УДК 340.12:172.12:316.72

ВЗАЄМОДІЯ ПРАВА ТА МОРАЛІ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

INTERCONNECTION OF LAW AND MORALITY IN THE INFORMATIONAL SOCIETY

Крилова Д.С.,
аспірант кафедри теорії та історії держави і права
Запорізького національного університету

У статті розглянуто проблеми та перспективи розвитку правового регулювання таких аспектів існування інформаційного суспільства, як електронна комерція, комп'ютерна злочинність, інформаційна безпека, інформаційні війни, а також інтелектуальна власність. Мета дослідження полягає у виявленні особливостей взаємодії права та моралі в інформаційному суспільстві та обґрунтуванні на цій основі шляхів удосконалення українського законодавства. У процесі аналізу встановлено, що в умовах інформаційного суспільства зростає роль як правових, так і моральних регуляторів.

Ключові слова: інформаційне суспільство, мораль, комп'ютерна злочинність, інформаційна безпека, інтелектуальна власність, електронна комерція, інформаційні війни.

В статье рассмотрены проблемы и перспективы развития правового регулирования таких аспектов существования информационного общества, как электронная коммерция, компьютерная преступность, информационная безопасность, информационные войны, а также интеллектуальная собственность. Цель исследования заключается в том, чтобы установить особенности взаимодействия права и морали в информационном обществе и обосновании путей усовершенствования украинского законодательства. В процессе анализа установлено, что в условиях информационного общества возрастает роль как правовых, так и моральных регуляторов.

Ключевые слова: информационное общество, мораль, компьютерная преступность, информационная безопасность, интеллектуальная собственность, электронная коммерция, информационные войны.

The article views in the problem and perspectives of legal regulation development of such aspects of informational society existence as electronic commerce, computer criminality, informational safety, informational wars and intellectual property. The purpose of the research lies in revealing this interoperating peculiarities and grounding on this basement the ways of Ukrainian legislation improvement. In the process of research the author estimates that under the conditions of informational society the role of legal and moral regulators grows considerably.

Key words: informational society, morality, cyber-crime, information security, intellectual property, electronic commerce, informational wars.

Вступ. Світовий та вітчизняний досвід суспільного розвитку свідчить, що впродовж всієї історії людства простежується складний і суперечливий процес взаємодії права та моралі як основних регуляторів поведінки людини. Зміст і характер цієї взаємодії визначається багатьма чинниками, які в кінцевому підсумку зумовлюють їх гармонійне поєднання або протистояння. В умовах становлення глобального інформаційного суспільства взаємодія права та моралі актуалізується, набуває нових форм і проявів. Зазначене зумовлено прискореним поширенням мережі Інтернет, що чинить вплив на мораль на всіх рівнях: від загальнолюдського до індивідуального. За таких умов виникає необхідність у трансформації правових регуляторів, відображення в них тих змін, які відбуваються у сфері моралі, могли б забезпечити більш оптимальне правове регулювання.

Методологічною основою дослідження взаємодії права та моралі в інформаційному суспільстві слугують праці тих учених, які досліджували правові аспекти інформаційного суспільства та окремі аспекти взаємодії права та моралі, зокрема, таких як О.Г.аДанильян, О.П. Дзьобань, І.В. Ховрак, В.В. Карасюк, М.А. Судейко, С.В. Шапочка, А.М. Куліш, В.В. Тютюнник, Л.Г. Удовика та інших. Проте на сьогодні недостатньо розробленою залишається тема взаємодії права та моралі в умовах існування інформаційного суспільства.

Мета дослідження полягає у виявленні особливостей взаємодії права та моралі в інформаційному суспільстві та обґрунтуванні на цій основі шляхів удосконалення вітчизняного законодавства.

Виклад основного матеріалу. Сучасний досвід прискореного розвитку інформаційно-комунікаційних технологій поставив перед інформаційним суспільством низку проблем, що перебувають на стику правового та морального поля. Так, О.Г. Данильян і О.П. Дзьобань зазначають, що в умовах інформаційного суспільства посилюється протистояння між традиційними та інноваційними цінностями. Гостро стоять питання опосередкованого спілкування, комп'ютерної злочинності, інформаційної безпеки, контролю над особистим життям, відповідності поведінки індивіда в реальному та віртуальному просторах, створення віртуальних (псевдо) особистостей тощо [1, с. 16]. Зазначений перелік не є вичерпним. До нього варто додати насамперед зростаючу кількість порушень прав інтелектуальної власності та необхідність правової охорони інформації. Особливої уваги заслуговує також проблема опосередкованого спілкування, яка має два виміри: правовий та моральний. У моральному вимірі ця проблема більшою мірою стосується скорочення

безпосередніх міжособистісних контактів. Проте у правовому вимірі вона виявляється скоріше у необхідності правового регулювання правочинів, укладених дистанційно, зокрема, електронної комерції.

