

**Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України
Відкритий міжнародний університет розвитку людини “Україна”**

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 2(21)

2017

Зареєстрований Міністерством юстиції України
(Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 20117-9917ПР від 05.07.13 р.)

**Згідно з Наказом МОН України від 11.07.16 р. № 820 (додаток 12)
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів доктора і кандидата наук у галузі юридичних наук**

м. Київ

УДК 002:340+316.4+338.46:002

Р е д а к ц і й н а к о л е г і я

ПИЛИПЧУК Володимир Григорович, доктор юридичних наук, професор, член-кореспондент
НАПрН України – *голова редакційної колегії,*
головний редактор;

БРИЖКО Валерій Михайлович, доктор філософії (Ph.D.) з юридичних наук, с.н.с.
– *зас. голови редакційної колегії,*
зас. головного редактора;

БЕБИК Валерій Михайлович, доктор політичних наук, професор – *зас. голови редакційної колегії;*
ПОПИК Володимир Іванович, доктор історичних наук, професор,
член-кореспондент НАН України – *зас. голови редакційної колегії;*

АРИСТОВА Ірина Василівна, доктор юридичних наук, професор;

БАРАНОВ Олександр Андрійович, доктор юридичних наук, с.н.с.;

БЄЛЯКОВ Костянтин Іванович, доктор юридичних наук, професор;

ДЗЬОБАНЬ Олександр Петрович, доктор філософських наук, професор;

ДОВГАНЬ Олександр Дмитрович, доктор юридичних наук, с.н.с.;

КОПАН Олексій Володимирович, доктор юридичних наук, професор;

КОРЖ Ігор Федорович, доктор юридичних наук, с.н.с.;

КУЙБИДА Василь Степанович, доктор наук з державного управління, професор;

ЛАНДЕ Дмитро Володимирович, доктор технічних наук, с.н.с.,

МАРУЩАК Анатолій Іванович, доктор юридичних наук, професор;

НАСТЮК Василь Якович, доктор юридичних наук, професор,
член-кореспондент НАПрН України;

НОР Василь Тимофійович, доктор юридичних наук, професор,
академік НАПрН України;

ОНИЩЕНКО Олексій Семенович, доктор філософських наук, професор,
академік НАН України;

ПЕТРИШИН Олександр Віталійович, доктор юридичних наук, професор,
академік НАПрН України;

ПОКУТНИЙ Сергій Іванович, доктор фізико-математичних наук, професор;

САВІНОВА Наталія Андріївна, доктор юридичних наук, с.н.с.;

СКУЛИШ Євген Деонізієвич, доктор юридичних наук, професор;

ТАЛАНЧУК Петро Михайлович, доктор технічних наук, професор;

ТИХИЙ Володимир Павлович, доктор юридичних наук, професор,
академік НАПрН України;

ФУРАШЕВ Володимир Миколайович, кандидат технічних наук, доцент, с.н.с.;

ШЕМШУЧЕНКО Юрій Сергійович, доктор юридичних наук, професор,
академік НАН України.

* * * * *

З М І С Т

Інформаційне право

ДЗЬОБАНЬ О.П., ЯРОЦЬКИЙ В.Л. Герменевтичний метод у сучасних цивілістичних дослідженнях: до питання про доцільність застосування.....	5
КРАВЧЕНКО О.М. Вдосконалення законодавства України щодо комерційної таємниці суб'єктів господарювання.....	13
ДУБНЯК М.В. Система основних термінів, як основа вдосконалення законодавства у сфері правового регулювання інформаційної взаємодії у місцевому самоврядуванні.....	20
НИКОЛАСНКО Г.В. Теоретичні засади правового регулювання державної статистики в Україні.....	34

Правова інформатика

БАРАНОВ О.А. Інтернет речей (ІоТ): правові моделі використання обмеженого радіочастотного ресурсу (Частина І).....	41
ДОРОНІН І.М. Використання сучасних технологій розподіленої обробки даних: право та функції держави.....	51
ТАРАСЮК А.В. Відкриті дані та інші дані у публічному доступі: правові аспекти...	59
ЛАНДЕ Д.В., ФУРАШЕВ В.Н. Термінологічна мережева модель як відображення процесів денцентралізації влади в Україні.....	66
ДОРОГИХ С.О. Модель Національної системи правової інформації в Україні.....	72

Інформаційна і національна безпека

СКУЛИШ Є.Д., ІРХА Ю.Б. Взаємозв'язок корупції та екстремізму: проблеми протидії.....	77
РАДЗІЄВСЬКА О.Г. Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей.....	88
ГУЦАЛЮК М.В. Вдосконалення чинного законодавства з питань протидії кіберзлочинності та забезпечення кібербезпеки.....	99
СЕРЬОГІН В.С., ЛЕОНОВ Б.Д. Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов'язаних з неправомірним дистанційним доступом до комп'ютерної інформації.....	108
СЕМЕНЮК О.Г. Комплексний підхід як методологічна основа дослідження проблем забезпечення охорони державної таємниці.....	116

Інформація в інших галузях права

РАДУТНИЙ О.Е. Кримінальна відповідальність штучного інтелекту..... **124**

КАТЕРИНЧУК К.В., ЮХИМЕЦЬ І.О. “Тілесні ушкодження” чи “школа здоров’ю”:
юридичний та судово-медичний погляд..... **133**

ШЕЛЯЖЕНКО Ю.В. Монополістична наукометрія з точки зору
академічної свободи та безпеки..... **144**

До відома читачів:

Рецензія на рукопис монографії кандидата юридичних наук, доцента
Гребенюка М.В. “Концептуальні засади забезпечення світової
продовольчої безпеки: теорія і практика”..... **154**

До відома авторів **158**

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.
Грамотичне коректування – Майстренко І.А. (укр., англ.).
Формат 70 x 108/16. Спосіб друку – різнографія. Ум. друк. арк. 14.0. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ “ПанТот” – Свідоцтво про внесення до
Державного реєстру видавничої продукції: Серія ДК № 2667 від 25.10.06 р.

Рекомендовано до друку Вченою радою НДІ інформатики і права
Національної академії правових наук України, протокол № 4 від 30.06.17 р.

Інформаційне право

УДК 340.115.3

ДЗЬОБАНЬ О.П., доктор філософських наук, професор,
головний науковий співробітник НДІ інформатики і права
Національної академії правових наук України
ЯРОЦЬКИЙ В.Л., доктор юридичних наук, професор,
завідувач кафедри цивільного права № 2
Національного юридичного університету ім. Ярослава Мудрого

ГЕРМЕНЕВТИЧНИЙ МЕТОД У СУЧАСНИХ ЦИВІЛІСТИЧНИХ ДОСЛІДЖЕННЯХ: ДО ПИТАННЯ ПРО ДОЦІЛЬНІСТЬ ЗАСТОСУВАННЯ

***Анотація.** Показано, що застосування герменевтичного підходу до дослідження цивільно-правової реальності дозволяє виявити системні проблеми в організації правової роботи окремих суб'єктів цивільних правовідносин, дати пропозиції щодо її вдосконалення і намітити шляхи досягнення поставлених завдань більш ефективними прийомами. Продемонстровано, що евристичний потенціал цього методу для здійснення досліджень у цивілістиці полягає в отриманні відомостей про смисл тексту, закладений у нього автором, і про те, для чого цей текст може бути використаний.*

***Ключові слова:** методи правового дослідження, юридичний текст, герменевтика, інтерпретація.*

***Аннотация.** Показано, что применение герменевтического подхода к исследованию гражданско-правовой реальности позволяет выявить системные проблемы в организации правовой работы отдельных субъектов гражданских правоотношений, дать предложения по ее совершенствованию и наметить пути достижения поставленных задач более эффективными приемами. Продемонстрировано, что эвристический потенциал этого метода для осуществления исследований в цивилистике заключается в получении сведений о смысле текста, заложенном в него автором, и о том, для чего этот текст может быть использован.*

***Ключевые слова:** методы правового исследования, юридический текст, герменевтика, интерпретация.*

***Summary.** It is shown that application of the hermeneutic approach to the study of the civil legal reality allows to identify systemic problems in the organization of legal work of individual subjects of civil relations, give suggestions for its improvement and to identify ways to achieve goals more effectively. It is demonstrated that the heuristic potential of this method for the implementation of research in civil law is to obtain information about the meaning of the text given by the author, and about why this text can be used.*

***Keywords:** methods of legal research, legal text, hermeneutics, interpretation.*

Постановка проблеми. Юридична методологія відіграє важливу роль у забезпеченні всеосяжного вивчення цивільно-правової матерії, адже застосування усієї доступної палітри апробованих у юриспруденції методів забезпечує найбільш якісне вивчення кожного окремого напрямку поставленої правником проблематики. Очевидно, що врахування на законодавчому рівні обґрунтованих цивільно-правовою наукою висновків та рекомендацій, у свою чергу, уможливорює подальше вдосконалення відповідних сегментів вітчизняного механізму цивільно-правового регулювання. Адже

його регулятивний вплив на особисті немайнові та майнові відносини повинен забезпечувати безперешкодність здійснення суб'єктивних прав управненими особами, належність виконання суб'єктивних обов'язків зобов'язаними особами, гармонізацію соціального середовища у сфері їх взаємодії і зміцнення взаємної довіри та співробітництва між ними.

Характерне для цивілістичних досліджень глибоке проникнення в сутність явищ, що підлягають вивченню, детермінує планомірне ускладнення пізнавального процесу, що вимагає посилення та урізноманітнення методологічного потенціалу на різних стадіях перманентного процесу пізнання. Пошук ефективних засобів, прийомів, способів пізнання явищ правової дійсності, що входять у предметну сферу цивілістики, викликає необхідність постійно вдосконалювати напрямки та методiku їх використання, не забуваючи при цьому про необхідність забезпечення об'єктивності і плюралізму науково-правової творчості.

Результати аналізу наукових публікацій. Гносеологічний огляд останніх доступних цивілістичних досліджень свідчить про те, що отримання правниками сучасності найбільш важливих результатів значною мірою обумовлене правильним вибором методологічно вивірених шляхів, які полегшили пошук істини і дозволили сформулювати обґрунтовані судження, висновки та пропозиції. Разом з тим, наявний арсенал цивільно-правових досліджень повинен постійно поповнюватись новими теоретичними даними, що вирізняються високим ступенем осмислення й кореляції з усталеними цивілістичними постулатами та вивіреними підходами загальної (інструментальної) теорії права.

Дотримання цієї умови, з урахуванням сучасного рівня розвитку цивілістики, повинно сприйматися як конкретний деонтологічний орієнтир, що дозволить в необхідних випадках виходити за межі юридичного позитивізму, який протягом тривалого часу стереотипізував основні напрямки цивілістичного праворозуміння і формував тенденційні дослідницькі установки та методологічний інструментарій, які задають вектор і визначають динаміку подальшого розвитку цивілістики.

Незважаючи на це, методологічний інструментарій пізнання правових явищ в сучасних умовах постійно вдосконалюється, зазнаючи кількісної та якісної трансформації. В цьому виявляється діалектична закономірність взаємозв'язку інтенсифікації та редукції проявів тенденції до пом'якшення догматичних підходів до розуміння сутності досліджуваних цивільно-правових феноменів.

Метою статті є спроба обґрунтування методологічної доцільності застосування герменевтики до наукових досліджень у юридичній науці.

Виклад основного матеріалу. Сучасна система методів наукового пізнання, які використовуються у дослідженнях правової реальності, відзначається високою складністю й диференційованістю.

Методи правового дослідження, як відомо, – це система розумових і/або практичних операцій, принципів, прийомів і правил, які націлені на вирішення певних пізнавальних завдань у сфері права з урахуванням певної пізнавальної мети, яка зумовлена духовними й матеріальними потребами суспільства і/або внутрішніми потребами самої правової науки.

Зазвичай методи правового дослідження включають в себе: сформульовану мету; описання об'єктивної ситуації, в межах якої вирішується практичне або теоретичне завдання; процедуру або перелік операцій, які необхідно здійснити для досягнення мети в заданих умовах.

Сучасна методологічна наука висуває до методів правового дослідження наступні вимоги: об'єктивність, відповідність методу об'єкта дослідження й рівню наукового пізнання; зрозумілість та загальнодоступність; детермінованість та відсутність стихійності і свавілля у застосуванні; здатність забезпечувати досягнення мети; здатність забезпечувати не тільки заплановані, але й не менш значущі побічні результати; надійність (здатність з високим ступенем достовірності забезпечувати бажаний результат); економічність (здатність давати результат з найменшими витратами коштів і часу) [1, с. 456].

Разом з тим, доводиться констатувати, що методологія сучасної цивілістики спирається на розроблену ще в радянські роки для всіх юридичних наук систему прийомів і способів здійснення наукового пізнання. Саме тоді були проведені фундаментальні дослідження основних категорій юридичної науки взагалі й цивілістики, зокрема, визначені базові підходи до вирішення основних наукових проблем. Дослідження сфери цивільно-правового регулювання з використанням розробленої юриспруденцією традиційної методології та апробованого набору методів не забезпечує необхідного рівня повноти наукового пошуку. Адже сфера приватно-правового ускладнюється наявністю значного масиву позанормативних регуляторів (звичаїв, односторонніх правочинів, договорів, статутів та інших локальних актів юридичних осіб тощо). Здійснення цивілістичних досліджень без застосування додаткових методів не дозволяє скласти достовірне уявлення про процеси й закономірності, що відбуваються в приватноправовій царині, і, як наслідок, не може дати повноцінний науковий результат, що задовольняє нагальні потреби законодавця, правозастосовчої практики та суб'єктів правореалізації.

Від застосовуваних методів дослідження в їх взаємодоповнюваності залежить якість одержуваного наукового результату, його достовірність і корисність для вирішення практичних завдань. Тому, сучасна розробка й уточнення цивілістичної методології – найважливіше наукове завдання, вирішення якого дозволяє отримувати якісно нові наукові результати в ході пізнання. Крім того, без фундаментальної наукової основи цивільно-правове регулювання ризикує набути значення безсистемного впливу на суспільні відносини, що формується під впливом випадкових, необґрунтованих наукою чинників, а тому може мати непередбачувані негативні наслідки [2 – 3]. Незважаючи на це, сама наука цивільного права, її предмет, методологія, структура наразі залишається без достатнього фахового наукового осмислення. Зазначене актуалізує спеціальні дослідження методології цивілістики на філософському й загальнонауковому рівнях.

Як відомо, будь-яке наукове дослідження починається з постановки наукової проблеми, визначення об'єкта і предмета дослідження й підбору адекватного обраному предмету набору дослідницьких методів [4 – 6].

Розглядаючи коло можливих методів дослідження поставленої проблеми, в теорії права використовують категорію “методологічна розкутість”. Вказане термінологічне словосполучення позначає одночасне можливе існування безлічі підходів до постановки наукової проблеми та обрання методології наукового пізнання. Евристичні можливості того чи іншого з цих підходів, їх порівняльний аналіз і критичне осмислення є предметом наукової дискусії [7].

Систематика цивілістичної науки за рівнями пізнання аналогічна за складом будь-якій науковій сфері. Дослідження у галузевих юридичних науках взагалі й цивілістиці, зокрема, можуть здійснюватися у кількох взаємопов'язаних, але все ж окремих напрямках – догматичному, соціологічному та аксіологічному. У межах даної статті

сконцентруємося на догматичному напрямку цивілістичних досліджень, для якого предметом аналізу є, перш за все, юридичні тексти, що використовуються у сфері дії механізму цивільно-правового регулювання. Юридичні тексти, що потрапляють у предметну царину науки цивільного права, є неоднорідними за своєю природою і формальним вираженням. До складу приватноправових текстів включаються не тільки акти зовнішнього (нормативного) регулювання, а й акти саморегулювання. Приватноправові тексти можуть міститися в нормативно-правових актах, правових звичаях, договорах, односторонніх правочинах, статутах, регламентах, положеннях та інших внутрішніх документах юридичних осіб тощо. Нормативно-правові акти є джерелом цивільного права, містять норми права, які виходять від держави, і завжди закріплені в письмовій формі. Правові звичаї також є джерелами права, проте не виходять від держави, а формуються суб'єктами права шляхом систематичного повторення і можуть виражатися не лише у формі письмового тексту, але й в усній формі і у формі поведінкових актів. Регламенти та інші внутрішні документи організації містять формально-визначені правила поведінки, що не наділені, однак, властивістю загальнообов'язковості, і можуть бути зафіксовані тільки в письмовій формі. Договори, що не містять норм права, можуть виражатися як у письмовій, так і в усній формі, або у формі поведінкових актів. Усі ці юридичні тексти вимагають вивчення, і на його основі побудови несуперечливих наукових висновків. Специфіка юридичних текстів, що потрапляють у предметну сферу науки цивільного права, безсумнівно, вимагає розробки науково-обґрунтованої методики їх дослідження.

У догматичну частину дослідження включаються приписи, що містяться у будь-яких джерелах регулювання діяльності суб'єктів, незалежно від суб'єкта, від якого така форма виходить – держави, суспільства, суб'єктів правореалізаційної діяльності тощо.

Основним методом наукових досліджень у цій царині є правова герменевтика – метод наукового дослідження, призначений для виявлення смислу юридичного тексту, виходячи з його об'єктивних (значення слів та їх історично обумовлені варіації) і суб'єктивних (наміри автора) підстав, інтерпретації та роз'яснення змісту юридичного тексту, зафіксованого в документі.

Можна виділити три основні завдання дослідження юридичних текстів, які вирішуються за допомогою правової герменевтики: виявлення смислу; роз'яснення змісту; інтерпретація змісту, виходячи із завдань, що вирішуються за допомогою юридичного тексту.

Юридичні тексти як предмет герменевтичного аналізу існують у вигляді нормативно-правових актів, актів судових органів, договорів, односторонніх правочинів, статутів, регламентів, положень, інших внутрішніх документів організацій тощо. Застосування стосовно вказаних текстів даного методу пов'язане зі складнощами, пов'язаними у свою чергу з виявленням тексту, що піддається подальшому дослідженню.

Необхідність застосування герменевтики виникає там, де “слово усвідомлюється як знак, що використовується для передачі повідомлення, де постає проблема розуміння таких знаків” [8, с. 16]. Розробку герменевтики як напряму філософії пов'язують з роботами німецького філософа, теолога й проповідника Фрідріха Шлейєрмахера, який описав мистецтво розуміння, а не лише тлумачення тексту, і назвав його герменевтикою. За Шлейєрмахером, наукова герменевтика повинна бути мистецтвом розуміння чужої мови і правильного повідомлення іншим думок інтерпретатора про її зміст. Тут простежується важливий момент діалогу між автором тексту і інтерпретатором, незважаючи на “застиглий” характер мови автора. Стосовно правової

герменевтики у цьому проявляється одна з основних проблем інтерпретації – накладення на розуміння сенсу досліджуваного юридичного тексту правосвідомості і правової культури інтерпретатора.

Основна мета методу герменевтики – зрозуміти автора і його працю краще, ніж він сам розумів себе і своє творіння [9 – 11]. Цей напрямок герменевтики називають “романтичною герменевтикою”. Саме такий підхід набув поширення у правовій герменевтиці – він дозволяє тлумачеві виходити за межі буквального розуміння тексту.

Розвиток уявлень про завдання тлумачення нормативно-правових актів (ця частина правової герменевтики традиційно розвивається інтенсивніше, ніж інші) призвело до практично однозначного переконання в тому, що у правовій герменевтиці основне завдання – за допомогою тлумачення якомога більш повно пристосувати юридичний текст до реалій, з принциповим збереженням основної його ідеї – смислу. Але, все ж пам’ятаючи, що юридичний документ складається заради фіксації тих соціальних зв’язків, на які він повинен впливати, саме їм він повинен бути в першу чергу адекватний. Як ілюстрацію сказаного згадаємо Цивільний кодекс Наполеона, складений в очевидно іншу історичну епоху. Це стало можливим завдяки правильній інтерпретації, з використанням усього багатства наявного в ті часи герменевтичного інструментарію. Те саме можна виявити і в тлумаченнях норм Цивільного кодексу України вищими судовими інстанціями, коли правові позиції щодо одного й того ж тексту з плином часу кардинально змінювалися.

