіку наслідків, що можуть проявлятися як у кіберпросторі, так і в реальному житті. Зроблено висновок, що оновлення теоретичних підходів та уточнення складу правопорушень у мережі Інтернет є ключовими умовами вдосконалення законодавства та підвищення ефективності юридичної відповідальності у сфері інформаційних відносин.

Ключові слова: Інтернет, правопорушення, юридична відповідальність, інформаційні технології, діджиталізація, правове регулювання, захист персональних даних.

Skomorovsky Vitalii Bohdanovych Doctor of Law, Professor, Professor of the Department of Theory and History of State and Law, University of Economics and Law “KROK”, Kyiv, <https://orcid.org/0000-0002-1020-2322>

Korolova Viktoriia Viktorivna Candidate of Law, Associate Professor, Head of the Department of Public-Law Disciplines, University of Economics and Law “KROK”, Kyiv, <https://orcid.org/0000-0003-2998-6144>

THEORETICAL AND LEGAL PRINCIPLES OF FORMING THE COMPOSITION OF OFFENSES ON THE INTERNET

Abstract. The article presents a comprehensive theoretical and legal study of the formation of offenses in the Internet, driven by the rapid development of digital technologies and the increasing number of unlawful acts occurring in the virtual environment. It is shown that modern legal doctrine employs a wide range of terminological constructions – information, computer, cyber offenses, and delicts in the field of information technologies – yet their substantive heterogeneity creates methodological difficulties in forming a unified approach to the legal analysis of digital offenses. The impact of the historical development of the Internet on the formation of legal approaches to its regulation is consistently revealed, and the key directions of scientific research that have laid the foundation for the development of information and digital law in Ukraine are outlined.

Particular attention is paid to the conceptual foundations proposed by O.Martsenyuk, who adapts the traditional four-component model of an offense to the specifics of the digital environment. It is shown that in the Internet space, each element of the offense acquires a new meaning: the object of encroachment becomes information, information resources, and telecommunication systems; the objective side is realized through technically mediated actions related to access, modification, blocking, or destruction of data; the subject is characterized by the possession of specialized IT knowledge and the ability to anonymize; the subjective side most often



manifests as an intentional form of guilt. The further development of the doctrinal approach, which led to the formation of the concept of information offenses as an interdisciplinary category, is analyzed, while emphasizing the inadmissibility of equating this category with the entire complex of Internet offenses.

It is demonstrated that the absence of a well-established conceptual apparatus and proper systematization of offenses in the digital sphere complicates the effective application of legal liability norms. The necessity of developing a holistic theoretical and methodological model of digital delicts is substantiated, which would take into account the peculiarities of the virtual environment, the technical nature of actions, and the specific consequences that may manifest both in cyberspace and in real life. The conclusion is drawn that updating theoretical approaches and clarifying the composition of offenses in the Internet is a key condition for improving legislation and enhancing the effectiveness of legal liability in the field of information relations.

Keywords: Internet, offenses, legal liability, information technologies, digitalization, legal regulation, personal data protection.

Постановка проблеми. Сучасна правова наука доволі вільно та регулярно керується термінологічним апаратом, який стосується особливостей правопорушень в мережі Інтернет. Наразі вже стійкими конструкціями у розрізі даної тематики є такі поняття, як інформаційні правопорушення, комп'ютерні правопорушення, правопорушення у сфері комп'ютерної інформації, правопорушення в галузі інформаційних технологій, правопорушення проти інформаційної безпеки, правопорушення в мережі Інтернет, кібернетичні правопорушення тощо [1, с. 38]. Не претендуючи на можливість та об'єктивність дослідження кожного з формулювань слушно зауважити, що своєрідна «легітимізація» цих понять була обумовлена стрімким і невинним розвитком технологій, що значно прискорило динаміку поширення цих термінів. Разом з цим, певне підґрунтя для цього форсованого процесу було окреслено деякими науковими розробками в частині правового регулювання деліктів і відповідальності за них у разі їхнього скоєння віртуально, без конкретного (точніше – обов'язкового) зв'язку з місцем скоєння.