Як зазначає І.В. Ховрак, електронну комерцію можна розглядати як одну із сучасних форм організації і здійснення господарської діяльності, відмінною рисою якої є використання загальнодоступних інформаційних систем та комп'ютерних мереж, об'єднаних Інтернетом [2, с. 16]. Вітчизняні вчені зазначають, що електронна комерція (e-commerce) – вид електронної комерційної діяльності – продаж, здача в оренду, надання ліцензій, постачання товарів, послуг або інформації та іншого з використанням інформаційних комунікаційних технологій. Поняття «е-комерція» ширше, ніж поняття «електронна торгівля», оскільки воно охоплює всі види електронної і комерційної діяльності. Інакше кажучи, це обмін матеріальних або віртуальних товарів/послуг на гроші (електронні) між об'єктами комерційної діяльності в мережі Інтернет, причому весь цикл комерційної трансакції або її частина здійснюється електронним способом [3, с. 33].

Такі вчені, як В.В. Карасюк та М.А. Судейко зазначають, що електронна комерція є комплексним поняттям, яке в технологічному плані спирається на обмін комерційною інформацією через мережу Інтернет, а в правовому плані має в основі такі категорії, як електронний документ, електронний підпис, електронний обмін документами, електронний договір, електронні розрахунки та деякі інші [4, с. 59].

У правовідносинах електронної комерції діють як правові, так і моральні регулятори. До моральних варто віднести такі чинники, як моральна свідомість суб'єкта, а також бажання уникнути суспільного осуду, що може призвести до втрати ділової репутації. До правових регуляторів належить цивільне, адміністративне та кримінальне законодавство. Цивільне право забезпечує належне здійснення електронної комерції, а також встановлює основні правила цього виду діяльності, регулює відшкодування шкоди, завданої у випадку порушень прав споживачів. Кримінальне та адміністративне законодавство передбачає санкції за правопорушення в цій сфері.

Однією з переваг електронної комерції, на думку вчених, є однаковий доступ до ринку як для великих корпорацій, так і для невеликих фірм [2, с. 19]. Це є досить позитивним з морального погляду, оскільки дає малому бізнесу можливість подальшого розвитку. Глобалізація поставила перед державами необхідність підтримки малого бізнесу, що в умовах гегемонії ТНК є досить складним завданням. Вважаємо, що подальший розвиток правового регулювання електронної комерції згодом стане одним із пріоритетних напрямів законотворчості як сучасних розвинутих держав, так і України.

Серед недоліків електронної комерції, які виокремлюються вченими, є низка таких, які мають також і моральне значення. Серед них зокрема такі, як: 1) низький рівень безпеки і захисту від шахрайства (разом зі зростанням обсягу ринків електронної комерції зростає і кількість комп'ютерних злочинців. Остерігаючись великих фірм, що мають надійні системи безпеки, комп'ютерні злочинці насамперед атакують невеликі інтернет-магазини та їх клієнтів); 2) обмеження прав споживача (оскільки споживачі не мають змоги повною мірою пересвідчитись у якості товару чи послуги доти, доки вони не будуть доставлені, то фірми часто розробляють умови транзакції, всіляко утискуючи права споживачів); 3) велика кількість непрофесіоналів серед фірм, зайнятих електронною комерцією [2, с. 19].