Прийоми романтичної герменевтики поширюються на правову герменевтику. Основними її ідеями є діалектика частини й цілого, попереднє розуміння і герменевтичне коло. Суть полягає у послідовному вивченні тексту – спочатку як цілого, що складається з окремих фрагментів – частин, а потім самого тексту – як частини, де цілим є весь соціокультурний простір, у якому даний текст створений. Герменевтика пропонує послідовний перехід від одного рівня дослідження до іншого і назад, з уточненням отриманих висновків. На кожному такому поверненні, як стверджує Г. Гадамер, відбувається попереднє розуміння тексту, і “вихід” з цього кругового ходіння може бути тільки після повного дешифрування сенсу тексту [12, с. 72-91].

Стосовно екстраполяції цих прийомів на предмет догматичної частини цивілістики – юридичний текст, що міститься в статутах, внутрішніх документах організацій, договорах та ін., це означає необхідність з’ясування його структури і зв’язків кожного його фрагмента з загальним масивом, і зіставлення всього тексту з тим оточенням, в якому він складався і на яке повинен був впливати.

Для цивільно-правового дослідження характерним є розширення кола юридичних текстів, що підлягають аналізу. До них відносяться не тільки нормативно-правові акти, складені з широким застосуванням науково-обґрунтованих прийомів юридичної техніки, що істотно спрощує процедуру з’ясування їхнього змісту. Сюди відносяться і юридичні тексти, складені без використання спеціальних прийомів найчастіше особами, які не мають навичок ведення договірної та іншої правової роботи. При складанні таких текстів в основному використовується повсякденна мова, що викликає пов’язані з цією обставиною проблеми інтерпретації.

Герменевтичний аналіз є методом дослідження, в ході якого емпіричний матеріал збирається й фіксується. Від належності засобів фіксації матеріалу залежить правильність виявлення його сенсу з позицій герменевтики. Зауважимо, що основний творчий науковий потенціал цивільно-правового дослідження значною мірою залежить від правильності застосування прийомів герменевтики, в межах яких відбувається початкове осмислення текстів, отриманих на першому етапі донаукового дослідження

(спостереження, збору емпіричного матеріалу тощо). Висновки, отримані в ході подальшого втілення програми герменевтичного аналізу, в подальшому потребують осмислення з урахуванням наукових результатів, отриманих на інших рівнях наукового дослідження (соціологічному й аксіологічному).

В даний час, незважаючи на досить розроблену методіку тлумачення нормативно-правових актів на рівні інструментальної теорії права і наявність наукових робіт, присвячених способам тлумачення договорів, механізм виявлення сенсу інших різновидів приватно-правових текстів достатньою мірою не розроблений. Разом з тим, саме інші тексти потрапляють у сферу галузевих правових досліджень найбільш часто. Так, на сьогодні відсутня методика інтерпретації положень актів саморегулювання (статутів, регламентів, положень та інших внутрішніх документів юридичних осіб). Відносно правових звичаїв, що застосовуються у механізмі цивільно-правового регулювання, не розроблена навіть науково обґрунтована методика їх виявлення та фіксації.

На нашу думку, доцільно взяти за основу алгоритм проведення герменевтично-правового вивчення текстів, що становлять предмет догматичної частини цивілістичного дослідження, запропонований С. Філіпповою [13, с. 34-35]. Дослідниця пропонує наступну послідовність дослідницьких процедур:

1) виявлення юридичного тексту, що підлягає вивченню і його фіксація. Для письмових документів цей етап дослідження спеціально може і не фіксуватися, але для усних текстів і текстів, які висловлюються в поведінкових актах, виявлення тексту вимагає спеціальної дослідницької роботи;

2) попереднє розуміння юридичного тексту з використанням граматичного аналізу: зміст юридичного тексту “схоплюється” в першому наближенні;

3) зіставлення юридичного тексту з системою юридичних текстів, в які він включений;

4) повернення у попереднє розуміння юридичного тексту з урахуванням виявлених зв’язків з іншими документами, причин створення даного юридичного тексту;

5) вивчення соціокультурної ситуації створення документа. На цьому етапі герменевтичне дослідження пов’язане з соціологічним рівнем вивчення ситуації. Відносно нормативного правового акта це робиться шляхом вивчення пакету законодавчої ініціативи, громадських обговорень законопроектів (проектів інших нормативно-правових актів), усталеної судової та адміністративної практики. Для інших юридичних документів приватно-правової сфери ситуація ускладнюється значною мірою закритим характером інформації про створення юридичного документа. Можна спиратися на повідомлення у ЗМІ, листування сторін, що не має правового характеру, їх повідомлення про ситуацію, що передусє складанню юридичного документа та ін., проте слід пам’ятати про можливість недостовірності таких відомостей;

6) коригування розуміння юридичного тексту з урахуванням виявлених закономірностей і зв’язків. На даному етапі завдання з’ясування змісту юридичного тексту повинне бути виконане. Такий результат носить характер припущення, за зауваженням Г. Гадамера, “хто хоче зрозуміти текст, той завжди робить припущення. Він передбачає смисл цілого, який здається йому першим змістом у тексті. Так виходить тому, що текст читають вже зі значним очікуванням певного сенсу” [14, с. 252];

7) виявлення завдань, які повинні вирішуватися за допомогою аналізованого документа. Юридична герменевтика спрямована не тільки на розуміння юридичного тексту, а й на його інтерпретацію, виходячи з тих потреб, які з його допомогою повинні задовольнятися на момент інтерпретації. Життя, відносини, регламентовані юридичним

текстом, є рухливими і не можуть зберігати, на відміну від тексту, застиглу форму. Через певний час, після неминучої зміни потреб суб'єктів, зафіксований текст виявляється неактуальним. Необхідність актуалізації змісту тексту, “підведення” його під існуючі на момент інтерпретації потреби призводить до необхідності телеологічної інтерпретації. У такому випадку важливо відчувати грань між розумінням тексту і свавіллям інтерпретатора. Мірилом правильного розуміння сенсу тексту є збереження мети його створення і його застосування. На цьому етапі герменевтичне дослідження перетинається з аксіологічним, у ході якого виявляються цілі створення і застосування юридичного тексту. Тобто, правильною інтерпретацією тексту є така, в якій незалежно від надання того чи іншого сенсу словам або вираженням, використаним у тексті, основна ідея тексту, закладена в нього мета залишаються незмінною;

8) роз'яснення смислу тексту – заключний етап герменевтичного тлумачення, що вимагає фіксації отриманих результатів у вигляді роз'яснення.

Як можна помітити, догматичне дослідження не може існувати ізольовано, в нього включаються висновки, одержувані при вивченні соціальної взаємодії суб'єктів (соціологічний рівень) і цілі регулювання (аксіологічний рівень). В ізоляції від цих результатів дослідження результат герменевтичного дослідження виявиться недостовірним. У цьому, як зазначалося у попередніх авторських публікаціях, проявляється єдність рівнів наукового пізнання, які в сукупності складають єдину цивілістичну науку [15].

Висновки.

Підводячи підсумки дослідження специфіки методології дослідження проблем цивілістики, зазначимо наступне.

В ідеалі, сучасні дослідження у цивілістиці повинні ґрунтуватись на трьох можливих рівнях наукового пізнання. Проаналізований у цій статті перший рівень (догматичний) полягає у дослідженні норм позитивного права, що містяться в актах цивільного законодавства України, приписів, що складають зміст правових звичаїв й інших джерел цивільного права, а також положень договорів, статутів, регламентів та інших внутрішніх документів юридичної особи. Їх всебічне вивчення здійснюється за допомогою методів правової герменевтики з урахуванням актуальних потреб в регулюванні і волі, вираженої в правовій нормі.

Застосування герменевтичного методу до дослідження цивільно-правової реальності дозволяє виявити системні проблеми в організації правової роботи окремих суб'єктів цивільних правовідносин, дати пропозиції щодо її вдосконалення і намітити шляхи досягнення поставленого завдання більш ефективними прийомами.

Евристичний потенціал цього методу для здійснення досліджень у цивілістиці полягає в отриманні відомостей про смисл тексту, закладений у нього автором, і про те, для чого цей текст може бути використаний. У науковому дослідженні такий результат повинен бути проміжним, давати підставу для роздумів вченого про правові явища і служити приводом для виявлення проблем в адекватності викладу фактичних обставин.

Таким чином, герменевтичний метод можна віднести до методів збору матеріалу для подальшого вивчення за допомогою інших наукових методів, а тому єдиним методом наукового дослідження він не є.

Використана література

1. Данильян О.Г. Методи правового дослідження / О.Г. Данильян, О.П. Дзьобань / Велика українська юридична енциклопедія : у 20 т. – Т. 2 : Філософія права ; редкол. С.І. Максимов (голова) та ін. – Х. : Право, 2017. – С. 456-459.