Аналіз останніх досліджень і публікацій. Попри на зростання кількості правопорушень в Інтернеті та значущість проблеми юридичної відповідальності за них, наукові дослідження цього напрямку в українській правовій науці залишаються обмеженими. Багато аспектів правопорушень у цифровому середовищі, зокрема визначення їх складу та адаптація існуючих інститутів юридичної відповідальності до специфіки Інтернету, досі не опрацьовані, а фундаментальної теоретико-методологічної моделі, яка б інтегрувала традиційні правові конструкції з особливостями цифрового простору, наразі не існує. Водночас певні результати представлені у публікаціях українських науковців, зокрема Д. Азарова, М. Антоновича, Н. Антонюк, Є. Алісової, В. Андрієшина, Н. Ахтирської, Ю. Барабаша, К. Басіни, О. Батанова, Л. Бели та інших.



Їхні роботи охоплюють класифікацію інформаційних правопорушень, проблеми правового регулювання Інтернету, механізми захисту інформації та застосування юридичної відповідальності за цифрові правопорушення, зокрема адміністративної та кримінальної. Проте більшість досліджень мають фрагментарний характер, зосереджуючись на окремих видах порушень або інститутах відповідальності, що не дозволяє сформуувати комплексну концепцію цифрових деліктів. Таким чином, наявна наукова база потребує систематизації та розробки узгодженої теоретико-правової моделі складу правопорушень в Інтернеті, що визначає актуальність подальших досліджень у цій сфері.

Мета статті – здійснити комплексний теоретико-правовий аналіз формування складу правопорушень у мережі Інтернет, визначити специфіку його елементів в умовах цифрового середовища.

Виклад основного матеріалу. У контексті наукових досліджень з приводу визначення місця юридичної відповідальності за правопорушення в мережі Інтернет значну роль цілком закономірно відіграє закордонний досвід. Насамперед це стосується США: це обумовлено історично, оскільки ця держава технологічно стала батьківщиною становлення цієї технології.

Однією з основних проблем, пов'язаних із недосконалістю правової системи у сфері кібербезпеки, є її нестабільність та швидкий розвиток. Бюрократичні структури інституту правової відповідальності неспроможні вчасно реагувати на ці зміни через свою консервативність. Нормативні правила, які створено раніше, вже не відповідають новим реаліям, оскільки правопорушення в мережі Інтернет не є тотожними звичним протиправним діям [2, с. 29]. В підсумку правові інститути не можуть розробити чітких та ефективних правил поведінки для охоплення всіх видів кіберзлочинів, оскільки ці види порушень вийшли за межі раніше створених законодавчих засад.

В сучасному світі постають нові вимоги до адекватності правового регулювання у сфері інформації, зокрема в контексті боротьби з порушеннями інформаційного характеру. Тому вчені й фахівці з кримінального та адміністративного права, криміналістики та кримінології все частіше проводять дослідження цих правопорушень, звертаючи увагу на юридичну відповідальність, методи виявлення, розслідування та запобігання порушенням. Проте проблема загального розуміння юридично значущих аспектів інформаційних правопорушень, їх взаємозв'язку з іншими видами порушень та юридичних заходів залишається малодослідженою як в рамках загальної теорії права, так і у науці інформаційного права. Інші комплексні наукові напрями спрямовані на вивчення інформаційних правопорушень, включаючи сферу інформаційної деліктології [3, с. 251].

Розглядаючи наукові дослідження в частині правопорушень в мережі Інтернет у багатьох роботах, присвячених даній тематиці, йдеться лише про юридичну відповідальність та правопорушення інформаційного характеру, ігноруючи той факт, що не кожне правопорушення, втілене в інформаційному



середовищі, є суто інформаційним. Наприклад, подібної думки дотримується І. Сторожук в рамках окреслення поняття «інформаційне правопорушення» [4, с. 166].

Інтернет як мережа бере своє коріння із військових розробок оборонно-наукових відомств США. У 1969 році за ініціативою Пентагону було створено Агентство передових дослідницьких проєктів Міністерства оборони США – DARPA (Department of Defense ARPA – Advanced Research Projects Agency) [5, с. 20]. До кінця 1969 р. було запущено та сполучено чотири хост-комп'ютери в первинну мережу ARPANET (Advanced Research Projects Agency Network – мережа Агентства Перспективних Досліджень), яка стала зародком мережі Інтернет [6, р. 31].