Інформаційне суспільство поставило перед державою необхідність захисту громадян від нового виду злочинів, насамперед, інтернет-шахрайства. Варто визнати, що моральні регулятори поведінки у цій сфері діють не так ефективно, як зі звичайним шахрайством. Це зумовлено низкою чинників, що включають, по-перше, «віддаленість» жертви від злочинця, відсутність безпосереднього спілкування між ними; по-друге, потерпілим від цього злочину може стати будь-хто, і злочинець не обирає жертву заздалегідь. Це може заспокоїти совість злочинця, у якого виникає ілюзія того, що потерпілі від його діяльності ті, у кого не соромно красти. Наприклад, він може уявляти, що в тих, хто може дозволити собі певну покупку через мережу Інтернет, є зайві гроші, втрата яких буде непомітною у бюджеті жертви. Або заспокоювати себе думкою, що потерпілий сам винен, бо був надто дурний, щоб запідозрити обман, і наступного разу буде розумніший, а злочинець навіть робить йому послугу, даючи гіркий урок.

Окрім того, інтернет-шахрай меншою мірою усвідомлює загрозу покарання, ніж злочинець, що діяв у безпосередньому контакті із жертвою. Адже його зв'язок із потерпілим є випадковим, а сам процес скоєння злочину залишився без свідків. Один з головних принципів кримінального права – принцип невідворотності покарання, втрачає для суб'єкта злочинної діяльності будь-який сенс.

За таких умов зростає необхідність у підсиленні правових регуляторів. Саме тому задля зменшення кількості інтернет-шахрайств необхідно звести до мінімуму латентність цього виду злочинів. Це є одним із провідних завдань сучасної криміналістики і водночас одним із найскладніших.

У контексті зазначеного С.В. Шапочка зазначає, що шахрайство, яке вчиняється з використанням комп'ютерних мереж, є порівняно новим видом злочину з високим рівнем латентності, величезною кількістю способів учинення, необмеженими часом і простором можливостями щодо вчинення, використанням специфіки мережі Інтернет – неможливості забезпечення стовідсоткового контролю за користувачами, які мають статус анонімності, несуть мінімальну відповідальність за свої дії та можуть з будь-якого місця, використовуючи комп'ютерно-телекомунікаційні пристрої, вчинити злочин у будь-якій точці світу, у будь-який час доби [5, с. 334–335]. Проте попри ці складнощі, проблема комп'ютерної злочинності потребує негайного вирішення, а завданням учених є виявлення факторів, що сприя-

ють зростанню цього виду злочинів, удосконаленню методики їх розслідування. Безпосереднім завданням держави в цьому напрямі є заохочення дослідників для плідної праці та розробка певних програм дій для координації наукових пошуків.

Щодо обмеження прав споживача в правовідносинах електронної комерції варто зазначити, що в правовому полі захистити споживача від зловживань можливо лише через вдосконалення законодавства. Але фірми і надалі знаходитимуть легальні засоби обійти небажані правові приписи. Проте громадськість може застосовувати суспільний осуд як міру впливу: висловлюючи свою думку про той чи інший інтернет-магазин на спеціальних сайтах, вона створює цьому магазину певну ділову репутацію. Якщо підприємець або юридична особа і далі бажає провадити успішну комерційну діяльність, то вони мають враховувати суспільну думку щодо своїх послуг. Тобто у цьому випадку мораль є більш дієвим засобом впливу.

Сучасний досвід свідчить, що непрофесіонали серед фірм, що займаються електронною комерцією, на жаль, не є рідкістю. Некомпетентність особи, що надає послуги або реалізує товари через мережу Інтернет, приводить до низької якості обслуговування клієнтів та в окремих випадках – до порушення прав споживачів. Варто зазначити, що підприємець-непрофесіонал у такому випадку не вважає, що порушує норми моралі: він діє добросовісно, проте його знань та вмінь не достатньо для належного виконання договору. Вирішувати цю проблему більш доцільно правовими засобами, через законодавчу регламентацію якості послуг електронної комерції, а також запровадження перевірок діяльності суб'єктів підприємницької діяльності, що діють через мережу Інтернет.

Проблеми комп'ютерної злочинності впродовж останніх років набирають особливої актуальності й становлять загрозу не лише окремим громадянам, фірмам, а навіть державній безпеці. А.М. Куліш та В.В. Тютюнник «комп'ютерні злочини» визначають як передбачені законодавством суспільно небезпечні дії, що посягають на встановлений у суспільстві порядок інформаційних відносин, і скоєння їх відбувається з використанням електронно-обчислювальних машин, тобто комп'ютерів, систем та комп'ютерних мереж. Таким чином, об'єктом злочину зазначених правопорушень виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється за їх допомогою [6, с. 230].