2. Суспільство, людина, право : сучасні дослідження актуальних проблем: монографія / [О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.] ; за ред. О.Г. Данильяна. – Х. : Право, 2014. – 392 с.
3. Сучасне суспільство : філософсько-правове дослідження актуальних проблем : монографія / [О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.] ; за ред. О.Г. Данильяна. – Х. : Право, 2016. – 488 с.
4. Методологія сучасних досліджень в політиці, економіці та соціальній сфері : матеріали Першої міжнародної науково-практичної конференції, (Донецьк, 12 квітня 2011 р.) / Донец. Інститут міжрегіон. акад. упр. персоналом [та ін.]. – Донецьк : Норд-Прес, 2011. – 472 с.
5. Остапчук М.В. Методологія та організація наукових досліджень : підручник / М.В. Остапчук, А.І. Рибак, О.С. Ванюшкін. – Одеса : Фенікс, 2014. – 375 с.
6. Малигіна В.Д. Методологія наукових досліджень : монографія / В.Д. Малигіна, О.Ю. Холодова, Л.М. Акімова. – Рівне : НУВГП, 2016. – 247 с.
7. Сырых В.М. Неоплатные долги позитивистской доктрины права / В.М. Сырых / Коммуникативная теория права и современные проблемы юриспруденции. – Т. 1. ; под ред. М.В. Антонова, И.Л. Честнова. – СПб., 2014. – С. 127-144.
8. Кузнецов В.Г. Герменевтика и гуманитарное познание / В.Г. Кузнецов. – М. : Изд-во МГУ, 1991. – 191 с.
9. Юркевич О.М. Герменевтика культурної форми розуміння : автореф. дис. на здобуття наук. ступеня д-ра філос. наук : 09.00.01 / О.М. Юркевич. – Х., 2005. – 40 с.
10. Попова Н.В. Герменевтичні практики і проблема їх філософського осмислення : автореф. дис. на здобуття наук. ступеня канд. філос. наук : 09.00.04 / Н.В. Попова. – Х., 2001. – 20 с.
11. Блуд О.О. Мова як трансценденція : автореф. дис. на здобуття наук. ступеня канд. філос. наук : 09.00.01 / О.О. Блуд. – К., 2007. – 18 с.
12. Гадамер Г.Г. Актуальность прекрасного / Г.Г. Гадамер [пер. с англ.] ; послесл. В.С. Малахова ; коммент. В.С. Малахова, В.В. Бибикина. – М. : Искусство, 1991. – 366 с.
13. Филиппова С.Ю. Инструментальная методология цивилистического исследования: дис. на здобуття наук. ступеня д-ра юрид. наук : 12.00.03 / С.Ю. Филиппова. – М., 2016. – 481 с.
14. Гадамер Г.Г. Истина и метод: основы философской герменевтики / Г.Г. Гадамер ; [пер. с нем.] ; общ. ред. и вступ. ст. Б.Н. Бессонова. – М. : Прогресс, 1988. – 699 с.
15. Дзедань А.П. Общеметодологические и эвристические аспекты современных цивилистических исследований / А.П. Дзедань, В.Л. Яроцкий / Методология исследования проблем цивилистики : сб. ст. посвящ. памяти проф. А.А. Пушкина ; под ред. Ю.М. Жорнокуя и С.А. Слипченко. – Х. : Право, 2017. – С. 176-205.

~~~~~ \* \* \* ~~~~~

УДК 340.11:347.7

**КРАВЧЕНКО О.**, аспірант, Академія праці, соціальних відносин і туризму,  
кафедра конституційного, адміністративного та господарського права

## **ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА УКРАЇНИ ЩОДО КОМЕРЦІЙНОЇ ТАЄМНИЦІ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ**

***Анотація*** У статті досліджено актуальні проблеми охорони комерційної таємниці суб'єктів господарювання в Україні. Визначено напрями вдосконалення законодавства України в сфері охорони комерційної таємниці шляхом прийняття Закону “Про комерційну таємницю”.

***Ключові слова:*** інформація з обмеженим доступом, комерційна таємниця, охорона комерційної таємниці, право інтелектуальної власності, конфіденційна інформація, суб'єкт господарювання.

***Аннотация.*** В статье исследованы актуальные проблемы охраны коммерческой тайны субъектов хозяйствования в Украине. Определены направления совершенствования законодательства Украины в сфере охраны коммерческой тайн путем принятия Закона “О коммерческой тайне”.

***Ключевые слова:*** информация с ограниченным доступом, коммерческая тайна, охрана коммерческой тайны, право интеллектуальной собственности, конфиденциальная информация, субъект хозяйствования.

***Summary.*** The article examines the topical problems of protection of trade secrets of economic entities in Ukraine. The ways of improving the legislation of Ukraine in the sphere of trade secrets by adopting of the Law of Ukraine “On Trade Secrets” are defined.

***Keywords:*** classified information, trade secrets, the protection of trade secrets, intellectual property rights, confidential information, economic entity.

**Постановка проблеми.** У більшості пострадянських держав ухвалено законодавство про комерційну таємницю. В Україні таке регулювання відсутнє, хоча й були розроблені проекти законів щодо охорони комерційної таємниці, але вони не знайшли підтримки. Чинне законодавство встановлює тільки загальні правила у сфері виявлення, збору, аналізу та передачі інформації, яка зазначена як комерційна, відтак питання унормування цієї сфери правових відносин залишаються актуальними.

Прийняття Закону України “Про комерційну таємницю” потрібне в першу чергу комерційним підприємствам, установам та організаціям, яким потрібно надійно захистити комерційну таємницю від конкурентів. В тому числі і від правоохоронних органів, які мають доступ до комерційної таємниці суб'єктів господарювання, але для яких не встановлено відповідальності за розголошення цих відомостей, як наприклад це передбачено в Законі України “Про банки і банківську діяльність”.

Актуальність наукової статті підвищується в зв'язку з перспективами вступу України до Європейського Союзу, що висуває необхідність виконання вимог Угоди про комерційне використання інтелектуальної власності TRIPS [1], зокрема, що стосується захисту комерційної таємниці. Тому, щоб врегулювати всі проблемні питання захисту комерційної таємниці суб'єктів господарювання, і потрібне прийняття Закону України “Про комерційну таємницю”.

**Результати аналізу наукових публікацій.** В основу наукової статті покладено аналіз міжнародних нормативно-правових актів, а також законодавства України з питань комерційної таємниці, та погляди на цю проблематику науковців. А саме, різним аспектам проблематики захисту комерційної таємниці в дослідженнях приділяють увагу такі фахівці, як А. Марущак, Г. Андрощук, П. Крайньов, Д. Задихайло, В. Пашков, А. Олефір, Б. Лундвалл, П. Бубенко, О. Орлюк, О. Бутнік-Сіверський, О. Давидюк, М. Хавронюк. Проведений аналіз свідчить, що в Україні вирішенням проблеми пов’язаної з комерційною таємницею повинно стати прийняття Закону “Про комерційну таємницю” та приведення українського законодавства у відповідність із законодавством розвинутих країн з ринковою економікою.

**Метою статті** є визначення нормативно-правових проблем в сфері, що стосується охорони комерційної таємниці суб’єктів господарювання.

**Виклад основного матеріалу.** На рівні кодифікованих законів України визначені основні положення про комерційну таємницю, а саме: ст. 162 Господарського кодексу України [2] передбачає правомочності суб’єктів господарювання щодо комерційної таємниці, а глава 46 Цивільного кодексу України [3] встановлює право інтелектуальної власності на комерційну таємницю, зокрема, поняття комерційної таємниці, майнові права інтелектуальної власності на комерційну таємницю, охорону комерційної таємниці органами державної влади, а також строк чинності права інтелектуальної власності на комерційну таємницю.

При створенні нових технологій, що є наслідком інтелектуальної праці, виникають насичені різноманітними відомостями інформаційні об’єкти, які мають комерційну цінність, – усілякі методики, перспективні технічні рішення, результати маркетингових досліджень тощо, спрямовані на досягнення підприємницького успіху, які потребують додаткового захисту від конкурентів. Інформація є першоосновою життя сучасного суспільства, предметом і продуктом його життєдіяльності, а процес її створення, накопичення, зберігання, передавання та обробки стимулює прогрес у сфері знярядь її виробництва, – електронно-обчислювальної техніки, засобів телекомунікації та системи зв’язку. Однак комп’ютерні технології – не єдина загроза комерційній таємниці. Комерційна таємниця як об’єкт інтелектуальної власності має певні особливості, зокрема, – це її універсальність серед інших об’єктів інтелектуальної власності, оскільки під поняття “комерційна таємниця” можна підвести найрізноманітніші відомості, пов’язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю суб’єкта господарювання. Отже, у сфері ринкової економіки інформація стає товаром, а тому її отримання, зберігання, передавання та використання мають підпорядковуватися законам товарно-грошових відносин, тобто інформація стає об’єктом та інструментом управління. Це, у свою чергу, потребує дослідження й деталізації поняття “комерційна таємниця”.

Відносини, що виникають між суб’єктами господарювання в зв’язку з наявністю і використанням комерційної таємниці, законодавчо в єдиному нормативно-правовому акті в Україні не урегульовані та теоретично мало вивчені.

Виникає необхідність у Законі “Про комерційну таємницю”, що обумовлено двома обставинами: 1) практичною потребою в регламентації певної групи суспільних відносин, що виникають у зв’язку з комерційною таємницею, які не урегульовані нормами права; 2) відсутністю законів, здатних виконати цю функцію згідно до стандартів ЄС.

А. Марущак рекомендує включати норму про нерозголошення комерційної таємниці в трудовий договір (контракт) як керівника підприємства, так й інших співробітників. Науковець зазначає, що зобов'язання про нерозголошення інформації може бути оформлене як записом безпосередньо у тексті трудового договору (контракту), так і у вигляді окремого документа, що є додатком до трудового договору (контракту) [4].

Г. Андрощук і П. Крайньов позитивно ставляться до захисту комерційної таємниці на підприємстві шляхом регулювання трудових відносин, та встановлення правил у локальних нормативних актах [5]. Науковці наголошують на важливості комплексного застосування напрацьованого арсеналу правових засобів, який дозволив би залежно від внутрішньої та зовнішньої ситуації оптимізувати управління економікою на тих засадах, що є найбільш ефективними в масштабі як усієї економіки, так і окремих її кластерів [6, с. 131-132, 136-137].

На думку В.М. Пашкова, для гарантування соціальної безпеки держава повинна постійно утримувати баланс між сферами публічного та приватного права [7, с. 86]. Захист інформації, що містить комерційну таємницю, від несанкціонованого використання має важливе правове значення: з моменту втрати конфіденційності майнові права особи на секрет виробництва припиняються.

Правова система ЄС (*acquis communautaire*) не містить окремого акту для охорони комерційної таємниці. Це пов'язано, зокрема, з відмінною від американської ідеологією ставлення до охорони об'єктів інтелектуальної власності, що виходить з пріоритетності вільної конкуренції та вільного руху товарів (робіт, послуг).

Правова система ЄС надає охорону інформації, що становить комерційну таємницю, у вигляді охорони “ноу-хау”, яка міститься в Європейській патентній конвенції. Під “ноу-хау” розуміється цілісна технічна інформація, що є секретною, зафіксованою в матеріальному об'єкті та може бути встановлена у будь-який можливий спосіб. “Секретний” означає “такий, що не є загально відомим або легко доступним”.

Патентне право ЄС створює додаткові стимули для використання режиму комерційної таємниці для охорони конфіденційної інформації. Це пов'язано з тим, що патентна охорона може бути не доступною для окремих технологій в Європі (наприклад, не підлягають патентуванню в окремих країнах методи медичного діагностування та лікування, фармацевтичні та комп'ютерні технології тощо). Навіть, якщо є можливим патентування певної технології, охорона інформації в якості комерційної таємниці може бути привабливішою. Це пов'язано з тим, що в Європі заявка на отримання патенту оприлюднюється до видачі патенту, що надає конкурентам достатньо часу, щоб скопіювати технологію. Неефективності патентної охорони також сприяють процедури обґрунтування патентної заявки, тривалий період набрання чинності патентом після його видачі, недостатній захист. На ефективність патентної охорони також впливає властиве європейським країнам право попереднього користувача, що передбачає надання третій особі, яка використовувала винахід до його патентування, права продовжувати використовувати винахід. Слід також звернути увагу на Першу Директиву Ради ЄС від 9 березня 1968 (з наступними змінами) щодо координації заходів безпеки. Статтею 2 Директиви визначається мінімальний перелік документів, які підлягають обов'язковому розкриттю (інакше кажучи, які не можна віднести до комерційної таємниці):

- установчий документ та статут, будь-які зміни, що до них вносяться;
- документи про призначення, припинення повноважень, відомості про осіб, які самостійно або в складі колективного органу є уповноваженими представляти компанію у відносинах з третіми особами, виступати від імені компанії, брати участь в управлінні, нагляді або контролі за компанією;

- принаймні щорічно суму акціонерного капіталу;
- бухгалтерську звітність за кожний фінансовий рік, яка підлягає оприлюдненню;
- відомості про зміну місця знаходження компанії;
- відомості про ліквідацію компанії, у тому числі відповідне рішення суду;
- відомості про призначення ліквідатора, інформація про останнього.

Огляд міждержавних угод, що стосуються охорони комерційної таємниці, свідчать про те, що така охорона більше не є справою виключно національного законодавства [8].

Важливою умовою інноваційного розвитку є гарантії прав приватних власників, баланс комерційних інтересів і справедливого задоволення соціальних потреб. З огляду на те, що лише патентний захист неспроможний задовольнити потреби дослідників [9, с. 79-94], окрім формальних і забезпечених публічною охороною правових засобів, на перший план виходять приватноправові, зокрема, режим охорони комерційної таємниці. Це сприяє підвищенню довіри між сторонами відносин, а отже, інтенсифікації інноваційних процесів, зменшенню часових і грошових витрат на переговори. На думку фахівців, важливим внеском в інноваційний процес є новий повсякденний досвід, діяльність менеджерів, інженерів, споживачів, окрім цього, інноваційний процес не обмежується лише сферою технологій [10]. Тому особливістю угод про передачу комерційної таємниці є те, що на компенсаційній основі передається право на використання знань і досвіду [11]. На думку І. Томберга, інформація – це 80 % інновацій [12, с. 7]. Комерційна таємниця є загальною формою правової охорони об'єктів інтелектуальної власності, поряд із патентною, реєстраційною, особливою (топології інтегральних мікросхем), авторським правом і суміжними правами. З цього погляду в Законі України “Про державне регулювання діяльності у сфері трансферу технологій” від 14 жовтня 2006 р. ноу-хау неправильно визначено як самостійний об'єкт технології, поряд із об'єктами права інтелектуальної власності. Тому не слід ототожнювати комерційну таємницю з ноу-хау або включати її до змісту останнього [13, с. 71-72].

На думку О.М. Давидюка, багатогранність природи технології, наявність двох основних форм її прояву – матеріальної та інформаційної – дозволяють зробити висновок про те, що її можна віднести як до матеріальних активів, так і до нематеріальних [14, с. 43].

Н. Хавронюк зазначає, що на конкретному підприємстві порядок отримання, використання, зберігання і поширення комерційної таємниці може бути відображений у трудових договорах або у спеціальних письмових зобов'язаннях, у правилах внутрішнього трудового розпорядку, в переліку відомостей, що становлять комерційну таємницю підприємства, в наказах про призначення осіб, відповідальних за режим комерційної таємниці, у положеннях (інструкціях) про службу безпеки підприємства, про режим доступу до інформації, що становить комерційну таємницю підприємства, про порядок реєстрації службових осіб організацій та органів, що проводять перевірку підприємства, про порядок надання державним та іншим органам за їх запитом відомостей, що становлять комерційну таємницю підприємства, тощо [15].

Як бачимо в цілому, погляди науковців на проблематику пов'язану з комерційною таємницею суб'єктів господарювання, зводяться до прийняття Закону України “Про комерційну таємницю”, де повинна бути прописана і відповідальність контролюючих органів за витік комерційної таємниці, якщо вона заподіяна з вини цих органів, як це наприклад, прописано в Законі України “Про банки і банківську діяльність”.

В Україні було три спроби прийняття Закону України “Про комерційну таємницю”.

У 2004 році народним депутатом Т. Довгим було розроблено проект Закону України “Про охорону прав на комерційну таємницю”.



В 2005 році народним депутатом А. Семиногою підготовлено проект Закону України “Про основні засади охорони комерційної таємниці в Україні”.

А у 2008 році розроблено проект Закону України “Про охорону прав на комерційну таємницю” Міністерством освіти і науки України, що схвалено розпорядженням Кабінету Міністрів України від 5 листопада 2008 р. № 1404-р.

Та попри все ці спроби були марними з різних обставин, а законопроекти повернуті на доопрацювання. Проаналізувавши ці законопроекти, можна зауважити, що на нашу думку обов’язки осіб, які мають доступ до комерційної таємниці, та відповідальність за розголошення відомостей, що становлять комерційну таємницю, юридичні та фізичні особи, в тому числі службові особи органів державної влади, включаючи службових осіб контролюючих та правоохоронних органів, а також органів місцевого самоврядування, які мають або мали доступ до комерційної таємниці суб’єктів господарювання, потрібно більш чітко визначити відповідальність цих державних органів за витік комерційної таємниці, як, наприклад, це передбачено стосовно банківської таємниці в Законі України “Про банки і банківську діяльність”. А саме, як це прописано в главі 10 Закону України “Про банки і банківську діяльність”, банківська таємниця та конфіденційність інформації, ст. 61 зобов’язання щодо збереження банківської таємниці, застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом. Органи державної влади, юридичні та фізичні особи, які при виконанні своїх функцій, визначених законом, або наданні послуг банку безпосередньо чи опосередковано отримали в установленому законом порядку інформацію, що містить банківську таємницю, зобов’язані забезпечити збереження такої інформації, не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб. У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами. Тому в Законі України “Про комерційну таємницю” потрібно чітко визначити відповідальність за розголошення комерційної таємниці. А саме адміністративну, кримінальну, а головне – матеріальну в повному обсязі, як юридичних, фізичних осіб, в тому числі службових осіб органів державної влади, включаючи службових осіб контролюючих та правоохоронних органів, а також органів місцевого самоврядування, які мають або мали доступ до комерційної таємниці, і з їх вини відбувся витік комерційної таємниці завдавши матеріальні збитки підприємству чи організації.

Варто відзначити, що у 2016 р. Конгрес США ухвалив Федеральний Закон про комерційну таємницю (Defend Trade Secrets Act of 2016, скорочена назва – DTSA). Закон систематизує норми щодо захисту комерційної таємниці у всіх штатах США, а також передбачає можливість притягнення до відповідальності співробітників і підрядників за розголошення комерційної таємниці компанії тощо [16]. Досить великий спектр проблематики стосовно охорони комерційної таємниці суб’єктів господарювання, був нами розкритий в попередніх наукових працях [17 – 23]. Тому, на нашу думку та на думку багатьох вчених, потрібно розробляти і впроваджувати в життя Закон України “Про комерційну таємницю” на кращих прикладах законодавчої бази розвинутих країн Європи та США.

#### **Висновки.**

З метою стимулювання інноваційного розвитку і захисту комерційної таємниці суб’єктів господарювання, варто запропонувати такі зміни до законодавства:

– прийняти Закон України “Про комерційну таємницю”;

– закріпити поняття “ноу-хау (секрет виробництва)” з вказівкою на те, що виключне право на секрет виробництва діє до тих пір, поки стосовно даного ноу-хау діє режим комерційної таємниці;

– у Кодексі законів про працю України закріпити обов’язок працівника не розголошувати (збирати, використовувати) комерційну таємницю, що належить роботодавцю, без спеціального дозволу, а також дозволити зазначати в трудовому договорі умову, згідно з якою для особи може встановлюватися заборона працювати певний строк (наприклад до 5 років) на підприємствах, які є конкурентами попереднього роботодавця за умови, якщо працівник мав доступ до комерційної таємниці останнього.

Таким чином, комерційна таємниця є складною правовою та економічною категорією, а для підприємства – не лише способом захисту інформації з обмеженим доступом, яка має комерційну цінність, а і економічним інтересом та стратегічним ресурсом, який здатний забезпечити конкурентні переваги на ринку промисловості.

### Використана література

1. Угода про торговельні аспекти прав інтелектуальної власності (TRIPS) : редакція від 06.12.05 р. – Режим доступу : [http://zakon3.rada.gov.ua/laws/show/981\\_018](http://zakon3.rada.gov.ua/laws/show/981_018). – (ВР України : База даних “Законодавство України” : документ 981\_018 ).
2. Господарський кодекс України : Закон України // Відомості Верховної Ради України (ВВР). – 2003. – № 18-22. – Ст. 144. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/436-15>. – (ВР України : База даних “Законодавство України” : документ 436-15).
3. Цивільний кодекс України : Закон України // Відомості Верховної Ради України (ВВР). – 2003. – № 40-44. – Ст. 356. – Режим доступу : <http://zakon1.rada.gov.ua/laws/show/435-15>. – (ВР України : База даних “Законодавство України” : документ 435-15).
4. Марущак А.І. Правові основи захисту інформації з обмеженим доступом : курс лекцій. – К. : КНТ, 2007. – 208 с.
5. Андрощук Г.А. Экономическая безопасность предприятия: защита коммерческой тайны / Г.А. Андрощук, П.П. Крайнев. – К. : Изд. дом “Ин Юре”, 2000. – 400 с.
6. Задихайло Д.В. Стратегія держави в системі законодавчого регулювання економічних відносин // Вісник Академії правових наук України. – 2006. – № 1 (44). – С. 129-138.
7. Пашков В.М. Правовий господарський порядок і урядова фармацевтична політика, її наслідки та уроки // Вісник Національної академії правових наук України. – 2009. – № 2 (57). – С. 84-95.
8. Організаційно-правові основи охорони комерційної таємниці ; укладачі В.І. Журавель, Т.Ю. Ткачук ; за заг. ред. О.Д. Довганя. – К. : НА СБ України, 2013. – 321 с.
9. Олефір А.О. Правове регулювання інтелектуальної власності та інноваційних відносин в Угоді про асоціацію України та ЄС // Теорія і практика інтелектуальної власності. – 2014. – № 5. – С. 79-94.
10. Lundvall B.A. National Systems of Innovation : Towards a Theory of Innovation and Interactive Learning / B.A. Lundvall. – London : Pinter Publishers, 1992. – 320 p.
11. Бубенко П.Т. Інтелектуальна власність : навч. посіб. / П.Т. Бубенко, В.В. Величко, С.М. Глухарев. – Х. : ХНАМГ, 2011. – 215 с.
12. Томберг И. Топ 7 энергетических инноваций / Бюллетень Ин-та общественного проектирования. – 2011. – № 5. – С. 6-7.
13. Право інтелектуальної власності : акад. курс : підруч. для студ. вищих навч. закладів / [О.П. Орлюк, Г.О. Андрощук, О.Б. Бутнік-Сіверський та ін.] ; за ред. О.П. Орлюк, О.Д. Святоцького. – К. : Вид. Дім “Ин Юре”, 2007. – 696 с.
14. Давидюк О.М. Технологія як об’єкт господарсько-правового регулювання : монографія / О. М. Давидюк. – Х. : ФІНН, 2010. – 176 с.

15. Хавронюк М. Підприємницьке шпигунство : розголошення комерційної таємниці, юридичний аналіз складів злочинів, питання удосконалення відповідальності // Предпринимательство, хозяйство и право. – 1999. – № 9. – С. 4-17.

16. Defend Trade Secrets Act of 2016. Public Law 114-153. – Режим доступу : <https://www.congress.gov/bill/114th-congress/senate-bill/1890/text> – Назва з екрана. – Дата звернення : 1.03.2017 р..

17. Кравченко О.М. Взаємодія правоохоронних органів з підприємствами, установами та організаціями в охороні комерційної таємниці // Вісник Академії праці, соціальних відносин і туризму. – 2016. – № 3-4. – С. 29-34.

18. Кравченко О.М. Проблеми правової природи комерційної таємниці як окремого виду таємної інформації в Україні // Вісник Академії праці, соціальних відносин і туризму. – 2015. – № 1-2. – С. 59-65.

19. Кравченко О.М. Перспективи адаптації законодавства України до міжнародних стандартів охорони комерційної таємниці // Право України. – № 2/2016. – С. 175-181.

20. Кравченко О.М. Впровадження інноваційних напрямів правового забезпечення охорони комерційної таємниці // Публічне право. – № 1(21)2016. – С. 353-360.

21. Кравченко О.М. Досвід зарубіжних країн в правовій охороні комерційної таємниці // Інформаційна безпека. – № 1(17)2015. – С.91-98.

22. Кравченко О.М. Нові парадигми сучасних загроз комерційній таємниці // Інформаційна безпека. – № 3(19)2015. – С. 111-121.

23. Кравченко О.М. Актуальні проблеми захисту комерційної таємниці суб'єктів господарювання // Інформаційна безпека. – № 1(20)2016. – С.69-82.

~~~~~ \* \* \* ~~~~~

УДК 34:004+342.553+571

ДУБНЯК М.В., аспірант НДІ інформатики і права НАПрН України

СИСТЕМА ОСНОВНИХ ТЕРМІНІВ, ЯК ОСНОВА ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ У МІСЦЕВОМУ САМОВРЯДУВАННІ

***Анотація.** В статті з'ясовано особливості розуміння деяких базових категорій інформаційного права у їх прикладному застосуванні до певної предметної сфери – місцевого самоврядування та сформульовані дефініції термінів “інформаційна взаємодія”, “інформаційний продукт”, “інструмент інформаційної взаємодії”. Обґрунтовано необхідність наявності взаємоузгодженої системи термінів як умови формування пропозицій щодо внесення змін в законодавство та запропоновано макет законопроекту щодо правового регулювання інформаційної взаємодії в процесі прийняття рішень на місцевому рівні із поясненням змісту конкретних правових норм та підходів щодо їх формулювання.*

***Ключові слова:** поняття, інформаційна взаємодія, місцеве самоврядування, інформаційне право.*

***Аннотация.** В статье выяснены особенности понимания некоторых базовых категорий информационного права в их прикладном применении к определенной предметной области – местному самоуправлению и сформулированы дефиниции терминов “информационное взаимодействие”, “информационный продукт”, “инструмент информационного взаимодействия”. Обоснована необходимость наличия взаимосогласованной системы терминов как условия формирования предложений по внесению изменений в законодательство и предложен макет законопроекта о правовом регулировании информационного взаимодействия в процессе принятия решений на местном уровне с объяснением содержания конкретных правовых норм и подходов к их формированию.*

***Ключевые слова:** понятие, информационное взаимодействие, местное самоуправление, информационное право.*

***Summary.** The article provides particular features of understanding of a certain basic categories of information law in their application to a specific subject area – local government. The following terms are defined: “information interaction”, “information product”, “the instrument of information interaction”. The necessity of mutually agreed terminology is justified, as a condition for proposition of legislation amendments. The draft law is proposed to address the legal regulation of information interaction in decision making process at the local government level, explaining the content of specific legal rules and approaches to their formulation.*

***Keywords:** terms, categories, information interaction, local government, information law.*

Постановка проблеми. Під час аналізу нормативно-правових актів (Закон України “Про місцеве самоврядування”, регламенти рад та статuti громад) стає зрозуміло, що всі етапи прийняття рішення базуються на інформаційній взаємодії між різними суб’єктами місцевого самоврядування, в тому числі і територіальною громадою, а якість прийнятих рішень безпосередньо залежить від можливості отримувати, використовувати та надавати для подальшої роботи повну, достовірну та своєчасну інформацію, тобто забезпечувати повний цикл ефективного обороту інформації.

Правове регулювання в частині забезпечення участі територіальної громади в процесі прийняття рішень нормами інформаційного права безперечно сприятиме підвищенню якості рішень та рівня життя територіальної громади. Результати теоретичних досліджень інформаційної взаємодії у місцевому самоврядуванні викладено

в роботі [1]. Зокрема, запропоновано соціальну модель процесу прийняття рішення, на її базі створено правову модель інформаційної взаємодії, при дослідженні інформаційних правовідносин виявлено дисбаланс у правовому регулюванні обсягу закріплених прав, обов'язків та відповідальності всіх суб'єктів місцевого самоврядування, а також встановлено, що способи участі членів територіальної громади в управлінні місцевими справами є недосконалими саме через неповноту правового регулювання обороту інформації між всіма зацікавленими суб'єктами.

З'ясовано, що на основі змісту дефініцій системи термінів, які використовуються для побудови такої моделі, в основному формується загально теоретичне та практичне уявлення про сутність та межі предмету дослідження – інформаційної взаємодії у місцевому самоврядуванні, а також певним чином визначається обсяг правового регулювання нормами інформаційного права.

Таким чином, є актуальним формування узгодженої та універсальної системи термінів інформаційної взаємодії в місцевому самоврядуванні, що забезпечить вдосконалення законодавства, в частині регулювання інформаційних відносин в процесі використання інструментів інформаційної взаємодії у місцевому самоврядуванні.

Результати аналізу наукових публікацій свідчить про те, що розробкою та удосконаленням термінологічного апарату інформаційного права присвячено роботи таких науковців І.В. Арістової, О.А. Баранова, К.І. Белякова, В.М. Брижка, В.Г. Пилипчука, Н.А. Савінової, О.М. Селезньової, І.М. Сопілко, В.М. Фурашева та інші. Окремі питання інформаційної взаємодії досліджували В.Я. Місюра, Ю.С. Назар, Т.Є. Сігаєва, А.Г. Спиркин, О. Ястремська.

Метою статті є дослідження системи термінів інформаційного права та встановлення особливостей їх праворозуміння при застосуванні у предметній сфері – в частині удосконалення законодавства щодо інформаційної взаємодії у місцевому самоврядуванні.

Виклад основного матеріалу. Дослідження інформаційних відносин є предметом галузі інформаційного права, а відтак необхідно з'ясувати чи мають свою специфіку “класичні” терміни та їх дефініції інформаційного права при їх застосуванні у будь-якій предметній сфері, в нашому випадку – в місцевому самоврядуванні.

Відповідно до системного галузевого і міжгалузевого характеру термінів та їх дефініцій правового інституту, галузі права та законодавства в цілому покликані виконувати ієрархічну системо та структуро-утворювальну функцію [2, с. 64]. Тобто, терміни незалежно від сфери їх застосування повинні розумітись однаково, що забезпечує єдність правової системи.

Досліджуючи значення дефініцій в законодавчих текстах А.В. Хворостянкіна, зазначає, що будь-який правовий припис виражається за допомогою термінів, як основних мовних одиниць, які мають бути зрозумілими для всіх осіб, яким адресовано припис. Одним із способів забезпечення такої зрозумілості є застосування в текстах нормативно-правових актів правових дефініцій [3].

В межах цієї статті проведемо дослідження основних термінів інформаційного права в контексті їх застосування при правовому регулюванні суспільних відносин у місцевому самоврядуванні: інформаційні потреби, інструмент інформаційної взаємодії, об'єкт інформаційних правовідносин, інформаційний продукт, інформаційна взаємодія.

Інформаційна потреба – усвідомлена необхідність у знаннях, або іншими словами – усвідомлення недостатності наявних знань [4, с. 327].

Під-час дослідження інформаційної діяльності у місцевому самоврядуванні встановлено, що обсяг інформації, який надається органом місцевого самоврядування

про свою діяльність, про етапи та зміст процесу прийняття рішення є неповним та таким, що вичерпно не може задовольнити інформаційних потреб громади.

Так, інформація про процес прийняття рішення, яка по суті повинна створити умови для забезпечення можливості громадянам брати участь в управлінні місцевими справами, насправді є фрагментарною та неповною, що не дозволяє громадянину скласти системне уявлення про етапи та зміст процесу прийняття рішення, а також про інструменти, за допомогою яких громадянин може вплинути на цей процес.