Кардинальним зламом у розповсюдженні Інтернету в якості інновації стали 90-і роки ХХ ст. Зокрема, у 1990 році відбулася історична подія – перший запуск Всесвітньої Павутини. Проте після цього етапу розвитку, Інтернет залишався в основному областю для технічних ентузіастів протягом наступних трьох років, і комерційний сектор та громадськість не виявляли до нього особливого інтересу [7, с. 53]. До червня 1993 року менше ніж 2 % центральних комп'ютерів, що були частиною цієї мережі, мали комерційний статус. У тому ж році група студентів в університеті штату Іллінойс, включаючи Марка Андерсена, який став співзасновником компанії Netscape Inc, розробила веббраузер і супутні програмні застосунки, які дозволяли користувачам переглядати все більше та більше вебсайтів, а також відображати й відправляти примітивну графіку та текст. Цей браузер, опублікований в мережі Інтернет, почав швидко поширюватися по всьому світу, В результаті як індивідуальні користувачі, так і компанії стали створювати особисті «домашні сторінки» для публікації різних матеріалів, спочатку просто для задоволення. Бурхливий ріст, який відбувся в кінці 1993 року, був надзвичайно швидким, навіть за технологічними стандартами. До липня 1996 року кількість комп'ютерів, підключених до мережі, зросла більш ніж в тисячу разів, досягнувши 150 тисяч. Бізнес великих розмірів також вступив у світ Інтернету, і до кінця 1996 року 90 % вебсайтів мали розширення «com» [8, р. 134-135].

Представлені події в світлі розвитку Інтернету є лише малою частиною стрімкого процесу еволюції Інтернету. В контексті поточного етапу дослідження висвітлення цих подій є побічним з урахуванням відмінностей у темпах розвитку наукової доктрини та самої мережі Інтернет як багатофункціонального інформаційно-комунікаційного середовища. До слова, одним з центральних об'єктів наукових розробок відносно мережі Інтернет, її правового регулювання є в першу чергу поняття «Інтернет».

Навіть зараз немає єдиного розуміння і визначення цього ключового поняття, розуміння його природи. Отже, і предмет регулювання є досить розпливчастим і неоднорідним. Серед першовідкривачів глибинного вивчення даної проблеми в Україні стали А. Тадейко та К. Шахбазян.



А. Тадейко вважає, що Інтернет – це електронна комунікаційна мережа, що зв'язує комп'ютери в усьому світі через телефонні лінії і кабелі з оптичних волокон [9, с. 116]. К. Шахбазян визначає поняття мережі Інтернет для міжнародного права як міжнародну телекомунікаційну мережу загального користування, призначену 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 [10]. О. Зайцева визначає Інтернет як глобальний інформаційний простір, що ігнорує державні кордони, і це робить його явищем нового рівня у світовій спільноті. Ця система є унікальним засобом доступу до інформації щодо будь-яких видів діяльності або інтересів людини. Вона також є об'єктом для розробки та впровадження новітніх програмних та інструментальних технологій, що робить Інтернет сферою інтенсивного розвитку в майбутньому [11, с. 193].

Репрезентовані вище дефініції, що були запропоновані науковцями, набули поширення та стали обговорюватися лише ХХІ столітті. Фактично, більшість фундаментальних дисертаційних праць та монографій, які хоча б дотично стосувалися проблеми за цим питанням, побачили світ вже після 2005 року, що свідчить про певний період стагнації у відношенні розробки поточної тематики: К. Беляков «Інформація та Інтернет в праві: теорія і практика» [12], І. Орехова «Державний контроль господарської діяльності: адміністративно-правові засади» [13], О. Леонідова «Адміністративна відповідальність за проступки у сфері телекомунікацій» [14], «Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію» О. Марценюка (2009) [15].