Щодо ролі моральних регуляторів в комп'ютерній злочинності, то вони навряд можуть стати достатньо дієвими, щоб забезпечити зниження рівня цього виду злочинів. Досить яскравим прикладом низької ефективності моралі в регулюванні цього виду правовідносин є те, що велику кількість хакерських атак вчиняє молодь, що прагне до самоствердження. Хакер не сприймає свій вчинок як щось ганебне і дуже часто навіть вихваляється своїми діями.

Сучасний стан правовідносин дає підстави стверджувати, що цей вид злочинності прогресуватиме в майбутньому, а тому необхідно забезпечити розробку дієвого механізму правової охорони відносин у сфері інформації, який ґрунтувався би на глибинному теоретико-правовому та філософсько-правовому осмисленні відносин у сфері інформації.

Особливої уваги потребує проблема інформаційної безпеки, яка гостро постала на початку третього тисячоліття. Якщо у минулому захист від інформаційних атак був досить простим завданням, то з поширенням мережі Інтернет дедалі складніше забезпечити інформаційну безпеку як суспільства, так і окремого індивіда. Особливо актуальною ця проблема є зараз, коли проти України робляться численні спроби інформаційних атак.

У контексті зазначеного В.О. Остроухов і В.М. Петрик зазначають, що інформаційна безпека – це стан захищеності об'єкта (особистості, суспільства, держави, інформаційно-технічної інфраструктури), за якого досягається його нормальне функціонування незалежно від внутрішніх і зовнішніх інформаційних впливів [7, с. 136]. Учені виділяють такі види загроз інформаційній безпеці: спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, комп'ютерна злочинність, інформаційна війна [7, с. 137].

Варто зауважити, що з моральної точки зору, на думку В.К. Конах та О.А.аЛазоренко, інформаційні атаки відрізняються «псевдогуманністю»: кіберзброя не спрямована безпосередньо проти людей, що спрощує моральні аспекти ухвалення рішень про її застосування, хоча вплив кібератаки на критичну інфраструктуру за наслідками може перевершити застосування зброї масового ураження [8, с. 75]. Вчені підкреслюють особливу роль моральних регуляторів у цьому питанні, вказуючи на те, що саме уявна гуманність інформаційної атаки робить її настільки поширеною зброєю в інформаційному суспільстві.

Відсутність необхідних умов і засобів, аби забезпечити захист інформації на різних рівнях, призводить до комп'ютерних злочинів та комп'ютерного тероризму. Зазвичай пріоритетними цілями кібератак є інформаційні та телекомунікаційні ресурси: органів державної влади, насамперед, вищої ланки управління, а також збройних сил і спецслужб, з метою дестабілізації соціально-політичної ситуації та погіршення керованості країною; фінансово-економічного сектора – платіжні системи, бази даних податкових і митних органів, персональних даних з метою дестабілізації економіки чи для скоєння фінансових злочинів; систем управління критично важливих галузей, насамперед енергетичної сфери, у тому числі ядерної, газотранспортної системи, хімічної промисловості з метою здійснення техногенних аварій та катастроф із суттєвими загрозами життю і здоров'ю населення та довкіллю [8, с. 75].

У таких умовах актуалізується необхідність правової охорони інформаційної безпеки. Варто зазначити, що в Україні правове регулювання інфор-

маційної сфери життя суспільства здійснюється Конституцією, а також низкою законів та підзаконних актів, зокрема Кримінальним кодексом, ЗУ «Про основи національної безпеки України», ЗУ «Про Концепцію Національної програми інформатизації», ЗУ «Про захист суспільної моралі» тощо.

Вітчизняні вчені В.С. Цимбалюк та А.В. Бабінська відзначають, що нині і на перспективу визначається нагальна потреба для суспільства, держави у фахівцях з інформаційного права. Це зумовлено посиленням негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванню суспільних цінностей і національної ідентичності [9]. Як ми бачимо, нездатність держави забезпечити достатню кількість фахівців з інформаційного права призводить до проблеми, що лежить в моральній площині.