Разом з тим, вбачається звуженням розуміння “забезпечення інформаційних потреб громадянина” тільки у контексті отримання інформації в порядку доступу до публічної інформації через подання заяв і звернень, а також отримання інформації про діяльність органу влади зі ЗМІ, оскільки, в такому випадку, є лише етап отримання інформації від органу влади про його діяльність, що звужує категорію “інформаційні потреби громадян”, не охоплюючи участь та взаємодію, що є складовими елементами “управління місцевими справами”.

Таким чином, надаємо наступне визначення терміну “інформаційна потреба у місцевому самоврядуванні” – усвідомлена суб’єктами інформаційної взаємодії необхідність отримання знань про етапи та зміст процесу прийняття та виконання рішення, а також про інструменти, за допомогою яких громада може брати участь в цьому процесі.

Тобто, в процесі інформаційної взаємодії задоволення інформаційних потреб громадян та інших суб’єктів можна розглядати як наявність доступу до будь-якої інформації та можливостей реалізувати права, пов’язані із оборотом інформації, необхідної для участі в процесі прийняття рішення органом місцевого самоврядування.

Один із підходів визначення процесу прийняття управлінського рішення запропонував А.С. Безруков, який розумів його як сукупність взаємозалежних цілеспрямованих послідовних управлінських дій, які забезпечують реалізацію управлінських завдань, що знаходять відображення у функціях управлінського апарату щодо аналізу ситуацій та прийняття рішень на стратегічне і короткострокове планування [5].

Зазначене визначення не розкриває змісту “послідовних управлінських дій”, а тому для формування системного уявлення про процес прийняття рішення необхідно акцентуватись саме на його складових, тому на основі результатів дослідження [6] для місцевого самоврядування пропонується таке визначення: “процес прийняття рішення у місцевому самоврядуванні” – сукупність логічно-послідовних етапів циклу управлінської діяльності, який включає: визначення проблемного питання, внесення пропозиції щодо вирішення проблем, аналіз альтернативних проектів вирішення проблеми та їх рейтингування, розробка проекту рішення, прийняття рішення, оприлюднення прийнятого рішення та плану його виконання, виконання рішення, контроль за виконанням рішення, коригування плану виконання на будь-якому проміжному етапі за умови забезпечення будь-якому суб’єкту місцевого самоврядування можливості впливу на прийняття рішення через оцінку та врахування інформаційних продуктів, створених у процесі використання інформаційних інструментів.

Процес прийняття рішення обумовлений оборотом інформації між всіма суб’єктами, тому необхідно розглянути способи, форми та прийоми за допомогою яких здійснюється такий оборот інформації.

Дуже важливим елементом реалізації інформаційної взаємодії є інструменти. В європейських документах зустрічається вичерпне описання понад 20 інструментів, у законодавстві України – їх близько 10, але стан правового регулювання є недосконалим.

Під інструментом в прямому значенні розуміють засіб, спосіб для досягнення мети, або впливу, контролю чи зміни стану властивостей [7]. Так, наприклад, у фінансовому

праві фінансовим інструментом є будь-який контракт, який приводить до виникнення фінансового активу у одного суб'єкта господарювання та фінансового зобов'язання або інструмента капіталу у іншого суб'єкта господарювання [8].

Отже, інструментом незалежно від його використання в предметній сфері є засіб за допомогою якого здійснюється вплив з метою зміни існуючого стану будь-чого. При цьому з визначення фінансового інструменту вбачається наступний зв'язок: якщо один суб'єкт реалізує своє право, то в іншого суб'єкта (або суб'єкта, на якого спрямована реалізація права) виникає обов'язок.

Розглянемо інший приклад – діяльність прес-служб органів влади.

До інформаційних інструментів прес-служб органів місцевого самоврядування віднесено: 1) брифінг; 2) прес-реліз; 3) анонс; 4) прес-пам'ятка, 5) медіа-комплекти, 6) прес-конференція, 7) інтерв'ю, 8) виставки, 9) газетні статті, 10) буклети і брошури, 11) громадські слухання, 12) громадські дорадчі комітети, 13) опитування громадської думки, 14) громадська експертиза, 15) офіційний веб-сайт [9, с. 61-62].

Очевидно, що наведені у переліку інструменти 1 – 10, 15 є односторонніми каналами інформування, але вони аж ніяк не забезпечують взаємодію, оскільки відсутній суб'єкт та мета такої взаємодії, за допомогою зазначених інструментів відбувається лише інформування (створення та передання інформації). Більш цікавими є інструменти під номерами 11 – 14 з переліку, оскільки вони обумовлюють ціль та мету взаємодії. Тобто їх застосування обумовлює активні дії обох сторін.

Тому під “інструментом інформаційної взаємодії у місцевому самоврядуванні” пропонується розуміти певну сукупність методів, інформаційних технологій та засобів забезпечення інформаційної взаємодії між суб'єктами місцевого самоврядування.

Для подальшого описання правової моделі інформаційної взаємодії суб'єктів місцевого самоврядування важливо мати уявлення про об'єкт інформаційних відносин. Змістовне, коректне та лаконічне визначення запропонував В.М. Брижко, за яким інформаційні відносини – це відносини, які виникають у всіх сферах життя і діяльності людини, суспільства і держави при збиранні, зберіганні, використанні та поширенні інформації [10, с. 86].

Об'єктом інформаційних правовідносин є інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [11]. Досліджуючи об'єкт інформаційних правовідносин, Д.О. Перов зауважує, що об'єктом правовідносин виступає благо, а не самі дії, незважаючи навіть на те, що вони будуть спрямовані на цей об'єкт [12, с. 92]. На нашу думку, зауваження вказаного дослідника є дещо передчасним, оскільки норми права регулюють майже всю різноманітність суспільних відносин, а тому звуження цього обсягу лише до визначення одного об'єкта, такого як “благо”, не забезпечує системності наукового дослідження.

Сучасному стану інформаційних відносин відповідає плюралістичний підхід, за яким об'єктом інформаційних правовідносин є матеріальні та нематеріальні блага, які можуть виступати у вигляді послуг, робіт, поведінки, дії та їх результатів [13, с.71].

Отже, об'єкт “інформаційних правовідносин у місцевому самоврядуванні” це матеріальні та нематеріальні блага, що є результатом інформаційної діяльності та поведінки суб'єктів місцевого самоврядування, які діють в рамках своїх юридичних прав і обов'язків та несуть юридичну відповідальність.

Таким чином, до об'єктів інформаційної взаємодії в місцевому самоврядуванні може бути віднесено: матеріальний об'єкт – інформаційні продукти, які створюються суб'єктами місцевого самоврядування (членами територіальної громади та суб'єктами органу місцевого самоврядування) та пов'язані із реалізацією права (подання письмової

заяви, пропозиції, скарги, місцевої ініціативи, е-петиції тощо) чи здійснення повноважень (складання проекту нормативного акту, звіту тощо); нематеріальний об’єкт – право на подання заяви; право на розгляд чи відхилення пропозиції; різновидом поведінки – дії суб’єктів місцевого самоврядування, що пов’язані із збором підписів, поданням заяви, дії щодо організації роботи комісії та інші [14, с. 44].

Оскільки інформаційні продукти є матеріальним об’єктом для подальшого описання правової моделі інформаційної взаємодії необхідно з’ясувати їх зміст. Під інформаційними продуктами можна розуміти – документи, інформаційні масиви, бази даних, які є результатом функціонування інформаційних систем, тобто систем, призначених для зберігання, обробки, пошуку, розповсюдження, передачі та надання інформації [15, с. 6]. Інформаційний продукт (продукція) – створена виробником сукупність документованої інформації, відомостей, даних і знань, які призначені для забезпечення інформаційних потреб користувача [16, с. 35].

Закон України “Про інформацію” надає наступне визначення інформаційної продукції – матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб’єктів інформаційних відносин [11].

Визначення, яке можливо використати із прямим запозиченням та адаптацією до предметної сфери, запропонував Баранов О.А.: інформаційний продукт – це будь-яка відокремлена інформація, представлена в конкретній організаційній формі та вигляді, з приводу якої можуть виникнути правові відносини [13, с. 166].

Проаналізувавши зазначені дефініції, запропонуємо наступне визначення: “інформаційні продукти суб’єктів місцевого самоврядування” – це будь-яка відокремлена інформація, представлена в конкретній організаційній формі та вигляді із зазначенням певних реквізитів, створена у зв’язку із здійсненням своїх повноважень органами і посадовими особами місцевого самоврядування, або у зв’язку із реалізацію права територіальної громади на участь в процесі прийняття рішення та управління місцевими справами.

До таких інформаційних продуктів можна віднести: проекти рішень та рішення органу місцевого самоврядування, розпорядження та звіти голів рад будь-якого рівня, звіти депутатів, протоколи комісій, робочих груп, експертні пропозиції, письмові запити, заяви, скарги, пропозиції, протоколи загальних зборів, проекти рішень поданих в порядку місцевої ініціативи, пропозиції за результатами громадських слухань та інші.

Базовим терміном, який необхідно використати для опису правової моделі інформаційної взаємодії суб’єктів місцевого самоврядування, є термін “інформаційна взаємодія”. Зазначений термін складається із двох змістовно-навантажених слів “інформація” та “взаємодія”.

Здійснюючи системний та узагальнюючий аналіз, Ю.С. Назар розглянув поняття “взаємодія” у філософському, управлінському та правовому аспекті та зробив наступні висновки: взаємодія – динамічне явище, яке відбувається на підставі певної діяльності суб’єктів, зумовлює розвиток певної упорядкованої якості – системи, приведеної у відповідність із соціально-бажаним станом з метою соціального управління, оскільки без відносно стійких зв’язків та взаємодії складових, система під впливом зовнішніх і внутрішніх дій розпадається [17, с. 9].

Взаємодія в управлінському аспекті розглядається як взаємодія між суб’єктом та об’єктом управління і як взаємодія між суб’єктами управлінського процесу щодо досягнення спільної мети [17, с. 11]. У філософському аспекті: взаємодія відображає процеси впливу об’єктів один на одного, їхню взаємну обумовленість [17, с. 17].

Взаємодія як діяльність суб'єктів – узгоджена за завданням, напрямом і часом дії різних суб'єктів для досягнення спільної мети [18, с. 8].

Ознаки взаємодії: це діяльність; наявність декількох суб'єктів (не менше двох); узгодженість заходів за ціллю, місцем, часом, методами; спрямованість функціонування взаємодіючих суб'єктів; наявність нормативної (правової) бази взаємодії; становище, за яким суб'єкти посідають в ієрархії системи; зміст завдань, які вирішуються суб'єктами взаємодії; спільна діяльність [19, с. 298-299].

Значення категорії “взаємодія”, за поглядами В.Я. Місюри, полягає в тому, що вона обумовлює наявність нових інтегративно-синергетичних якостей цілісної системи, не властивих окремим частинам і компонентам, що її утворюють. Ефективним напрямом модернізації системи державного управління в такому аспекті видається впровадження взаємодії як провідного організаційного принципу в саму логіку та зміст функціонування системи [20, с. 13].

Інформаційну взаємодію також розуміють як процес забезпечення інформацією, сукупність форм документів, нормативної бази та реалізованих рішень щодо обсягів, розміщення та форм існування інформації, яка використовується в інформаційній системі в процесі її функціонування [21, с. 142]. Термін “взаємодія” означає також взаємний зв'язок явищ, понять, погодженість дій [22].

Підхід щодо особливостей розуміння класичних термінів інформаційного права у певній предметній сфері також простежується у роботі Т.Є. Сігаєвої, яка розглядала інформаційну взаємодію підприємства з суб'єктами зовнішнього середовища в процесі інвестування. Так, під інформаційною взаємодією в процесі інвестування вона розуміє наступне: активний обмін інформацією між підприємством (про свої здобутки і можливості запроваджуваного інвестиційного проекту) та суб'єктами зовнішнього середовища, що мають намір або беруть участь в процесі інвестування (про цілі, очікувану ефективність від вкладання капіталу) [23, с. 6].

Позитивними рисами цього визначення є те, що дослідник, на думку автора, виділив три універсальні характеристики інформаційної взаємодії: 1) обмін інформацією, 2) суб'єкти такого обміну 3) мету обміну, а також ним було ціннісний орієнтир – фактор “оцінки” очікуваних результатів взаємодії.

Заслуговує на увагу думка О. Ястремської, яка зауважила, що інформаційна взаємодія має бути побудована як активна та симетрична система, що має два напрямки: від підприємства до зовнішнього середовища і навпаки. Симетричність передачі інформації має відображати стан поінформованості про ефективність роботи, стан зовнішнього середовища, передачу інформації про можливості та результати діяльності з метою формування вигідних та конструктивних взаємовідносин [24, с. 60].

Отже, надамо наступне визначення: “інформаційна взаємодія суб'єктів місцевого самоврядування” – це інформаційна діяльність всіх суб'єктів місцевого самоврядування, результатом якої є інформація (інформаційні продукти, документи, дані тощо), якою обмінюються всі суб'єкти, що є учасниками процесу прийняття рішень, та яка на будь-якому його етапі здатна задовольнити їх інформаційні потреби, повинна бути розглянута, оцінена та врахована.

Таким чином, інформаційна взаємодія спрямована на задоволення інформаційних потреб громадян та посадових осіб органів місцевого самоврядування, що обумовлює підвищення ефективності діяльності у місцевому самоврядуванні в цілому.

Для удосконалення форм участі громадян у процесі прийняття рішень та участі в управлінні місцевими справами необхідне відповідне правове регулювання всіх етапів обороту інформації із зазначенням форми інформаційних продуктів, які утворюються в

результаті такої діяльності, інформаційних інструментів, за допомогою яких це можливо здійснити, на базі єдиної системи вищезазначених термінів.

Прикладне застосування вищевикладених положень та визначень системи основних термінів інформаційного права у місцевому самоврядуванні дозволили сформулювати конкретні пропозиції щодо удосконалення правового регулювання інструментів інформаційної взаємодії, як форм безпосередньої демократії (зустрічі з територіальною громадою, консультації з територіальною громадою та громадська експертиза).

Відповідно до законодавства правове регулювання таких форм безпосередньої демократії в переважній більшості випадків має бланкетний характер та вимушено деталізується на рівні підзаконних актів представницького органу місцевого самоврядування або статутом територіальної громади.

Більшість таких підзаконних актів просто копіюють положення статей Закону України “Про місцеве самоврядування” [25] без будь-якої деталізації правового регулювання процедур та механізмів реалізації певних форм демократії чи адаптації до місцевих умов. Таке правове регулювання не містить деталізації процедур та механізмів і залишає громаду без дієвих правових механізмів.

Пропонується здійснити побудову законопроекту на основі модельного підходу – визначення в тексті закону основних правових принципів, механізмів та положень, що регламентують правове регулювання суспільних відносин, пов’язаних з реалізацією певних форм безпосередньої демократії, з таким ступенем деталізації, яка унеможливить зайву дискрецію органів місцевого самоврядування. Законопроект не встановлює детальних процедур реалізації певних форм демократії, тому принцип правової та організаційної самостійності органів місцевого самоврядування буде дотримано. Структуру законопроекту наведено далі.

Проект Закону України “Про внесення змін до Закону України “Про місцеве самоврядування” щодо удосконалення інформаційної взаємодії в процесі прийняття рішень”

Розділ I. Загальні положення

Розділ II. Організаційно-правова основа місцевого самоврядування

Глава 1. Повноваження сільських, селищних, міських рад

Глава 2. Повноваження виконавчих органів сільських, селищних, міських рад

Глава 3. Сільський, селищний, міський голова

Глава 4. Повноваження районних і обласних рад

Глава 5. Порядок формування, організація роботи органів та посадових осіб місцевого самоврядування

Розділ III. Матеріальна і фінансова основа місцевого самоврядування

Розділ IV. Гарантії місцевого самоврядування. Відповідальність органів та посадових осіб місцевого самоврядування

Розділ V. Інформаційна взаємодія в процесі залучення громадян до прийняття рішень

ГЛАВА 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ

Стаття 81. Основні принципи правового регулювання інформаційної взаємодії в місцевому самоврядуванні

Стаття 82. Інформаційна взаємодія в процесі прийняття рішення

Стаття 83. Оприлюднення інформації

Стаття 84. Особливості оприлюднення інформації на веб-сайтах органів місцевого самоврядування

- Стаття 85. Інструменти інформаційної взаємодії в процесі прийняття рішення
- Стаття 86. Інформаційні продукти
- Стаття 87. Правовий режим інформаційних продуктів

ГЛАВА 1.1. Консультації з територіальною громадою, як інструмент інформаційної взаємодії

- Стаття 88. Консультації з територіальною громадою
- Стаття 89. Суб'єкти консультації з територіальною громадою
- Стаття 90. Інформаційні продукти консультацій з територіальною громадою та порядок їх оприлюднення
- Стаття 91. Ініціювання та підстави проведення загальної консультації
- Стаття 92. Ініціювання та підстави для проведення прямої консультації
- Стаття 93. Підстави для відмови у розгляді повідомлень
- Стаття 94. Розгляд повідомлень отриманих в процесі консультації
- Стаття 95. Врахування результатів консультацій

ГЛАВА 1.2. ЗУСТРІЧІ З ТЕРИТОРІАЛЬНОЮ ГРОМАДОЮ, ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ

- Стаття 96. Зустрічі з територіальною громадою
- Стаття 97. Суб'єкти зустрічей
- Стаття 98. Інформаційні продукти зустрічей
- Стаття 99. Ініціювання та підстави проведення зустрічі
- Стаття 100. Порядок проведення зустрічей
- Стаття 101. Завершення зустрічі

ГЛАВА 1.3. ГРОМАДСЬКА ЕКСПЕРТИЗА, ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ

- Стаття 102. Громадська експертиза діяльності органів місцевого самоврядування
- Стаття 103. Суб'єкти громадської експертизи
- Стаття 104. Інформаційні продукти строк та порядок їх оприлюднення
- Стаття 105. Ініціювання та підстави проведення громадської експертизи
- Стаття 106. Прийняття рішення про проведення громадської експертизи
- Стаття 107. Підстави для відмови у проведенні громадської експертизи
- Стаття 108. Проведення громадської експертизи
- Стаття 109. Сприяння проведенню громадської експертизи
- Стаття 110. Закінчення проведення громадської експертизи
- Стаття 111. Розгляд та врахування експертних пропозицій
- Стаття 112. Особливості притягнення до відповідальності за порушення прав територіальної громади на інформаційну взаємодію

Розділ VI. Прикінцеві та перехідні положення.

Загальна характеристика та основні положення законопроекту щодо вдосконалення правового регулювання інформаційної взаємодії з метою забезпечення участі громади у процесі прийняття і виконання рішень органами місцевого самоврядування.

Законопроект складається з одного розділу, який пропонується включити в структуру Закону України “Про місцеве самоврядування” перед “Прикінцевими і перехідними положеннями” з продовженням наскрізної нумерації статей Закону. Розділ містить “Загальні положення” та три глави, присвячених правовому регулюванню наступних інструментів інформаційної взаємодії: “консультації з територіальною громадою”, “зустрічі з територіальною громадою”, “громадська експертиза”, та містить 32 статті.

Пропонується внести зміни до ст. 1 Закону із визначенням 4 нових термінів, які розкривають зміст та суть відносин з інформаційної взаємодії: “інформаційна взаємодія суб’єктів місцевого самоврядування”, “оприлюднення інформації суб’єктів місцевого самоврядування”, “інформаційні продукти суб’єктів місцевого самоврядування”, “інструмент інформаційної взаємодії”.

В загальних положеннях законопроекту щодо вдосконалення правового регулювання інформаційної взаємодії визначаються специфічні правові принципи, визначено загальні положення щодо оприлюднення інформації, які додатково можуть бути деталізовані статутом територіальної громади; встановлено обов’язок органів місцевого самоврядування оприлюднювати інформацію в рубриках “прийняття рішення”, “участь громадян” та в їх відповідних підрубриках офіційного веб-сайту органу місцевого самоврядування, які повинні забезпечити системне уявлення про процес прийняття рішення та механізмів участі громадськості в цьому процесі.

Визначено перелік інформаційних продуктів – які створюються під час виконання повноважень чи реалізації прав та підлягають обов’язковому оприлюдненню в порядку, визначеному законопроектом та у строк, визначений Законом України “Про доступ до публічної інформації”.