І. Орехова резюмує, що державний контроль за функціонуванням мережі Інтернет має бути закріплено в рамках поняття державного контролю у сфері господарської діяльності та належним чином закріплено (враховуючи положення спеціальних законів, наприклад ЗУ «Про телекомунікації») [13, с. 10]. Науковиця вказує, що контроль за змістом використання мережі Інтернет деякими групами суб'єктів є не менш важливим в контексті втілення контрольної та превентивної функцій, ніж податковий, ціновий чи антимонопольний види контролю.

О. Леонідов, розглядаючи юридичну відповідальність за правопорушення в мережі Інтернет у світлі регламентації телекомунікацій, пропонує встановити особливості провадження у справах про адміністративні правопорушення, вчинені у сфері функціонування мережі Інтернет. При цьому з огляду на нерозробленість видів та юридичних складів правопорушень вчений рекомендує проводити градацію таких правопорушень і на законодавчому рівні узгодити й прийняти критерії зіставлення юридичної відповідальності, санкції/покарання за нього зі звичайним аналогічним правопорушенням [14, с. 9].



О. Марценюк в якості універсального способу врегулювання спеціального режиму юридичної відповідальності за правопорушення в мережі Інтернет пропонував прийняття профільної кодифікації – Інформаційного кодексу України [15, с. 39]. Цінність даної роботи полягає у тому числі в намаганні автором чітко визначити склад правопорушень в мережі Інтернет. Закономірно, що при різноманітні можливих протиправних і суспільно небезпечних дій в мережі Інтернет уніфікований склад не здатний відтворити всі потенційні варіанти. Разом з цим його визначення власне сприяє розвитку ідеї особливого підходу до питання юридичної відповідальності за ці правопорушення.

О. Марценюк, аналізуючи природу правопорушень, що вчиняються в мережі Інтернет, пропонує розглядати їх крізь призму традиційного чотирикомпонентного складу правопорушення, однак наголошує на тому, що кожен елемент цього складу набуває специфічного цифрового змісту. На думку дослідника, правопорушення в Інтернеті спрямоване передусім на інформацію, інформаційні ресурси, інформаційні системи, телекомунікаційні мережі та права суб'єктів на доступ чи використання інформації, що відрізняє такі діяння від звичайних правопорушень у матеріальному світі. Особливістю об'єктивної сторони є те, що ці дії здійснюються у віртуальному середовищі та реалізуються за допомогою спеціальних технічних засобів — комп'ютерів, мережевого обладнання, програмного забезпечення чи інших цифрових технологій. Спосіб їх вчинення полягає у доступі до даних, їх модифікації, копіюванні, блокуванні, знищенні, розповсюдженні чи іншому впливі на інформаційний контент або структуру системи. Наслідки таких діянь можуть виявлятися як у кіберпросторі (порушення роботи ресурсу, втрата або спотворення інформації), так і в реальному житті (матеріальні збитки, обмеження прав громадян або суб'єктів господарювання), а причинний зв'язок між дією та наслідком часто має опосередкований характер через функціонування мережевих технологій. Суб'єкт правопорушення, як зазначає Марценюк, є фізичною або юридичною особою, яка має навички роботи з інформаційними технологіями, володіє знаннями у сфері комп'ютерної техніки або електронних комунікацій та може здійснювати дії дистанційно, використовуючи засоби анонімізації — проксі-сервери, VPN, TOR та інші способи приховування даних про себе. Суб'єктивна сторона таких діянь переважно характеризується умислом: правопорушник усвідомлює цифровий характер своїх дій, передбачає можливість настання негативних наслідків і бажає чи допускає їх настання. Мотиви можуть бути корисливими — наприклад, при викраденні даних, шахрайстві чи вимаганні; хуліганськими — при зламуванні сайтів або поширенні шкідливого програмного забезпечення; ідеологічними — у випадках кібератак; або ж заснованими на особистих мотивах, як-от помста чи недобросовісна конкуренція. Таким чином, Марценюк фактично формує уявлення про правопорушення в Інтернеті як про суспільно небезпечне, протиправне діяння, вчинене у цифровому середовищі з використанням інформаційно-телекомунікаційних систем, яке має особливу



технічну природу, спрямоване на інформацію та її носії та здатне спричиняти наслідки як у віртуальному, так і у реальному світі.