Слушною є думка вчених, які пропонують правовими засобами забезпечити: 1) організацію підтримання режиму, охорони та захисту небажаної для суб'єкта впливу за допомогою технічних засобів. Тобто засоби протидії мають бути адекватними засобам і технологіям дії; 2) організацію протидії негативному впливу на учасників інформаційних відносин; 3) розроблення механізму, що в разі порушення функціонування інформаційної системи дасть змогу визначити майнові втрати та мінімізувати їх [10, с. 32]. Конкретні заходи, що допоможуть здійснити вищевказане, мають бути розроблені з активною участю вчених-правників і, зокрема, науковців у сфері теорії держави і права, що мають закласти теоретичний базис у ці механізми.

Досить актуальною є проблема контролю над особистим життям та відповідності поведінки індивіда в реальному та віртуальному просторах, що зачіпає як моральні, так і правові аспекти суспільного життя. У цьому контексті вважаємо за доцільне навести концепцію І.І. Припхан. Вчена слушно зауважує, що, захищаючи право приватності користувачів мережі Інтернет, у тому числі недобросовісних, держава забуває про захист суспільної моралі. У цьому контексті потрібно звернути увагу на те, що маніпулювання цінностями демократичної правової держави, зокрема, правом приватності, ставить українське суспільство у надзвичайно загрозливу ситуацію. До прикладу, кожен користувач мережі Інтернет може, не виходячи з приміщення, самовільно створити будь-який інтернет-ресурс та розмістити на ньому будь-яку інформацію. При цьому жодна перевірка персональних даних такої особи державними органами не здійснюється. Таким чином, навіть якщо дії інтернет-користувача будуть визнані злочинними, з'ясувати його особу, а тим паче притягнути його до відповідальності буде не реально [11, с. 29]. Сучасний стан інформаційної безпеки України свідчить про те, що контроль за певними інтернет-ресурсами є досить бажаним. Вкрай необхідним за таких умов є захист інтернет-користувачів від інформації, що спрямована на підрив територіальної цілісності України.

Вважаємо, що держава має створити спеціальний орган, що займався би контролем мережі Інтернет та завчасно блокував би подібну інформацію, а потім встановлював порушників. За таких умов це ускладнило би ведення інформаційної війни проти нашої держави.

Інформаційна війна – це вид протиборства між різними суб'єктами (державами, неурядовими, економічними чи іншими структурами), який здійснюється з метою досягнення односторонніх воєнних, соціально-політичних чи економічних переваг над супротивником [7, с. 137]. Складно заперечити, що з поширенням мережі Інтернет вести інформаційні війни стало простіше. Це посилює необхідність у створенні відповідного державного органу, діяльність якого концентрувалася виключно навколо захисту інформаційної безпеки України від негативних впливів через мережу Інтернет.

Наразі розробкою систем контролю комунікацій займаються такі держави, як США, Великобританія, Канада, Австралія, Нова Зеландія та Європейський Союз. Вважаємо, що Україні також варто приєднатися до таких проектів.

Підтримуємо думку тих учених, які вважають, що саме стрімкий розвиток інформаційних технологій, а також надмірно високий рівень захищеності персоніфікованих даних їхніх користувачів виступають факторами, які значною мірою зумовлюють зростання кількісного показника правопорушень у сфері захисту суспільної моралі. При цьому відсутність реального правового механізму притягнення до відповідальності за порушення норм суспільної моралі приводить до усвідомлення недобросовісними користувачами комунікацій безкарності своїх дій, створюючи у такий спосіб підґрунтя для нових протиправних посягань на моральність суспільства [11, с. 29]. Ми вбачаємо в такій ситуації замкнене коло: падіння суспільної моралі через неналежне реагування держави на подібні порушення породжує нову кількість осіб, які в майбутньому також скоюватимуть дії, спрямовані на підрив моральних засад суспільства.

Досить складну проблему для українського законодавства становить охорона прав інтелектуальної власності і, зокрема, авторського права. Незважаючи на зусилля законодавців у цьому напрямі, стан правової охорони авторського права в Україні залишається в критичному становищі. За офіційними даними Центру досліджень соціальних комунікацій, через постійне зростання піратства і недостатню увагу в боротьбі з ним з боку держави, Міжнародний альянс інтелектуальної власності, що об'єднує сім найбільших асоціацій американських виробників контенту, включив Україну в список особливої уваги. Середній рівень піратства у світі становить 42 %, і тільки за 2010 р. воно нанесло збитків на 59 млрд дол. Головна проблема, як зазначається в дослідженні Альянсу ділового програмного забезпечення Business Software Alliance (BSA), у країнах, що розвиваються, де жителі не бачать різниці між ліцензійними та неліцензійними продуктами. Для порівняння, рівень піратства у Китаї становить 71%, у Росії – 65%, у Польщі – 54%, в Угорщині – 41%.