Крім того, в законопроекті запропоновані правові механізми регулювання таких інструментів інформаційної взаємодії, як: консультації з територіальною громадою, зустрічі з територіальною громадою, та громадська експертиза на місцевому рівні.

У консультаціях з територіальною громадою передбачено два види консультації – загальна, яка проводиться обов’язково та пряма, яка проводиться за ініціативою органів та посадових осіб місцевого самоврядування або територіальної громади. В законопроекті пропонується – загальну консультацію, результати якої є обов’язковими для врахування при прийнятті будь-якого рішення, проводити на офіційних веб-сайтах органів місцевого самоврядування.

Оскільки проекти рішень відповідно до Закону України “Про доступ до публічної інформації” оприлюднюються за 20 днів до їх розгляду та остаточного прийняття, то строк проведення загальної консультації становить 15 днів з дня оприлюднення проекту рішення.

Таким чином, проведення консультації не буде перешкоджати та гальмувати усталену практику процесу прийняття рішення, а лише забезпечить можливість участі в ньому громади. Крім того, з моменту закінчення консультації з територіальною громадою орган місцевого самоврядування має 5 днів для розгляду і врахування пропозицій у разі їх отримання.

Пряма консультація оголошується органом місцевого самоврядування, щодо проекту рішення чи за результатом виконання прийнятого рішення.

Новелою законопроекту є встановлення правового обов’язку органу місцевого самоврядування вести Реєстр осіб та організацій, які брали участь в консультаціях або подали заяви про включення їх до зазначеного Реєстру. До Реєстру включається така інформація: П.І.Б для фізичної особи, її місце проживання; найменування для юридичної особи чи об’єднань громадян відомостей про їх легалізацію; адреси електронної пошти; іншої контактної інформації, додатково повідомленої суб’єктами консультацій, в тому числі щодо конкретної сфери суспільних відносин (пріоритетної сфери), з яких органи та посадові особи місцевого самоврядування мають відповідні повноваження. Зазначений Реєстр має бути допоміжним інструментом для органу місцевого самоврядування при оголошенні прямих консультацій, оскільки містить інформацію про пріоритетні сфери, щодо яких громадськість бажає брати участь в консультаціях.

Також законопроектом пропонується встановлення правового обов'язку органів місцевого самоврядування щодо складання звіту за результатами проведених консультацій. Встановлено критерії та зміст, яким має відповідати звіт та строки його підготовки: для загальних консультацій – 2 рази на рік, для прямих – протягом 5 днів з моменту їх завершення.

Глава “Зустрічі з територіальною громадою як інструмент інформаційної взаємодії” розкриває зміст нових форм зустрічей з територіальною громадою, таких як: “громадські слухання”, “експертні слухання”, “громадські обговорення”, “відкриті засідання”, “форуми”.

Необхідність уніфікації зазначених форм безпосередньої участі громадян у процесі прийняття рішень обумовлена тим, що в національному законодавстві є непоодинокі приклади застосування процедури громадських слухань, зокрема, в законах України “Про місцеве самоврядування в Україні” (ст. 13), “Про регулювання містобудівної діяльності” (ст. 21) “Про охорону навколишнього природного середовища” (ст. ст. 6, 9, 20), Постанові Кабінету Міністрів України “Про затвердження Порядку проведення громадських слухань щодо врахування громадських інтересів під час розроблення проектів містобудівної документації на місцевому рівні” від 25.05.11 р. № 555, але певні норми мають різний правовий зміст, а значить – і різні правові наслідки.

Визначення публічних слухань законом не закріплено, а зі змісту зазначених норм видно, що громадські (публічні) слухання використовують для отримання письмових пропозицій щодо проектів містобудівної документації та програм охорони навколишнього природного середовища.

При цьому механізм проведення громадських слухань здійснюється шляхом подання письмових пропозицій від визначеного цими нормативними актами суб'єктів.

За чинною редакцією ст. 13 Закону України [25] громадські слухання визначаються як зустріч територіальної громади з депутатами відповідної ради та посадовими особами місцевого самоврядування, під час яких члени територіальної громади можуть заслуховувати їх, порушувати питання та вносити пропозиції щодо питань місцевого значення, що належать до відання місцевого самоврядування.

Таким чином, кваліфікуючими ознаками громадських слухань є те, що це: 1) безпосередні зустрічі територіальної громади із депутатами ради та посадовими особами місцевого самоврядування; 2) форми роботи зустрічі – заслуховування; порушення питань; внесення пропозицій; 3) питання мають належати до відання місцевого самоврядування.

Правове регулювання лише однієї форми роботи громадських слухань, як внесення пропозицій щодо двох предметів – містобудування та охорони навколишнього природного середовища – не вбачається вірним з огляду на таке.

По-перше, отримання письмових обґрунтованих пропозицій доцільно здійснювати іншим інструментом інформаційної взаємодії – консультації з громадськістю (територіальною громадою), які проводяться переважно у письмовій формі.

По-друге, Законом України [25] визначено повноваження виконавчих органів рад у 17 сферах, які безпосередньо стосуються інтересів членів територіальної громади.

Чинна редакція ст. 13 Закону України [25] не передбачає можливість територіальної громади заслуховувати посадових осіб виконавчих органів рад.

Таким чином, пропонується удосконалити правове регулювання застосування інструменту громадських слухань, акцентувавши увагу саме на тому, що: це є зустрічами територіальної громади з визначеними суб'єктами; що до суб'єктів, яких вони заслуховують додаються експерти, виконавчі органи рад, інші органи влади. В такому випадку слухання трансформуються в експертні слухання, громадські

обговорення, відкриті засідання, форуми, відповідні визначення яких з кваліфікуючими ознаками закріплено в нормах законопроекту.

В законопроекті також визначено мету зустрічей: 1) пояснення політики і рішень; 2) надання інформації про плани, тактику і стратегію щодо вирішення конкретного питання; 3) визначення пріоритетів діяльності; 4) надання інформації про результати діяльності депутата ради, органів і посадових осіб місцевого самоврядування за визначений період; 5) збір та аналіз інформації про оцінку територіальною громадою ефективності запропонованого органами і посадовими особами місцевого самоврядування, депутатом ради шляху вирішення питання; 6) збір та аналіз інформації щодо думок і побажань територіальної громади стосовно вирішення певних питань суспільного життя; 7) отримання інформації про підтримку територіальною громадою рішення чи плану виконання для представлення і захисту інтересів територіальної громади перед іншими органами та їх посадовими особами; 8) забезпечення та формування нових механізмів прозорості у діяльності органів і посадових осіб місцевого самоврядування, депутатів рад з метою підвищення довіри.

При цьому зазначені цілі не пов'язані із конкретною сферою повноважень, що надає можливість поширити такий інструмент інформаційної взаємодії на всі сфери, щодо яких депутати ради, органи та посадові особи місцевого самоврядування мають відповідні повноваження.

Законопроектом передбачено правові норми, які встановлюють вимоги щодо змісту інформації, яка має оприлюднюватись при ініціюванні та скликанні будь-якої форми зустрічі, вимоги до протоколу зустрічі – як результату їх проведення, а також складання звітів про результати їх розгляду і врахування.

У законопроекті запропоновано визначення громадської експертизи на місцевому рівні, адаптоване з урахуванням особливостей здійснення місцевого самоврядування: “громадська експертиза діяльності органів місцевого самоврядування (далі громадська експертиза)” – це процес, метою якого є отримання оцінки діяльності органів та посадових осіб місцевого самоврядування, депутатів за результатами відповідного дослідження та підготовка експертних пропозицій щодо розв'язання суспільно значущих проблем для їх подальшого врахування.

Крім того, запропоновано правовий механізм, яким структуровано процес громадської експертизи за етапами: ініціювання; розгляд пропозиції; підстави для відмови; призначення; порядок проведення; результати; розгляд звіту та його врахування; які охоплюють всі етапи реалізації зазначеного інструменту на практиці.

Передбачено право органів та посадових осіб призначати громадську експертизу – що є новелою даного законопроекту, оскільки в умовах кадрового і ресурсного обмеження органів і посадових осіб місцевого самоврядування залучення громадян та їх об'єднань забезпечить раціональне використання обмежених ресурсів та сприятиме виробленню проекту рішення, який достатньою мірою буде відображати інтереси населення.

При цьому передбачено урівноважуючий правовий механізм, який дозволить запобігти призначенню громадських експертиз, як важелю політичного впливу або тиску серед представників місцевої влади. Законопроект визначає суб'єктів та предмети, щодо яких органи і посадові особи місцевого самоврядування уповноважені призначати громадську експертизу.

Визначено чіткі правові підстави для відмови у проведенні громадської експертизи, такі як: 1) предмет або мета не відповідають законодавству; 2) предмет виходить за межі компетенції відповідного органу місцевого самоврядування та її виконавчого комітету; 3) запит або пропозиція щодо проведення громадської експертизи не відповідає

вимогам; 4) не досягнуто згоди про об'єднання та спільне проведення громадської експертизи за умов, зазначених в у законопроекті.

Вичерпне закріплення правових підстав для відмови створить умови для виключення вільного тлумачення та зловживань органів і посадових осіб при вирішенні питання призначення громадської експертизи.

Вочевидь, становлення та розвиток громадянського суспільства повинні відбуватись, в першу чергу, саме на місцевому рівні, оскільки органи місцевого самоврядування є найближчою до громадянина ланкою у системі публічного управління. У зв'язку із децентралізацією місцеві органи різних рівнів отримують додаткові повноваження та ресурси, а тому врахування інтересів громади, щодо їх розподілу актуалізується. А відтак саме удосконалення правового регулювання інструментів інформаційної взаємодії на місцевому рівні дозволить посилити виявлення волі народу через механізми прямої демократії.

Висновки.

Якість прийнятих рішень безпосередньо залежить від якості правового регулювання обігу інформації, який відбувається між всіма суб'єктами місцевого самоврядування.

Для удосконалення процесу обігу інформації досліджено правову модель інформаційної взаємодії, в процесі чого було виявлено ряд специфічних термінів, які виникли у зв'язку із використанням класичних термінів інформаційного права у предметній сфері – місцевому самоврядуванні.

Система термінів інформаційного права має універсальний характер та високий ступінь абстрагування, що забезпечує їх використання у будь-якій предметній сфері, але за умови певної адаптації.

Для вдосконалення правового регулювання інформаційної взаємодії нормами інформаційного права пропонується внести відповідні зміни до Закону України “Про місцеве самоврядування” та закріпити їх у відповідних розділах, а статтю 1 доповнити такими термінами: “інформаційна взаємодія у місцевому самоврядуванні”, “інформаційні продукти суб'єктів місцевого самоврядування”, “оприлюднення інформації суб'єктів місцевого самоврядування”, “інструмент інформаційної взаємодії”.

Для подальшого удосконалення законодавства у сфері місцевого самоврядування доцільно використовувати підхід, за допомогою якого можливо закріпити права та обов'язки всіх суб'єктів на всіх етапах обороту інформації із зазначенням критеріїв форми та змісту інформаційних продуктів, які утворюються в результаті такої діяльності та інструментів, за допомогою яких здійснюється така взаємодія.

Завдяки застосуванню модельного підходу до удосконалення Закону України “Про місцеве самоврядування” будуть створені умови для забезпечення однаковості реалізації державної політики зміцнення демократичних форм участі громад в управлінні місцевими справами на основі інформаційної взаємодії з одночасною можливістю враховувати на рівні підзаконних актів регіональні та місцеві особливості.

Використана література

1. Баранов О.А., Дубняк М.В. Зміцнення прямої демократії на місцевому рівні шляхом удосконалення правового регулювання інформаційної взаємодії / Європейський політико-правовий дискурс : в 3-х вип. – [Вип. 3]. – 2017. – № 4. – С.109-117.
2. Апт Л.Ф., Дорофеева Т.А. Методические рекомендации по формированию понятийного аппарата законопроекта // Юридический вестник. – 2009. – № 3-4. – С. 64-70.
3. Хворостянкін А. Дефініції в законодавчих текстах : питання теорії // Право України. – 2005. – № 11. – С. 28-32. – Режим доступу : <http://old.minjust.gov.ua/6669>

4. Волкова В.Н. Теория информационных процессов и систем : учебник и практикум для бакалавриата. – М. : Из-во Юрайт, 2014. – 502 с. – (Сер. Бакалавр. Академический курс). – Режим доступа : http://stud.com.ua/34384/informatika/informatsiyni_potrebi_informatsiynye_obs_lug_ovuvannya
5. Безруков А.С. Правовая модель как инструмент юридической науки и практики : дис. на соискание ученой степени к.ю.н : 12.00.01 / Алексей Сергеевич Безруков, 2008. – 151 с. – Режим доступа : <http://lawtheses.com/pravovaya-model-kak-instrument-yuridicheskoy-nauki-ipraktiki#ixzz4KWmGRhq3>
6. Дубняк М.В. Соціально-правова модель прийняття рішень у місцевому самоврядуванні // Право і суспільство. – 2017. – № 1. – С. 149-153.
7. Інструменти. Wikipedia – вільна енциклопедія – Режим доступа : <https://uk.wikipedia.org/wiki/%D0%86%D0%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82>
8. Міжнародний стандарт бухгалтерського обліку 32 (МСБО-32) фінансові інструменти : подання. – Режим доступа : [//zakon3.rada.gov.ua/laws/show/929_029](http://zakon3.rada.gov.ua/laws/show/929_029)
9. Основні засади діяльності прес-служб органів державної влади та місцевого самоврядування : світовий та український досвід : довідник ; під. наук. кер. О.С. Поважного. – Донецьк : ДонДУУ, 2011. – 96 с.
10. Брижко В.М. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / В.М. Брижко, О.М. Гальченко та ін. ; за ред. Р.А. Калюжного та М.Я. Швеця. – К. : “Інтеграл”, 2002 р. – 220 с.
11. Про інформацію : Закон України від 02.10.92 р. № 2657-ХІІ ; станом на 01.01.17 р. // Відомості Верховної ради України (ВВР). – 1992. – № 48. – Ст. 650. – Режим доступа : <http://zakon2.rada.gov.ua/laws/show/2657-12>
12. Перов Д.О. Склад інформаційних правовідносин / Актуальні проблеми держави і права. – 2014. – № 71. – С. 88-95. – Режим доступа : <http://apdr.in.ua/index.php/vipusk-71.html>
13. Баранов О.А. Правове забезпечення інформаційної сфери : теорія методологія і практика: монографія / О.А. Баранов. – К. : Едельвейс, 2014. – 434 с.
14. Дубняк М.В. Теоретико-методологічні положення реалізації інформаційних правовідносин у місцевому самоврядуванні // Науковий вісник Херсонського державного університету. – (Серія “Юридичні науки”). – 2016. – № 5. – Т. 2. – С. 43-46.
15. ГОСТ 7.0-99. Информационно-библиотечная деятельность, библиография. Термины и определения. – Минск : ИПК Издательство стандартов, 1999. – 23 с.
16. Варенко В.М. Інформаційно-аналітична діяльність : навч. посіб. / В.М. Варенко. – К. : Університет “Україна”, 2014. – 417 с.
17. Назар Ю.С. Взаємодія органів внутрішніх справ із місцевими органами виконавчої влади та органами місцевого самоврядування у профілактиці адміністративних правопорушень : монографія / Ю.С. Назар. – Львів : Львівський державний університет внутрішніх справ, 2012. – 160 с.
18. Спиркин А.Г. Взаимодействие / А.Г. Спиркин. – (БСЭ). – [3-е изд.]. – М., 1971. – Т. 5. – С. 8.
19. Організація управління персоналом в органах внутрішніх справ : монографічне дослідження / [В.Д. Сущенко, А.М. Смирнов, О.І. Коваленко, А.А. Смирнов]. – К.: Національна академія внутрішніх справ України, 1999. – 352 с.
20. Місюра В.Я. Особливості взаємодії політичних партій та органів місцевого самоврядування в розбудові громадянського суспільства в Україні (державно-управлінський аспект) : автореф. дис на здобуття наук. ступеня канд. наук. з державного управління : за спец. 25.00.02 – механізм державного управління / Вадим Ярославович Місюра. – К., 2006. – 19 с. – Режим доступа : http://academy.gov.ua/NMKD/library_nadu/Avtoreferat/382b971e-99a4-4f2f-a916-0e760422b318.pdf
21. Економічний аналіз : навч. посіб. / [М.А. Болнох, В.З. Бурчевський, М.І. Горбаток та ін.] ; за ред. М.Г. Чумаченка. – К. : КНЕУ, 2001. – 540 с.

22. Великий тлумачний словник сучасної української мови ; уклад. і голов. ред. В.Т. Бусел. – К. : Ірпінь, 2001.

23. Сігаєва Т.Є. Інформаційна взаємодія підприємства з суб'єктами зовнішнього середовища в процесі інвестування : автореф. дис. на здобуття наук. ступеня канд. економічних. наук : за спец. 08.00.04 – економіка та управління підприємством. – Харків, 2010. – 22 с.

24. Ястремсяка О. Інформаційна взаємодія суб'єктів господарювання на основі іміджу // Вісник КНУ ім. Т. Шевченка. – (Серія Економіка). – №.137/2012. – С. 59-63.