Згодом, внаслідок ревізії цієї позиції, у вітчизняній доктрині усталено вважається, що інформаційні правопорушення як окремий міжгалузевий вид правопорушень охоплює усі протиправні діяння, які певним чином пов'язані з інформацією і за які встановлюється кримінальна, адміністративна, цивільно-правова та інша юридична відповідальність [16, с. 52]. Слід зауважити, що звичайно ототожнення інформаційних правопорушень з кластером усіх правопорушень в мережі Інтернет неприпустимо.

Висновки. Проведене дослідження доводить, що теоретико-правові засади формування складу правопорушень у мережі Інтернет перебувають у стадії активного становлення та характеризуються відсутністю усталеної доктринальної єдності. Стрімкий розвиток цифрових технологій зумовлює появу нових форм протиправних діянь, які не вкладаються у межі традиційних правових конструкцій, що створює значний розрив між реальною практикою та можливостями правового регулювання. Аналіз наукових підходів, зокрема позиції О. Марценюка, свідчить про необхідність адаптації класичної моделі складу правопорушення до специфіки цифрового середовища, у межах якого змінюється зміст кожного елементу – об'єкта, об'єктивної та суб'єктивної сторони, а також суб'єкта правопорушення.

Водночас розширення доктринального розуміння інформаційних правопорушень не повинно призводити до їх некоректного ототожнення з усім спектром правопорушень, що вчиняються в Інтернеті. Удосконалення понятійного апарату та формування концептуально цілісної моделі цифрових деліктів є необхідною передумовою подальшого розвитку законодавства та підвищення ефективності юридичної відповідальності у сфері інформаційних відносин.

Література:

1. Тихомиров О.О. Інформаційні правопорушення: теоретико-правова концепція. Інформаційна безпека людини, суспільства, держави. 2015. № 1 (17). С. 38-47.
2. Загребельна Н.А. Поширення юридичної відповідальності за правопорушення в мережі Інтернет в умовах воєнного стану. Аналітично-порівняльне правознавство. 2022. № 2. С. 28-32.
3. Максименко Ю.Є. Засади розвитку інформаційної деліктології. Право України. 2013. № 10. С. 249-256.
4. Сторожук І.П. До питання структурування категорії «інформаційне правопорушення». Юридичний науковий електронний журнал. 2020. № 5. С. 165-168.
5. Спасибо І.А. Щодо історії виникнення глобальної мережі Інтернет. Право та інновації. 2014. № 3 (7). С. 15-26.
6. Cohen-Almagor R. Internet history. Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice. 2013. P. 19-39.
7. Новицький А.М. Міжнародний досвід правового регулювання Інтернету. Юридичний вісник. 2014. № 2 (31). С. 52-58.
8. Yoshai Benkler. From Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access, 2000. 561 p.



9. Гуцу С.Ф. Правове регулювання мережі Інтернет: міжнародний і вітчизняний досвід. Вісник НТУУ «КПІ». Політологія, соціологія, право. 2018. № 2 (38). С. 114-118.
10. Шахбазян К.С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: автореф. дис ... канд. юрид. наук: 12.00.11. Київ, 2009. 19 с.
11. Зайцева О.К. Становлення міжнародної політики регулювання Інтернет-середовища. Вісник НТУУ «КПІ». Політологія, соціологія, право: зб. наук. праць. Київ: ІВЦ «Політехніка», 2009. № 4. 193 с.
12. Беляков К.І. Інформація в праві: теорія і практика: монографія. Київ: видавництво «КВЦ». 2006. 116 с.
13. Орехова І.С. Державний контроль господарської діяльності: адміністративно-правові засади: автореф. дис. ... канд. юрид. наук : 12.00.07 / І.С. Орехова; кер. роботи С.В. Ківалов; НУ «ОЮА». Одеса, 2009. 21 с.
14. Леонідова О. Адміністративна відповідальність за проступки у сфері телекомунікацій: автореферат дис. канд. юрид. наук 12.00.07. Харківський національний університет внутрішніх справ. Харків, 2010. 19 с.
15. Марценюк О. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію: дис. канд. юрид. наук 12.00.07. Київський національний університет внутрішніх справ. Київ, 2009. 242 с.
16. Кирилюк А.В. Поняття та види інформаційних правопорушень. Часопис цивілістики НУ «ОЮА». 2020. № 26. С. 51-56.