Рівень комп'ютерного піратства в Україні становить 86% [12].

Подібний стан речей зумовлений не тільки прогалинами в законодавстві, але й моральними чинниками. Піратство не набуло б такого поширення в мережі Інтернет, якби споживачі відмовлялися б від контрафактної продукції. Так, якщо більшість людей вважає викрадення майна аморальним вчинком, то мало хто усвідомлює, що інтернет-піратство за своєю суттю мало чим відрізняється від звичайної крадіжки. У контексті зазначеного, разом із удосконаленням правових регуляторів авторських прав варто провадити серед населення заходи, спрямовані на роз'яснення того факту, що піратство суперечить моральним засадам людства та засуджується суспільством в більшості розвинутих країн.

Висновки. Зазначене вище дає підстави зробити такі висновки. В умовах інформаційного суспільства зростає роль як правових, так і моральних регуляторів. В Україні склалася критична ситуація, за якої падіння суспільної моралі через неналежне реагування держави на порушення в інформаційній сфері породжує нову кількість осіб, які в майбутньому також скоюватимуть дії, спрямовані на підрив моральних засад суспільства. Саме тому необхідно спрямувати зусилля держави на вдосконалення правових регуляторів одночасно з провадженням певних заходів з підвищення суспільної моралі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Данильян О.Г. Інформаційне суспільство: морально-етичний дискурс / О.Г. Данильян, О.П. Дзьобань // Інформація і право. – 2014. – № 1(10). – С. 16–25.
2. Ховрак І.В. Електронна комерція в Україні: переваги та недоліки / І.В.аХоврак // Економіка. Фінанси. Право. – 2013. – №. 4. – С. 16–20.
3. Тардаскіна Т.М. Електронна комерція : [навч. посіб.] / Т.М. Тардаскіна, Є.М. Стрельчук, Ю.В. Терешко. – Одеса : ОНАЗ ім. О.С. Попова. – 2011. – 244 с.
4. Карасюк В.В. Електронна комерція: проблеми правового забезпечення безпеки транзакцій / В.В. Карасюк, М.А. Судейко // Правова інформатика. – 2009. – №. 2(22). – С. 58–68.
5. Шапочка С.В. Кримінологічна характеристика шахрайства, що вчиняється з використанням комп'ютерних мереж / С.В. Шапочка // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2011. – №. 25–26. – С. 329–336.
6. Куліш, А.М. Комп'ютерна злочинність: нормативно-правове врегулювання / А.М. Куліш, В.В. Тютюнник // Сучасні інформаційні системи і технології : матеріали Першої міжнародної науково-практичної конференції, м. Суми (15–18 травня 2012 р.) / ред. кол.: А.С. Довбиш, О.А. Борисенко, І.В. Баранова. – Суми : СумДУ, 2012. – С. 229–231.
7. Остроухов В. До проблеми забезпечення інформаційної безпеки України / В. Остроухов, В. Петрик // Політичний менеджмент. – 2008. – № 4(31). – С. 135–141.
8. Конах В.К. Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації / В.К. Конах, О.А. Лазоренко // Стратегічні пріоритети. – 2014. – №. 2. – С. 73–78.
9. Цимбалюк В.С. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики / В.С. Цимбалюк, А.В. Бабінська. – [Електронний ресурс]. – Режим доступу : http://applaw.knu.ua/index.php/holovna/item/284-pravove-rehulyuvannya-informatsiynoyi-bezpeky-v-ukrayini-problemy-teoriyi-ta-praktyky-tsymbaliuk-v-s-babynska-a-v.
10. Цимбалюк В.С. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2004. – №. 8. – С. 30–33.
11. Припхан І.І. Право на приватність персоніфікованої інформації та захист суспільної моралі / І.І. Припхан // Університетські наукові записки. – 2010. – №. 1. – С. 26–31.
12. Беззуб І. Боротьба з інтернет-піратством в Україні: оцінки експертів / І.аБеззуб. – [Електронний ресурс]. – Режим доступу : http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=874:internet-piratstvo&catid=8&Itemid=350.