25. Про місцеве самоврядування : Закон України від від 21.05.97 р. № 280/97-ВР ; станом на 04.06.17 р. // Відомості Верховної Ради України (ВВР). – 1997. – № 24. – Ст. 170. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80>

~~~~~ \* \* \* ~~~~~

УДК 342.311:351.

НИКОЛАЄНКО Г.В., аспірантка НДІ інформатики і права НАПрН України

## ТЕОРЕТИЧНІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ ДЕРЖАВНОЇ СТАТИСТИКИ В УКРАЇНІ

**Анотація.** *Стаття присвячена розробці проблеми правового регулювання функціонування системи державної статистики в Україні. Здійснено теоретичне обґрунтування специфічності діяльності у цій сфері, зокрема доведено, що особливістю правового регулювання державної статистики в Україні є використання органами державної влади та органами місцевого самоврядування всього комплексу національних та міжнародних нормативно-правових актів, що діють у сфері державного статистичного обліку.*

**Ключові слова:** *статистична діяльність; інформаційні відносини; принципи статистики.*

**Аннотация.** *Статья посвящена разработке проблемы правового регулирования функционирования системы государственной статистики в Украине. Осуществлено теоретическое обоснование специфичности деятельности в этой сфере, а именно доказано, что особенностью правового регулирования государственной статистики в Украине является использование органами государственной власти и органами местного самоуправления всего комплекса национальных и международных правовых актов, которые действуют в сфере государственного статистического учета.*

**Ключевые слова:** *статистическая деятельность, информационные отношения, принципы статистики.*

**Summary.** *This article is devoted to development of the problem of legal regulation of the state statistics system in Ukraine. The author provides theoretical justification for the specificity of activity in this area, proving, in particular, that feature of the state statistics regulation in Ukraine is state authorities and local authorities using the entire complex of national and international regulations in force in the State statistical records.*

**Постановка проблеми.** Специфіка функціонування державної статистики, а також стратегічні імперативи її розвитку визначаються, насамперед, особливостями соціально-економічного розвитку країни та її суспільно-політичним устроєм. Формування вітчизняної системи державного статистичного обліку почалося з набуттям незалежності України і супроводжувалося створенням не лише її правових основ, але й власної наукової та методологічної бази. Цьому сприяла значна активізація співпраці із провідними міжнародними статистичними центрами та відповідними службами європейських країн. В Україні, як і в більшості європейських країн, акцентується увага саме на державній статистиці, чим виділяється офіційний характер даного виду управлінської діяльності в якості необхідної умови розвитку країни в сучасних цивілізаційних умовах.

Специфічність статистичної інформації і, відповідно, – діяльності у цій сфері, вимагає наукового аналізу та вирішення актуальних питань щодо нормативного забезпечення організації державного статистичного обліку, організаційних форм забезпечення державної статистики в Україні, аналізу цієї проблеми за допомогою сучасних методологічних підходів. Разом з цим, ефективність державної статистики в Україні визначається досконалістю її правової основи, тому вивчення проблем становлення та розвитку нормативної регламентації офіційної статистичної діяльності є актуальним як у теоретичному, так і в прикладному аспекті.

**Результати аналізу наукових публікацій.** Найбільш числену групу спеціальних досліджень проблем державного статистичного обліку складають роботи, в яких статистика розглядається в якості інституту економічної теорії, що видається цілком виправданим з огляду на те, що в основу статистики як науки покладено складну систему економіко-математичних розрахунків.

Якщо розглядати проблематику державної статистики в якості галузі адміністративно-правового регулювання, то питома вага спеціальних досліджень залишається вкрай недостатньою. Насамперед, необхідно відзначити дисертаційне дослідження А. Кондратьєва [1], в якому автором наведено визначення адміністративно-правового регулювання державної статистики в Україні як у широкому, так і вузькому розумінні. У широкому сенсі адміністративно-правове регулювання державної статистики в Україні полягає в адмініструванні органами державної влади порядку подання або використання даних державних статистичних спостережень відповідно до принципів офіційного статистичного обліку. У вузькому значенні адміністративно-правове регулювання державної статистики в Україні – це процес упорядкування організації і діяльності суб’єктів офіційного статистичного обліку та формування стійкого правового порядку їх функціонування з використанням інформаційно-комунікаційних технологій та електронного документообігу.

О. Довганем [2] досліджувалися правові засади формування і розвитку системи забезпечення інформаційної безпеки України та її складових. Автором було обґрунтовано і запропоновано шляхи правового вдосконалення інформаційної безпеки, а також правових механізмів формування системи безпеки та захисту інформаційних ресурсів, у контексті розвитку інформаційної сфери суспільства.

О. Барановим [3] запропоновано і обґрунтовано авторське визначення об’єкту правовідносин в інформаційній сфері як матеріальні та нематеріальні блага, що представлені у вигляді: інформаційних продуктів, особистих паперів, документів, особистих нематеріальних благ, послуг і робіт, а також їх результатів, результатів поведінки і дії в процесі обігу інформації або забезпечення цього обігу, та задовольняють потреби і інтереси, як суб’єктів цих правовідносин, що діють в рамках своїх юридичних прав і обов’язків, так і інших суб’єктів.

К. Галинською наведено поняття адміністративно-правового забезпечення інформаційного правопорядку як здійснюване державою комплексне нормативне упорядкування інформаційно-публічних відносин, їх законодавче закріплення, здійснення охорони з використанням заходів адміністративного примусу: а) попередження, б) припинення, в) відповідальності [4].

Таким чином, незважаючи на наявність досліджень проблем регулювання інформаційної сфери, багато її аспектів, зокрема питання правового забезпечення функціонування державної статистики в Україні потребує подальшої конкретизації та розвитку.

**Метою статті** є дослідження основ правового регулювання державної статистики в Україні та встановлення закономірностей розвитку вітчизняної системи статистичного обліку.

**Виклад основного матеріалу.** В період трансформації економічної та соціальної системи суспільства, підсистемою якої є, в свою чергу, національна статистика, формування інформаційної системи набуває специфічних рис, оскільки значно підвищується рівень відкритості й динамізму новостворюваної системи [5]. Розвиток такої системи повністю корелює з інтенсивністю впливу зовнішніх чинників та віддзеркалює діалектику її розвитку. Взагалі, система вважається сталою, лише тоді, коли між її елементами утворюється взаємозв’язок, коли нова якість набуває незворотного характеру.

Реалізація системного підходу до формування державної статистики передбачає наявність такого важливого етапу, як концептуалізація її правового регулювання. На перший погляд, маючи власний і вивчивши зарубіжний практичний досвід функціонування системи статистичного обліку, а також беручи до уваги відповідні рекомендації міжнародних статистичних служб, можна було б безпосередньо впроваджувати останні у національну статистичну практику. Однак автоматичне перенесення міжнародних стандартів на національний ґрунт в умовах перехідної економіки на концептуальному рівні може призвести до результатів, які прямо протилежні очікуваним.

Основними елементами системи правового регулювання є, перш за все, норми права – загальнообов’язкові, формально визначені правила поведінки, які встановлені або санкціоновані державою та забезпечені її примусовою силою [6, с. 39]. Нормативно-правові акти, що врегульовують відносини у сфері державної статистичної діяльності, можна класифікувати наступним чином: міжнародні нормативні акти; нормативно-правові акти загального характеру, що регулюють організацію державного статистичного обліку в Україні; спеціальні нормативно-правові акти, що регулюють діяльність органів державної влади та недержавних установ щодо збору, обробки та надання статистичних даних.

Щодо міжнародних документів, то статистичною комісією ООН у 1994 році було схвалено Основні принципи офіційної статистики (UN Fundamental Principles of Official Statistics). Вони визначали загальні підходи та засадничі принципи, яких мали дотримуватися державні статистичні служби: значимість, об’єктивність, загальнодоступність; професійні стандарти і етика; підзвітність і транспарентність; недопущення нецільового використання; конфіденційність; законність; національна координація; використання міжнародних стандартів; міжнародне співробітництво [7].

Іншим одним із визначальних актів міжнародного характеру, що регулюють статистичну діяльність, є Декларація якості Європейської статистичної системи (далі – Декларації якості ЄСС), яка була прийнята у 2001 рр. за ініціативи Комітету ЄС зі статистичних програм. Ця Декларація включає програмну заяву Європейської статистичної системи, виклад її концепції та Принципи, що були запозичені з наведених вище “Фундаментальних принципів офіційної статистики ООН” [8].

На основі Основних принципів офіційної статистики ООН, Декларації якості ЄСС, Керівних принципів міжнародної статистичної діяльності, з метою інтеграції інституційних систем та систем забезпечення якості (ISO 9000), у 2005 році Комітет ЄС зі статистичних програм розробив і затвердив Кодекс діяльності європейської статистики (European Statistics Code of Practice), яким встановлено основні принципи діяльності ЄСС щодо інституційного середовища, статистичних процесів і продукції європейських статистичних служб [9].

У 2009 році Європейським Парламентом було прийнято Регламент (ЄС) № 223/2009 щодо європейської статистики, яким визначено, що з метою підвищення довіри до європейської статистики національні статистичні служби повинні мати професійну незалежність і забезпечувати неупередженість і високу якість офіційної статистики згідно з принципами, викладеними у Кодексі [10].

В основу правового регулювання здійснення державної статистичної діяльності в Україні покладено нормативний аспект, що передбачає розробку та юридичне закріплення відповідних норм поведінки людей. У свою чергу, нормативна регламентація державної статистики виходить із сутності предметної області статистичної науки, якою виступає комплекс взаємообумовлених дисциплін, що

вивчають кількісні характеристики соціально-економічних явищ і процесів, характерних для суспільного розвитку тих чи інших країн. Цей комплекс може включати:

- загальну теорію статистики, предметом дослідження якої є розробка науково обґрунтованої методології збору, контролю, обробки та аналізу інформації, що відображає кількісні характеристики досліджуваних явищ і процесів;
- математичну статистику, в основу якої покладено математико-статистичні методи аналізу та прогнозу різних суспільних явищ і процесів (найбільшого поширення набула для характеристики соціально-економічної ситуації в окремо взятій країні);
- систему національних рахунків (СНР), що відображає передумови, процеси та результати економічної діяльності з використанням системи взаємоузгоджених узагальнених економічних показників, які представлені у вигляді статистичних таблиць;
- соціально-економічну (макроекономічну) статистику, предметом дослідження якої є кількісні характеристики соціально-економічних явищ і процесів;
- галузеві статистики, що вивчають кількісні характеристики явищ і процесів в різних галузях економічного чи суспільного розвитку (статистика промисловості, статистика сільського господарства, статистика зовнішньоекономічних зв'язків, правова статистика тощо). Кожна з галузевих статистик використовує єдині методологічні принципи, що можуть базуватися на методах математичної статистики, загальної теорії статистики чи макроекономічної статистики. Разом з цим, галузеву систему показників кожна з них будує з урахуванням специфіки конкретної галузі, що підлягає статистичному вивченню.

В Україні законодавчо визначені такі принципи інформаційних відносин: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації.

Правовою основою державної статистичної діяльності є Конституція України, Закон України “Про державну статистику”, інші закони України та нормативно-правові акти, що регулюють відносини у галузі статистики, інформації, інформатизації, науково-технічної діяльності, стандартизації, а також міжнародні договори України в галузі статистики, згода на обов'язковість яких надана Верховною Радою України [11].

Закон України “Про державну статистику” (далі – базовий Закон) має на меті регулювання правових відносин в галузі державної статистики, а також визначає права і функції органів державної статистики, організаційні засади здійснення державної статистичної діяльності з метою отримання всебічної та об'єктивної статистичної інформації щодо економічної, соціальної, демографічної та екологічної ситуації в Україні та її регіонах і забезпечення нею держави та суспільства. Вказаним законодавчим актом значно конкретизуються норми щодо визначення державної статистичної діяльності – це сукупність дій, пов'язаних з проведенням державних статистичних спостережень та наданням інформаційних послуг, спрямована на збирання, опрацювання, аналіз, поширення, збереження, захист та використання статистичної інформації, забезпечення її достовірності, а також удосконалення статистичної методології. Окрім того, статистичною інформацією є також дані банківської, фінансової і митної статистики, статистики платіжного балансу тощо, які складаються на підставі адміністративних даних, отриманих Національним банком України та спеціально уповноваженими державними органами (крім органів державної статистики) відповідно до їх компетенції. Законодавство поряд із такими аспектами, як функції офіційної статистики, її роль у суспільстві, незалежність від стороннього впливу, взаємовідносини з респондентами і користувачами, формує основи статистичної

системи. Так, органами державної статистики є: центральний орган виконавчої влади, що реалізує державну політику у сфері статистики, а також функціональні органи державної статистики – підприємства, установи та організації, які знаходяться у сфері управління центрального органу виконавчої влади, що реалізує державну політику у сфері статистики.

На підставі базового Закону органи державної статистики мають право вивчати стан первинного обліку і статистичної звітності, перевіряти достовірність первинних і статистичних даних, поданих респондентами, а також застосовувати при цьому у порядку, встановленому спеціально уповноваженим центральним органом виконавчої влади у галузі статистики, метод безпосереднього відвідування виробничих, службових та інших приміщень, ділянок тощо юридичних осіб, їх філій, відділень, представництв та інших відособлених структурних підрозділів, а також громадян – суб’єктів підприємницької діяльності.

Розглядаючи питання правового забезпечення державної статистики, необхідно розрізняти поняття “законодавство” і “законодавче поле” статистичної діяльності. Під законодавством, що регулює державну статистику, доцільно розуміти сукупність законодавчих та підзаконних актів, що регламентують безпосередньо статистичну діяльність щодо визначеної сфери. В свою чергу, законодавче поле повинне регламентувати не лише певну статистичну діяльність, але й загальний статус статистики у суспільстві, діяльність окремих суб’єктів, а також формування національного інформаційного простору.

До основних компонентів сучасного статистичного законодавства належать такі:

- статистична організація має поширювати інформацію без політичного втручання за умови дотримання звичайних професійних стандартів;
- статистична організація повинна систематично поширювати інформацію;
- статистичній організації має бути гарантована незалежність від політичного контролю;
- статистична організація має запровадити регулярне звітування про свою діяльність або перед статистичною комісією, або перед Урядом чи Парламентом [12, с. 118 ].

Значну роль у регулюванні статистичних відносин відіграють нормативно-правові акти Президента України та Кабінету Міністрів України. Найбільш вагомим актом Президента України, що до 2007 року регулював порядок державного статистичного обліку, слід визнати Указ “Про Державну службу статистики України”, яким було затверджено Положення про Державну службу статистики України. Даним нормативно-правовим актом визначався статус Державної служби статистики України – це спеціально уповноважений центральний орган виконавчої влади у галузі статистики, діяльність якої спрямовується і координується Кабінетом Міністрів України через Міністра економічного розвитку і торгівлі України. Основними завданнями Держстату України стала реалізація державної політики у сфері статистики та внесення пропозицій щодо її формування [13].

Серед нормативно-правових актів можна виділити Постанову Кабінету Міністрів України “Про Концепцію побудови національної статистики України та Державну програму переходу на міжнародну систему обліку і статистики” від 04.05.93 р. [14]. В Постанові, зокрема, зазначалося, що підвищення ролі статистичних органів у вивченні соціально-економічних явищ під час переходу до ринкової економіки передбачає створення нової та удосконалення діючої статистичної методології, застосування стандартів, розроблених міжнародними статистичними організаціями.

Виходячи з Постанови Кабінету Міністрів України “Про затвердження Положення про Державну службу статистики України” від 23.09.14 р. № 481 [15], основними завданнями Держстату на сьогодні є: реалізація державної політики у сфері статистики; внесення на розгляд Міністра економічного розвитку і торгівлі пропозицій щодо забезпечення формування державної політики у сфері статистики.

Значна кількість правових норм, що регулюють статистичну діяльність, міститься у відомчих нормативних Державної служби статистики України. Серед них слід виділити Наказ Державного комітету статистики України “Про затвердження Принципів діяльності органів державної статистики” від 14.06.10 р. № 216 [16]. Наказом визначено, що принципи діяльності органів державної статистики України – це звід стандартів у галузі статистики, дотримання яких гарантує державі та суспільству, що офіційна статистична інформація розробляється і поширюється на основі професійної незалежності, неупередженості, об’єктивності, надійності, економічності та статистичної конфіденційності. Принципами загального управління органів державної статистики визначено наступне: професійна незалежність; повноваження щодо збирання даних; відповідність ресурсів; зобов’язання щодо забезпечення якості; конфіденційність статистичних даних; неупередженість і об’єктивність; управління діяльністю та професійна етика; результативність діяльності; постійне удосконалення.

### **Висновки.**

Структура національної статистичної системи, завдання, відносини між статистичними установами, респондентами та користувачами даних, гарантії захисту конфіденційної інформації повинні обов’язково визначатися на законодавчому рівні. Дотримання даної умови зумовлюється специфікою діяльності статистичних органів у будь-якій країні, а названі елементи є загальними основоположними принципами функціонування національних статистик. При регулюванні відносин у сфері державного статистичного обліку термін “закон” вживається в якості узагальнюючого поняття, при цьому розуміються усі нормативні акти, які мають силу закону, до яких належать й основи законодавства, статuti, кодекси, положення та інші акти, які приймаються Верховною Радою України.

Державна статистика повинна розглядатися в якості упорядкованої системи, елементами якої виступають: звід офіційних документованих даних; діяльність відповідних органів державної влади як складова державного управління; органи Державної служби статистики України. Наведена система визначає предмет офіційної державної статистики в Україні та основоположні засади її правового регулювання.

Загалом проблема формування правового поля у державній статистичній діяльності вирішується на двох рівнях. Перший – це послідовна і комплексна адаптація європейських актів і формування пакету національних нормативних документів. Другий – це подальше розроблення пакету внутрішньосистемних регламентів, інструкцій та методик стосовно статистичної діяльності, які повністю узгоджуються з нормативними актами першого рівня і є обов’язковими для використання в органах державної статистики.

### **Використана література**

1. Кондратьєв А.Ю. Адміністративно-правове регулювання державної статистики в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / Андрій Юрійович Кондратьєв. – Запоріжжя : Державний вищий навчальний заклад “Запорізький національний університет Міністерства освіти і науки України”, 2015. – 20 с.

2. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації : теоретико-правові та організаційні аспекти : монографія / О.Д. Довгань. – К. : НБУ ім. В.І. Вернадського, 2015. – 386 с.
3. Баранов О.А. Правове забезпечення інформаційної сфери : теорія, методологія і практика : монографія / О.А. Баранов. – К. : Едельвейс, 2014. – 434 с.
4. Галинська К.Ю. Адміністративно-правове забезпечення інформаційного правопорядку в Україні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / Каріна Юріївна Галинська. – К. : НДІ інформатики і права НАПрН України, 2016. – 17 с.
5. Осауленко О.Г. Моделювання сталого розвитку соціально-економічних систем : монографія / О.Г. Осауленко. – К. : 2001. – 66 с.
6. Загальна теорія держави і права ; за ред. В.В. Копейчикова. – К. : Юрінком, 1997. – 320 с.
7. Fundamental Principles of National Official Statistics. – Режим доступу : <https://unstats.un.org/unsd/dnss/gp/fundprinciples.aspx>
8. ESS Quality Declaration. – Режим доступу : <http://ec.europa.eu/eurostat/documents/64157/4392716/quality-declaration-ESS.pdf>
9. European Statistics Code of Practice. – Режим доступу : <http://ec.europa.eu/eurostat/web/quality/european-statistics-code-of-practice>
10. Правовая основа европейской статистики. – Режим доступу : <http://www.cisstat.com/rus/event/335.pdf>.
11. Про державну статистику : Закон України. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2614-12>
12. Осауленко О.Г. Національна статистична система : стратегічне планування, методологія та організація : монографія / О.Г. Осауленко. – К. : ДП “Інформ.-аналіт. Агентство”, 2008. – 415 с.
13. Про Державну службу статистики України : Указ Президента України. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/396/2011>
14. Про Концепцію побудови національної статистики України та Державну програму переходу на міжнародну систему обліку і статистики : Постанова Кабінету Міністрів України від 04.05.93 р. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/326-93-п>
15. Про затвердження Положення про Державну службу статистики України : Постанова Кабінету Міністрів України від 23.09.14 р. № 481. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/481-2014-п>
16. Про затвердження принципів діяльності органів державної статистики : Наказ Державного комітету статистики України від 14.06.10 р. № 216. – Режим доступу : [http://www.ukrstat.gov.ua/prc\\_dk/prc\\_ddos.htm](http://www.ukrstat.gov.ua/prc_dk/prc_ddos.htm)

~~~~~ \* \* \* ~~~~~


Правова інформатика

УДК 002.6:004:340.1+316.329.8

БАРАНОВ О.А., доктор юридичних наук, с.н.с.,
керівник Центру теоретико-правових проблем
інформаційної сфери НДІ інформатики і права НАПрН України

ІНТЕРНЕТ РЕЧЕЙ (IoT): ПРАВОВІ МОДЕЛІ ВИКОРИСТАННЯ ОБМЕЖЕНОГО РАДІОЧАСТОТНОГО РЕСУРСУ (Частина I)

Анотація. Аналізується генезис правового регулювання використання радіочастотного ресурсу для надання послуг електронних комунікацій. Досліджуються теоретико-методологічні засади формування правових моделей використання обмеженого радіочастотного ресурсу в умовах інтернету речей на основі вивчення соціальної моделі сфер діяльності суб'єктів з використанням послуг електронних комунікацій та соціальної моделі системи надання послуг електронних комунікацій.

Ключові слова: модель, радіочастотний ресурс, електронні комунікації, правове регулювання, бізнес-модель, спільне користування, послуги, Інтернет речей.

Аннотация. Анализируется генезис правового регулирования использования радиочастотного ресурса для предоставления услуг электронных коммуникаций. Исследуются теоретико-методологические основы формирования правовых моделей использования ограниченного радиочастотного ресурса в условиях Интернета вещей на основе изучения социальной модели сфер деятельности субъектов с использованием услуг электронных коммуникаций и социальной модели системы предоставления услуг электронных коммуникаций.

Ключевые слова: модель, радиочастотный ресурс, электронные коммуникации, правовое регулирование, бизнес-модель, совместное пользование, услуги, Интернет вещей.

Summary. The genesis of the legal regulation of the use of radio frequency resources for the provision of electronic communication services is analyzed. The theoretical and methodological foundations of the formation of legal models for the use of a limited radio frequency resource in the conditions of the Internet of Things are studied on the basis of the study of the social model of spheres of activity of subjects using the services of electronic communications and the social model of the system of providing electronic communications services.

Keywords: model, radio frequency resource, electronic communication, legal regulation, business model, shared use, services, Internet of Things.

Постановка проблеми. В умовах широкого поширення технологій Інтернету речей (IP, Internet of Things, IoT), на думку експертів, кількість об'єктів, підключених до мережі Інтернет, до 2025 року може досягти 100 млрд, при цьому значна їх частина буде генерувати великий обсяг даних, що будуть передаватись за допомогою бездротових телекомунікацій. При цьому прогнозується, що трафік передачі даних мобільних операторів зросте на три порядки (в 1000 разів) [1; 2], отже, значно збільшиться навантаження на різні діапазони радіочастотного ресурсу (далі – РЧР), що призведе до різкого зростання актуальності вирішення проблеми ефективного користування обмеженим РЧР.