References:

1. Tykhomyrov, O.O. (2015). Informatsiyni pravoporushennia: teoretyko-pravova kontseptsiiia [Information offenses: Theoretical and legal concept]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy*, (1)17, 38–47. [in Ukrainian]
2. Zahrebelna, N.A. (2022). Poshyrennia yurydychnoi vidpovidalnosti za pravoporushennia v merezhi Internet v umovakh voiennoho stanu [Extending legal liability for Internet offenses under martial law]. *Analychno-porivnialne pravoznavstvo*, (2), 28–32. [in Ukrainian]
3. Maksymenko, Y.E. (2013). Zasady rozvytku informatsiinoi deliktologii [Principles of the development of information delictology]. *Pravo Ukrainy*, (10), 249–256. [in Ukrainian]
4. Storozhuk, I.P. (2020). Do pytannia strukturuvannia katehorii «informatsiine pravoporushennia» [On the issue of structuring the category “information offense”]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (5), 165–168. [in Ukrainian]
5. Spasibo, I.A. (2014). Shchodo istorii vynyknennia hlobalnoi merezhi Internet [On the history of the emergence of the global Internet]. *Pravo ta innovatsii*, (3)7, 15–26. [in Ukrainian]
6. Cohen-Almagor, R. (2013). Internet history. In *Moral, ethical, and social dilemmas in the age of technology: Theories and practice* (pp. 19–39). [in English]
7. Novytskyi, A.M. (2014). Mizhnarodnyi dosvid pravovoho rehuliuвання Internetu [International experience in Internet legal regulation]. *Yurydychnyi visnyk*, (2)31, 52–58. [in Ukrainian]
8. Benkler, Y. (2000). *From consumers to users: Shifting the deeper structures of regulation towards sustainable commons and user access* (561 p.). [in English]
9. Huts, S.F. (2018). Pravove rehuliuвання merezhi Internet: mizhnarodnyi i vitchyzniannyi dosvid [Legal regulation of the Internet: International and domestic experience]. *Visnyk NTUU “KPI”. Politolohiya, sotsiolohiia, pravo*, (2)38, 114–118. [in Ukrainian]
10. Shakhbazian, K.S. (2009). Mizhnarodno-pravovi osnovy rehuliuвання vidnosyn v merezhi Internet [International legal foundations for regulating relations in the Internet] (Author’s abstract of PhD dissertation, Kyiv). 19 p. [in Ukrainian]





11. Zaitseva, O.K. (2009). Stanovlennia mizhnarodnoi polityky rehuliuвання Internet-seredovyscha [Formation of international Internet regulatory policy]. *Visnyk NTUU "KPI". Politolohiya, sotsiologhiia, pravo: zb. nauk. prats*, (4), 193 p. [in Ukrainian]
12. Beliakov, K.I. (2006). *Informatsiia v pravi: teoriia i praktyka* [Information in law: Theory and practice]. Kyiv: KVITS. 116 p. [in Ukrainian]
13. Orekhova, I.S. (2009). Derzhavnyi kontrol hospodarskoi diialnosti: administratyvno-pravovi zasady [State control of economic activity: Administrative-legal principles] (Author's abstract of PhD dissertation, Odesa). 21 p. [in Ukrainian]
14. Leonidova, O. (2010). Administratyvna vidpovidalnist za prostupky u sferi telekomunikatsii [Administrative liability for offenses in telecommunications] (Author's abstract of PhD dissertation, Kharkiv). 19 p. [in Ukrainian]
15. Martseniuk, O. (2009). Teoretyko-metodolohichni zasady informatsiinoho prava Ukrainy: realizatsiia prava na informatsiiu [Theoretical and methodological foundations of information law in Ukraine: Implementation of the right to information] (PhD dissertation, Kyiv National University of Internal Affairs). 242 p. [in Ukrainian]
16. Kyryliuk, A.V. (2020). Poniattia ta vydy informatsiinykh pravoporushen [Concept and types of information offenses]. *Chasopys tsyvilityky NU "OYuA"*, (26), 51–56. [in Ukrainian]