Кілька десятиліть тому з проблемою неефективності використання РЧР першими зіткнулися окремі держави, які проводили лібералізацію ринку надання послуг комунікацій, заснованих на використанні радіотехнологій. Причини неефективності були закладені практично з самого початку винаходу і використання радіотехнологій та зводяться до наступних: хаотичний і необґрунтований розподіл окремих діапазонів РЧР для різних радіослужб і радіотехнологій [3]; задіяння “витратних”, з точки зору використання спектру, радіотехнологій (недосконалість технічних засобів передачі і прийому радіосигналів, значні позасмугові випромінювання; неоптимальні методи і способи обробки та модуляції сигналів тощо); недосконалість правового регулювання користування РЧР.

Крім того, досить давно стало зрозумілим, що використання РЧР не може обмежуватися тільки національним правовим регулюванням, а також вимагає пильної уваги до транскордонних і міжнародних аспектів внаслідок особливостей характеристик поширення радіохвиль, міжнародного характеру ринків послуг, що базуються на використанні радіозв'язку, і, нарешті, необхідності уникати шкідливих перешкод між радіослужбами різних держав.

Протягом декількох десятиліть Міжнародний союз телекомунікацій (ITU), Європейський Союз, національні Адміністрації зв'язку та Національні регуляторні органи в сфері телекомунікацій (електронних комунікацій) докладають значних зусиль з пошуку шляхів вирішення проблеми забезпечення гармонізованого ефективного користування окремими діапазонами радіочастотного ресурсу. Як правило, раніше ці зусилля зводилися до проведення регуляторних (правових), організаційних, інженерних та інженерно-технічних заходів. Звичайно, перш за все пошук підвищення ефективності користування радіочастотним ресурсом спрямовується в технічному напрямі. Операторами електронних комунікацій стали інтенсивно впроваджуватися нові радіотехнології, які мали кращі характеристики радіосигналів, що дозволяло передавати значні обсяги даних на одиницю спектра та надало потенційні можливості для обслуговування більшої кількості користувачів. Але задіяння технічного потенціалу не дозволило повною мірою вирішити проблему підвищення використання РЧР.

Тому зростання протягом трьох останніх десятиліть споживчих очікувань і вимог до обсягу, переліку та якості послуг електронних комунікацій, що базуються на радіотехнологіях, стимулювало появу прогресивних бізнес-моделей діяльності операторів електронних комунікацій (далі – оператор) в частині користування окремими діапазонами РЧР. Вочевидь кардинальна зміна користувацьких вимог до послуг електронних комунікацій, яка обумовлена появою і функціонуванням технологій IP, буде мати наслідком необхідність створення нових бізнес-моделей діяльності операторів електронних комунікацій, що власне обумовлює актуальність дослідження правових моделей користування діапазонами РЧР з метою їх удосконалення як одного з основних механізмів підвищення ефективності цього користування.

Результати аналізу наукових публікацій Дослідження в області ефективного використання радіочастотного ресурсу в сучасних умовах знайшли відображення в роботах ряду авторів і організацій: Forge S., Шалагінова А., ITU, Європейський парламент, Ofcom, Cisco, Qualcomm та інших.

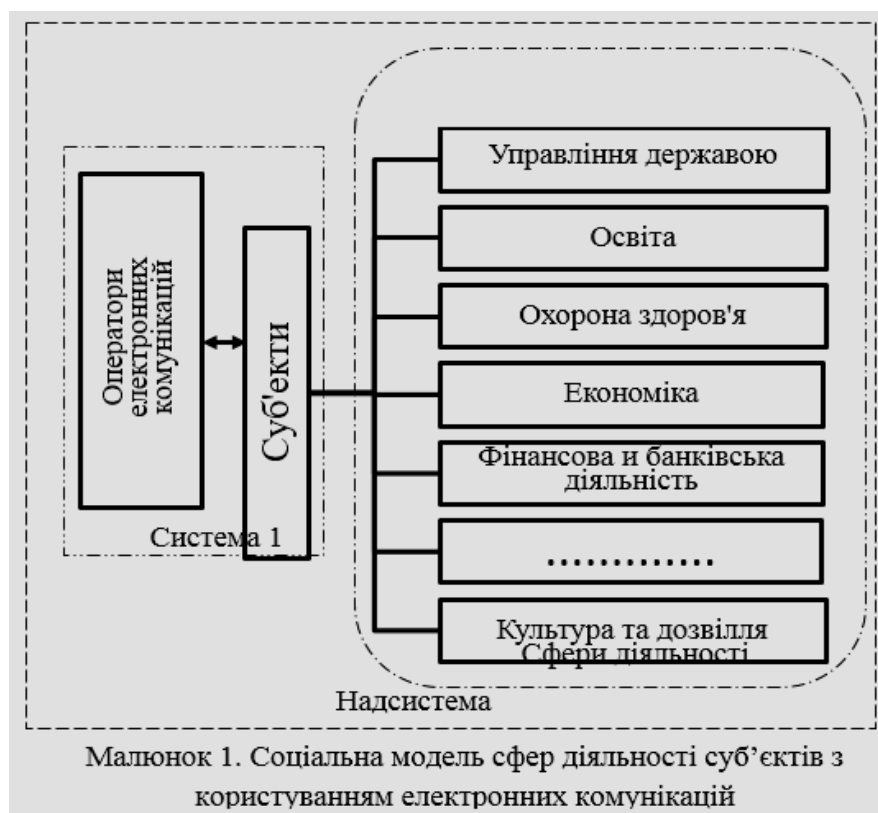
Метою статі є визначення теоретико-методологічних засад формування правових моделей використання обмеженого радіочастотного ресурсу в умовах Інтернету речей.

Виклад основного матеріалу. Проблеми правового регулювання використання РЧР методологічно доцільно досліджувати, як і будь-які інші правові проблеми, вивчаючи соціальні моделі предметної сфери і правові моделі, які є надбудовою для цих

соціальних моделей. При цьому будемо вважати, що визначення і локалізація проблем, в тому числі правових, пошук причин їх виникнення та шляхів вирішення буде більш ефективним, якщо це здійснювати не тільки в рамках досліджуваної соціальної системи деякої предметної сфери, але також в межах соціальної надсистеми вищого порядку, яка включає в себе досліджувану систему у всьому різноманітті її взаємозв'язків з іншими складовими цієї надсистеми. Це відповідає основному принципу системного підходу: аналіз проблеми слід проводити з урахуванням системи більш високого рівня, ніж та, в якій ця проблема має місце.

Для даної теми досліджень соціальна модель, яка потребує вивчення – це соціальна модель системи надання послуг електронних комунікацій, а надсистемою є соціальна система сфер діяльності суб'єктів з використанням послуг електронних комунікацій як сукупність операторів електронних комунікацій, суб'єктів і сфер діяльності цих суб'єктів. На малюнку 1 зображена соціальна модель сфер діяльності суб'єктів з використанням послуг електронних комунікацій (надсистема) зі складовим елементом – соціальною моделлю системи надання послуг електронних комунікацій (система 1).

У соціальній моделі (Мал. 1): суб'єкти – це будь-які фізичні або юридичні особи, які виявляють свою активність в різних сферах діяльності та можуть бути споживачами послуг електронних комунікацій; оператори електронних комунікацій – це господарюючі суб'єкти, які відповідно до національного законодавства отримали право на надання загальнодоступних послуг електронних комунікацій, в тому числі, мобільних; сфери діяльності – це сфери державної, ділової, професійної, особистої і будь-якої іншої активності суб'єктів, яка може або повинна здійснюватися з використанням послуг електронних комунікацій, в тому числі, мобільних.



Істотний вплив на зміст і ефективність суспільних процесів, що відображаються соціальною моделлю діяльності суб'єктів з використанням послуг електронних комунікацій, здійснюють закономірності розвитку і особливості діяльності її трьох складових:

- система управління, регулювання та використання РЧР;
- оператори електронних комунікацій;
- суб’єкти.

Кожна з цих трьох складових може бути відображена відповідною соціальною моделлю.

Соціальна модель системи управління, регулювання та використання РЧР повинна описувати суспільні процеси у сукупності міжнародних і національних інституцій, що мають повноваження у сфері використання РЧР, операторів електронних комунікацій, які користуються окремими діапазонами або номіналами частот РЧР, та суб’єктів.

Зміст суспільних процесів в системі управління, регулювання та використання РЧР детермінується положеннями міжнародного права і національного законодавства. Останнє, в свою чергу, формується з метою задоволення суспільного інтересу в наявності системи електронних комунікацій як технологічної складової інформаційної сфери України, основи функціонування та розвитку всіх сфер життєдіяльності особистості, суспільства і держави на базі використання інформаційно-комп’ютерних технологій.

Соціальна модель операторів електронних комунікацій може бути представлена у вигляді опису бізнес-моделі їх діяльності як суб’єктів ринку електронних комунікацій, що користуються частиною РЧР. При цьому зміст суспільних процесів детермінується в основному положеннями національного законодавства, а також, в деяких випадках, положеннями міжнародного права. Крім того, зміст суспільних процесів детермінується цілями і інтересами як в цілому ринку електронних комунікацій, так і окремих операторів або груп операторів.

Соціальна модель суб’єктів як користувачів послуг електронних комунікацій практично зводиться до опису користувацьких вимог (очікувань) до номенклатури, змісту та якості цих послуг, які формуються під впливом особливостей їх діяльності в різних сферах соціального життя.

На Мал. 2 наведена історично сформована соціальна модель системи управління, регулювання та користування РЧР, яку складено на прикладі України. Внаслідок подібності змісту багатьох соціальних процесів, які мають місце у сфері використання РЧР, в багатьох країнах, з тією чи іншою мірою наближення, соціальні моделі системи управління, регулювання та користування РЧР схожі на модель, зображену на Мал. 2.

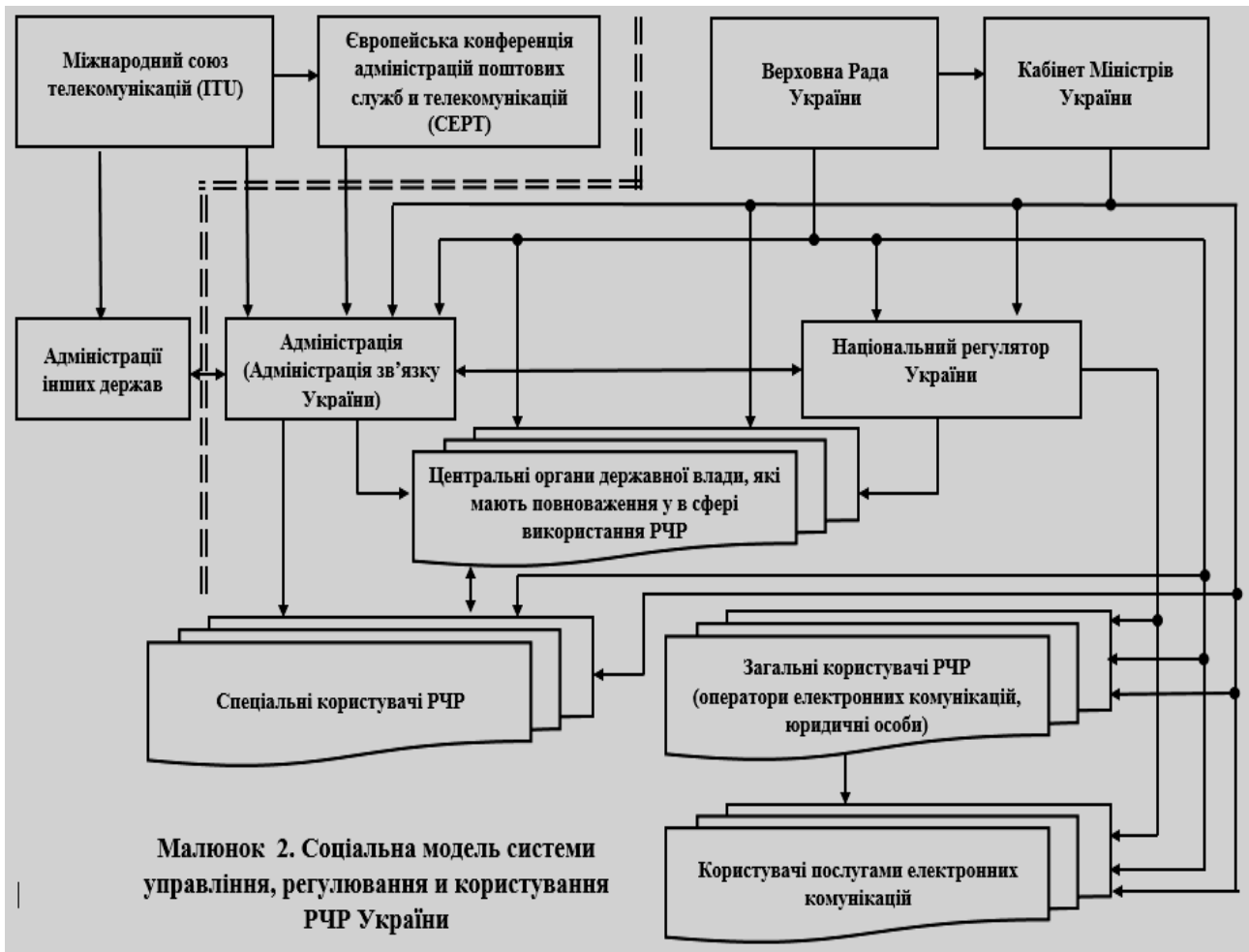
Ця соціальна модель включає в якості основних складових: Міжнародний союз телекомунікацій (ІТУ), Європейську конференцію адміністрацій поштових служб і телекомунікацій (СЕРТ), Верховну Раду України, Кабінет Міністрів України, державні органи управління та регулювання користування радіочастотним ресурсом України та інших країн, центральні органи державної влади, що мають повноваження у сфері використання РЧР, спеціальних користувачів РЧР, загальних користувачів РЧР, в тому числі, операторів електронних комунікацій, що використовують радіотехнології для надання послуг електронних комунікацій і суб’єктів (споживачів послуг).

Державні органи управління використання РЧР, відповідальні за виконання зобов’язань, визначених Статутом, Конвенцією Міжнародного союзу телекомунікацій та Адміністративними регламентами, прийнято називати Адміністрацією [4], а державні органи регулювання використанням РЧР – Національним регулятором.

Зміст суспільних процесів взаємодії всіх елементів соціальної моделі (Мал. 2) детермінується положеннями міжнародного права та національного законодавства (для України це закони “Про телекомунікації” та “Про радіочастотний ресурс”).

Соціальна модель системи управління, регулювання та користування РЧР після трансформації 80-90 років минулого століття практично до сьогодення залишається в основному стабільною. Однак, функції, повноваження та обов’язки

складових цієї системи періодично зазнають змін, адаптуючись до мінливих цілей та умов функціонування як глобального ринку електронних комунікацій, так і локальних регіональних або національних ринків.



Набагато більш динамічні зміни відбуваються з бізнес-моделями діяльності операторів електронних комунікацій як відповідь на виклики, пов'язані зі змінами користувацьких вимог, іноді дуже кардинальними, з боку суб'єктів (споживачів послуг).

Протягом близько 40 останніх років в рамках соціальної моделі (Мал. 1) діяльність операторів стільникових електронних комунікацій, які користуються РЧР, в основному була зорієнтована на надання послуг суб'єктам, які використовують поодинокі кінцеві пристрої (мобільні термінали).

До кінця 90-х років минулого століття світовий ринок загальнодоступних послуг електронних комунікацій, в тому числі, мобільних електронних комунікацій (МЕК), розвивався в основному як ринок надання послуг голосової телефонії. Основною відмінною рисою соціальної моделі системи 1 (Мал. 1) в ці роки була орієнтованість кожного оператора МЕК на власну самостійність (автономність) при наданні послуг своїм абонентам. З урахуванням останнього, бізнес-модель діяльності операторів МЕК відповідну соціальну модель системи 1 умовно назовемо “автономна”.

Виходячи з загальнодоступності послуг МЕК, система 1 є системою масового обслуговування, тобто системою з однаковою номенклатурою, змістом і показниками якості послуг для всіх користувачів або їх окремих груп. При цьому особливості змісту активності суб'єктів в найрізноманітніших сферах діяльності не впливають на вимоги до

показників якості надання послуг МЕК. Слід зауважити, що виконання певних функцій в деяких сферах діяльності обумовлювало формування особливих вимог до показників якості послуг голосової телефонії. Але для цих випадків створювалися окремі, спеціальні мережі МЕК, які не належали до мереж загального користування.

Під впливом широкого поширення комп'ютерних та Інтернет-технологій з 2000-го року став впроваджуватися розроблений Міжнародним союзом телекомунікацій (ITU) стандарт мобільного зв'язку 3G (3 покоління), який дозволив надавати користувачам набір послуг МЕК, що об'єднують як високошвидкісний мобільний доступ до мережі Інтернет, так і технологію радіозв'язку, яка формує канал передачі даних.

Для бізнес-моделі “автономна”, в переважній більшості випадків, показники надійності і стійкості роботи мережі мобільних електронних комунікацій не є критичними, як не є критичними випадки тимчасового припинення надання послуг для конкретного користувача або навіть груп користувачів. Також для оператора не є критичною проблема надійного забезпечення географічно суцільного покриття по всій території країни для забезпечення можливості надання послуг.

Таким чином, для формального опису бізнес-моделі “автономна”, яка домінувала в світі на ринку послуг МЕК до кінця 1990-х років, характерно наступне.

А. В частині використання РЧР:

- 1) ліцензування – наявність ліцензії, виданої регулятором, – єдина підстава для користування виділеним діапазоном РЧР;
- 2) дві ліцензії – одна послуга: ліцензія на право користування РЧР видається тільки оператору, який має відповідну ліцензію на право надання послуг МЕК;
- 3) ексклюзивність – діапазоном РЧР користується тільки той оператор, якому видано ліцензію на нього;
- 4) суцільне покриття – вимога забезпечення надання послуг МЕК на всій території на яку видано ліцензію на користування РЧР;
- 5) національне покриття – прагнення мати ліцензію на право користування РЧР на всій території країни;
- 6) нераціональність – еkleктичні показники ефективності користування РЧР оператором.

У більшості країн, що входять до ІТУ, під ліцензією розуміють спеціальний документ, що засвідчує юридичне право суб'єкта на користування частиною РЧР. Так в Регламенті радіозв'язку є імперативна норма – “жодна передавальна станція не може встановлюватися або експлуатуватися приватною особою або будь-яким підприємством без ліцензії, виданої у відповідній формі та відповідно до положень цього Регламенту урядом або від імені уряду країни, в якій знаходиться дана станція” [5]. При цьому уряд, котрий видає ліцензію на мобільну станцію або мобільну земну станцію повинен вказувати в ній в ясній формі дані про станцію, включаючи її назву, позивний і, при необхідності, категорію публічної кореспонденції, а також загальні характеристики установки. А для наземних мобільних станцій ліцензія повинна містити пункт про заборону роботи цих станцій за межами кордонів країни, що видала ліцензію.

Б. В частині мережі мобільних електронних комунікацій:

- 1) ексклюзивність – конкретна мережа МЕК, як комплекс технічних засобів електронних комунікацій і споруд, експлуатується лише одним оператором;
- 2) національне покриття – мережа мобільних електронних комунікацій для надання послуг МЕК будується по всій території країни;
- 3) невимогливість – невисокі вимоги до стабільності, надійності і стійкості функціонування мережі.

В. В частині послуг, що надаються:

- 1) однорідність – однакові вимоги до якості послуг, що надаються будь-яким оператором будь-якому користувачеві;
- 2) інваріантність – вимоги до показників якості надання послуг не залежать від особливостей сфери діяльності суб’єктів (користувачів послуг);
- 3) невимогливість – невисокі вимоги до безперервності, надійності та стійкості надання послуг;
- 4) одноманітність – потенційно однакова номенклатура послуг, що надаються всіма операторами для будь-якого з користувачів;
- 5) рівність – відносно однакова собівартість надання конкретної послуги при інших рівних умовах (ємності мережі, зони покриття, радіотехнологіях).

Однак, нові вимоги суб’єктів до послуг, що надаються, особливо, в частині мобільності, привели до необхідності вирішення проблеми можливого використання операторами ресурсів МЕК іншого оператора.

Першим прикладом такого “запозичення” ресурсів може служити використання можливостей мереж МЕК інших операторів в інтересах забезпечення роумінгу, який з’явився після 1991 року з введенням в експлуатацію нового стандарту мобільного зв’язку – 2G (друге покоління). Роумінг – це надання послуг мобільного (стільникового зв’язку) користувачеві поза зоною обслуговування “домашньої” мережі МЕК його оператора за рахунок використання ресурсів іншої (гостьової) мережі МЕК. При цьому, бізнес-модель діяльності операторів як і раніше залишалася “автономною”.

З початком процесу лібералізації в галузі телекомунікацій (початок 1990-х років), особливо, після прийняття Директиви 95/62/ЄС Європейського парламенту від 13 грудня 1995 [6], відкрилися правові можливості доступу для будь-якого оператора до інфраструктури оператора домінуючого на ринку послуг на прозорій, розумної вартості і недискримінаційній основі. Така ситуація стимулювала появу нової бізнес-моделі діяльності операторів – мобільний віртуальний мережевий оператор (MVNO, Mobile Virtual Network Operator).

На сьогодні ні практика, ні наука поки не виробили єдиного і узгодженого визначення MVNO. Одне з найбільш ранніх визначень дав регулятор Великобританії Ofcom: MVNO – підприємство, яке купує оптові мобільні послуги, але не володіє або не керує мережею МЕК [7]. Фактично мова йде про провайдинг послуг мобільного зв’язку. У матеріалах ІТУ дано таке визначення: MVNO – оператор, що надає послуги мобільного зв’язку для кінцевих користувачів, але не має державної ліцензії на використання своєї власної радіочастоти [8].

Отже, можна констатувати, що сутність бізнес-моделі MVNO полягає в використанні ресурсів мережі іншого оператора: мережевих або частотних, або тих і інших разом для надання послуг МЕК.

На розвиток бізнес-моделі MVNO вплинули дві тенденції: ринкова і регуляторна.

Ринкова пояснюється, з одного боку, бажанням оператора отримати хоча б якийсь дохід від своїх незавантажених мережевих і частотних ресурсів, надаючи їх в користування (оренду) іншому оператору, а з іншого – бажанням задовольнити такі вимоги суб’єктів, які не можуть бути задоволені в рамках надання масових загальнодоступних послуг МЕК або, іншими словами, мова йде про адаптацію показників якості послуг МЕК для конкретного функціонально і/або географічно обмеженого сегмента діяльності споживача послуг.

Регуляторна пояснюється прагненням Національного регулятора підвищити ефективність користування РЧР за рахунок пошуку нових бізнес-моделей діяльності

операторів, шляхом формування для домінуючих операторів можливих додаткових зобов'язання щодо підключення до власних МЕК сторонніх MVNO.

Починаючи з 2000 року, бізнес-модель MVNO стала застосовуватися в різних країнах з різною інтенсивністю. На сьогодні відомі 4 базових моделі MVNO: Branded Reseller MVNO, Light MVNO, Full MVNO, MVNE (Mobile Virtual Network Enabler). Крім того, завдяки новим комп'ютерним технологіям, зокрема технологіям хмарних обчислень, нещодавно з'явилася інноваційна п'ята модель віртуального MVNO (vMVNO), в якій компоненти мережевої операторської інфраструктури реалізовані на стандартному ІТ-обладнанні (дата-центри, сервери, системи зберігання даних, локальні мережі, мережі передачі даних тощо) [9; 10]. Кожна з названих бізнес-моделей має свою специфіку, але всіх їх об'єднує те, що вони орієнтовані на використання операторами MVNO мережевих ресурсів радіодоступу та частотних ресурсів іншого оператора [10].

Таким чином, з початку 2000-х років почався етап розвитку нового підходу до використання РЧР – спільне використання частини РЧР декількома операторами. Таку бізнес-модель діяльності операторів і віртуальних мобільних операторів (MVNO) назвемо “автономно-спільна”, що означає збереження основних характеристик бізнес-моделі “автономна” зі створенням правових умов для спільного використання певних частотних ресурсів, наданих в користування одному оператору іншим оператором.

Для бізнес-моделі “автономно-спільна” у порівнянні з бізнес-моделлю “автономна” є відмінності тільки в наступних пунктах.

А. В частині використання РЧР:

3) спільність – діапазоном РЧР користується не тільки той оператор, якому видано ліцензію на нього, а й інший, який не має ліцензії;

4) суцільне покриття або локальне покриття – вимога забезпечення надання послуг МЕК на всій території, на яку видано ліцензію на користування РЧР та можливість надання послуг МЕК іншим оператором на частині території першого оператора;

6) відносна раціональність – збільшення показників ефективності користування РЧР оператором за рахунок більшої інтенсивності його використання.

Б. У частині мережі мобільних електронних комунікацій:

1) спільність – конкретна мережа МЕК оператора, як комплекс технічних засобів електронних комунікацій і споруд, може експлуатуватися ще й іншими операторами.

В. В частині послуг, що надаються:

5) варіативність – різна собівартість надання конкретної послуги для оператора, що має мережу МЕК і право на користування РЧР, і для оператора, що використовує ресурси першого.

Одночасно, практично з початку 2000 років під впливом зростання попиту на послуги МЕК як в частині їх наявності, так і в частині їх якості та різноманітності, на міжнародному та національному рівнях став інтенсивно проводитися пошук інших результативних напрямків підвищення ефективності використання РЧР.

Першим сигналом про розуміння наступаючого обмеження можливостей жорсткого регулювання використання РЧР та інженерно-технічних рішень була поява концепції WAPECS (Wireless Access Policy for Electronic Communications Services) – політики бездротового доступу для надання електронних комунікаційних послуг, яка стала реалізовуватися в ЄС з 2005 року [11]. За думкою С. Фордже, реалізація концепції WAPECS стала центром зусиль Комісії Євросоюзу з координації регіонального (європейського – *авт.*) руху в спектральній політиці в бік нейтральності технологій та послуг, а також “гнучкого користування” розподіленими діапазонами частот [3]. Одночасно, автори цього звіту також вважають, що реалізація WAPECS досі не дала

доказів тези про те, що жорстка регуляторна політика призвела до неефективного використання спектра.

І з цим можна погодитися. Звичайно, не жорстке регулювання використання РЧР спричинило малоефективний розподіл і виділення РЧР як в світовому масштабі, так і в національному. Особливо, в національному. Але саме в умовах жорсткого регулювання використання РЧР стало можливим хаотичне (волюнтаристичне) розподілення та виділення радіочастот. Причини неефективності такого розподілу при цьому могли бути найрізноманітнішими: починаючи від історичних і технічних і закінчуючи банальними – корупційними, але результат виявився такий, що стає одним із серйозних бар’єрів на шляху широкого впровадження технологій ІР.

Отже, протягом кількох десятків років користувацькі вимоги до номенклатури, змісту та якості послуг електронних комунікацій істотно не змінювалися, за винятком вимоги до можливості передачі цифрових даних. Більш того, користувацькі вимоги до цих послуг формувалися в основному під впливом змісту пропозицій операторів електронних комунікацій.

Однак, все кардинально змінюється в умовах використання технологій ІР, які по суті забезпечують і забезпечуватимуть реальну діяльність фізичних і юридичних осіб як з надання найрізноманітніших послуг, так і з проведення робіт різного змісту практично у всіх сферах людської активності. Для споживача, чия діяльність базується на технологіях ІР, вимоги до надійності і стійкості роботи мережі мобільних електронних комунікацій, які забезпечують функціонування технологій ІР, стають критичними, а вимоги до якості надання послуг, в тому числі і до географічного покриття такими послугами, досить суворі. Кількість можливого кінцевого обладнання (мобільних пристроїв), задіяного в технологіях ІР у одного споживача, може обчислюватися сотнями і десятками тисяч. Переривання надання послуг мобільних електронних комунікацій практично повністю виключається тому, що може призвести до зупинки діяльності, наприклад, руху автономного автомобільного транспорту.

Висновки.

Аналіз сучасного ринку електронних послуг дає підстави для висновку про те, що вирішення проблеми задоволення кардинальної зміни користувацьких вимог до номенклатури, змісту та якості цих послуг стане можливим тільки за умови переходу від системи масового обслуговування “невимогливих” користувачів до створення “локальних” екосистем електронних комунікацій для окремих суб’єктів або їх груп.

Пропонуючи вихід з ситуації, що склалася, коли в умовах вже розподілених діапазонів частот стало явно недостатньо ресурсу РЧР для розгортання перспективних радіотехнологій в інтересах технологій Інтернету речей, Євросоюз оголошує про нову радіоспектральну політику та установлює, що держави-члени у співпраці з Комісією повинні сприяти колективному використанню спектру, а також спільному використанню спектру (стаття 4 Рішення 243/2012/ЄС Європейського Парламенту та Ради “Розробка довгострокової програми політики в галузі радіочастотного спектру” від 14 березня 2012 року) [12].

Крім того, в преамбулі цього Рішення, відзначається, що торгівля правами на використання спектру в поєднанні з гнучкими умовами використання може істотно допомогти економічному зростанню, а смуги частот, в яких гнучке використання вже було введено законодавством Євросоюзу, повинні негайно стати предметом торгівлі відповідно до Директиви 2002/21/ЄС, в тому числі, для цих діапазонів радіочастот права користування могли б передаватися або здаватися в оренду. Тому в якості однієї з цілей політики в області радіочастотного спектру визначено створення нормативно-правової

бази для забезпечення можливості торгівлі правами на використання спектру, створюючи тим самим можливість для майбутніх цифрових послуг в масштабах всього ЄС.

Таким чином, з кінця нульових років ХХІ століття як у світі, так і в окремих національних державах, активізуються роботи за трьома основними напрямками підвищення ефективності використання РЧР: гнучке спільне і гнучке колективне використання РЧР, а також торгівля правами на користування РЧР. При цьому, звичайно, стає актуальним створення правових умов для колективного і спільного використання окремих діапазонів радіоспектру, а також для торгівлі правами на його використання як в рамках законодавства національних держав, так і в міжнародному праві.

Використана література

1. Cisco visual networking index: global mobile data traffic forecast update, 2015 – 2020. Cisco White Paper, 2014. – Режим доступу : <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf>
2. The 1000x mobile data challenge. Qualcomm Presentation, 2013. – Режим доступу : <http://www.qualcomm.com/media/documents/files/1000x-mobile-data-challenge.pdf>
3. Forge S. Perspectives on the value of shared spectrum access. Final Report. Support for the preparation of an impact assessment to accompany the Commission's Initiative on the Shared Use of Spectrum. 10 February 2012. – Режим доступу : https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/scf_study_shared_spectrum_access_20120210.pdf
4. Constitution of the International Telecommunication Union (ITU). – Режим доступу : [http://www.jus.uio.no/english/services/library/treaties/07/7-06/itu_const.xml#treaty-header1-1\\$](http://www.jus.uio.no/english/services/library/treaties/07/7-06/itu_const.xml#treaty-header1-1$);
Convention of the International Telecommunication Union (ITU). – Режим доступу : <http://www.jus.uio.no/english/services/library/treaties/07/7-06/international-telecommunication-union.xml#treaty-header2-5>
5. Radio Regulations Articles. Edition of 2012. ITU 2012.
6. Directive 95/62/EC of the European Parliament and of the Council of 13 December 1995 on the application of open network provision (ONP) to voice telephony – Режим доступу: http://freecases.eu/Doc/LegalAct/3659263#art_13
7. Mobile Evolution. Ofcom's mobile sector assessment. London, 17 December 2009. – Режим доступу : https://www.ofcom.org.uk/__data/assets/pdf_file/0022/37138/msa_statement.pdf
8. Virgin Mobile an example of an MVNO. – Режим доступу : <http://www.itu.int/itunews/issue/2001/08/mvno.html#top>
9. Уберизация телекоммуникаций : MVNO. 04.07.2016. – Режим доступу : <http://nag.ru/articles/article/29543/uberizatsiya-telekommunikatsiy-mvno.html>
10. Шалагинов А. Бизнес-модель конвергентного MVNO. 31/03/2017 г. – Режим доступу : <https://shalaginov.com/2017/03/31/%D0%B1%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C-%D0%BA%D0%BE%D0%BD%D0%B2%D0%B5%D1%80%D0%B3%D0%B5%D0%BD%D1%82%D0%BD%D0%BE%D0%B3%D0%BE-mvno>
11. Radio spectrum policy group opinion on. Wireless Access Policy for Electronic Communications Services (WAPECS) (A more flexible spectrum management approach). Final – November 23, 2005. – Режим доступу : http://rspg-spectrum.eu/wp-content/uploads/2013/05/rspg_05_102_op_wapecs.pdf
12. Decision no 243/2012/EU of the European Parliament and of the Council of 14 March 2012 establishing a multiannual radio spectrum policy programme. – Режим доступу : <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012D0243&from=EN>

~~~~~ \* \* \* ~~~~~

УДК 340.134:[351.86+004.75]

**ДОРОНІН І.М.**, кандидат юридичних наук, доцент,  
в.о. завідувача наукової лабораторії  
НДІ інформатики і права НАПрН України

## **ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ РОЗПОДІЛЕНОЇ ОБРОБКИ ДАНИХ: ПРАВО ТА ФУНКЦІЇ ДЕРЖАВИ**

***Анотація.** У статті досліджено проблему впливу сучасних технологій розподіленої обробки даних на суспільний розвиток, зміни у відносинах, що викликають необхідність в належному правовому регулюванні та державному впливі.*

***Ключові слова:** розподілена обробка даних, блокчейн, криптовалюта, DL-технології, правове регулювання, функції держави.*

***Аннотация.** В статье исследована проблема влияния современных технологий распределенной обработки данных на общественное развитие, изменения в отношениях, что вызывает необходимость в надлежащем правовом регулировании и государственном вмешательстве.*

***Ключевые слова:** распределенная обработка данных, блокчейн, криптовалюта, DL-технологии, правовое регулирование, функции государства.*

***Summary.** The article explores the problem of the influence of modern technologies of distributed data processing on social development, changes in social relations, which calls for proper legal regulation and state influence.*

***Keywords:** distributed data processing, distributed ledger technology, blockchain, cryptocurrency, legal regulation, state functions.*

**Постановка проблеми.** Стрімкий розвиток комп'ютерних технологій, що спостерігається останнє десятиріччя, значно впливає і на соціальні відносини, вирішення суто технічних завдань та пов'язані із цим зміни соціальних відносин призводять до проблем, що потребують правового регулювання.

Розвиток технології розподіленої обробки даних відбувався паралельно з розвитком технологій використання комп'ютерних мереж. Особливості існування цих технологій та вирішення різного роду технічних завдань тривалий час не створювали якихось особливих проблем правового характеру, оскільки суто технічна специфіка, не здійснюючи прямого впливу на суспільні відносини, не викликала необхідності у відповідному нормативно-правовому регулюванні цієї діяльності. У подальшому при технічному розвитку сфери комп'ютерних технологій виникла технологія розподілених реєстрів (Distributed Ledger Technology, DLT), одним із напрямків якої є “блокчейн” – технологія розподіленої системи даних, що закладена в основу криптовалют (віртуальних валют, які не мають фізичного аналогу і, як правило, одного емітента), найвідомішою з яких на сьогодні є система “Біткойн”. Впровадження та стрімке розповсюдження технології “блокчейн” викликає зміни у суспільних відносинах, що потребує правового регулювання. Останні пропозиції щодо розширення сфери застосування технології “блокчейн” на різні сфери суспільного життя – банківську справу, фінанси, оподаткування, державні реєстри, виборче законодавство, земельні відносини тощо викликає і нові соціальні та правові проблеми.

**Результати аналізу наукових публікацій.** На сьогодні питання використання комп'ютерних систем розподіленої обробки даних (у сучасній літературі вживається також термін “розподілені інформаційно-обчислювальні системи”) та відповідних

технологій були предметом досліджень у сфері технічних наук. В окремих працях з соціології та права в основному зверталась увага саме на “блокчейн”-технології, а найчастіше – використання криптовалюти “біткойн”.

Слід зазначити, що DL-технологія (одним із підвидів якої є “блокчейн”-технологія) на сьогодні однозначно термінологічно не визначена в українській мові. В основі скорочення DLT лежить термін “ledger”, який, починаючи з XIX сторіччя розуміється як “основна бухгалтерська книга” або grosбух [1, с. 555; 2; 3], а походить від співзвучного застарілого і скоріш за все запозиченого з голландської мови терміну “leg[g]er” – “річ, що знаходиться в основі чогось” [1, с. 555; 4, с. 382]. Слід зазначити, що важливість цього терміну для розуміння суті технології підкреслюється обраною для першого академічного журналу з DL-технологій, який видається Бібліотекою Університету Пітсбурга, назвою “Ledger”.

Питанням соціальних, організаційних, інформаційних, технічних аспектів використання “біткойну” та “блокчейн”-технологій присвячені численні публікації, здебільшого в англійській науковій літературі останніх років, у т.ч. і монографічного змісту [5; 6], але особливостям правового регулювання відносин, які виникають навколо технології “блокчейн” та криптовалюти “біткойн”, уваги приділено дещо менше. Серед публікацій останнього часу необхідно звернути увагу на праці Т. Ківіата, С. Щербака, К. Сінгха [8 – 10]. Слід також згадати огляди та звіти державних органів, аналітичних і дослідницьких установ, присвячені окремим питанням використання та розвитку DL-технологій, здебільшого з точки зору аналізу економічного впливу розповсюдження криптовалют [7; 11 – 16]. При цьому практично відсутні публікації стосовно правових аспектів використання DL-технологій та інших (альтернативних “біткойну”) криптовалют.

В Україні питання використання зазначених технологій переважно згадуються в ЗМІ або у досить значному масиві електронних публікацій, присвячених торгівлі “біткойн” та пов’язаним із цим проблемам. Серед робіт правового характеру можливо зазначити наукову статтю О. Конашевича [17] та огляд законодавства, що регламентує обіг криптовалют в різних країнах, підготовлений фахівцями юридичної компанії “Axon Partners” [18].

Питання ж державного впливу та урядування у цій сфері також залишаються поза увагою вітчизняної правової науки.

**Метою статті** є проведення аналізу наукових, практичних та аналітичних напрацювань щодо правових аспектів DL-технологій, їх впливу на суспільні відносини, які зумовлюють пов’язані із розповсюдженням зазначених технологій зміни в предметі та межах правового регулювання. Окремо необхідно дослідити особливості державного впливу на суспільні відносини при використанні DL-технологій в контексті трансформації функцій держави у сучасних умовах.

**Виклад основного матеріалу.** Використання систем розподіленої обробки даних для вирішення різного роду технічних завдань застосовується досить давно. Перші програми використання потужностей електронно-обчислювальних машин для проведення спільних обчислень з’явилися понад 40 років тому практично одночасно зі створенням комп’ютерних мереж. Застосування технологій обумовлено вирішенням суто технічних завдань та економічними потребами – перші їх розробники забезпечували проведення обчислень на електронно-обчислювальних машинах, які не використовувались у неробочий час та у вихідні, або не були задіяні у вирішенні інших завдань.

Розвиток такої технології відбувався паралельно з розвитком технологій побудови і використання комп’ютерних мереж, а також передачі інформації у таких системах, особливо значний вплив на їх розвиток спричинили “пірінгові” мережі, які дозволили

відійти від традиційної побудови за принципом “клієнт-сервер” [5, с. 677-678; 6, с. 424, 441-442]. Особливості існування цих технологій тривалий час не створювали специфічних проблем правового характеру за винятком захисту прав інтелектуальної власності при розповсюдженні інформації у “пірингових” мережах, що призвело до юридичної “війни проти торентів” і є значною проблемою правового регулювання до цього часу.

У подальшому з’явилась технологія розподілених реєстрів (Distributed Ledger Technology, DLT) і, нарешті технологія “блокчейн”, яка стала на сьогодні трендом в гуманітарних науках, що вивчають аспекти інформаційних технологій. На нашу думку створенню і розповсюдженню DL-технологій сприяло технічне вирішення двох проблем – передачі інформації за відсутності централізованого серверу і взагалі відхід від побудови мереж за принципом “клієнт-сервер”. Відома американська дослідниця філософських і соціологічних проблем впровадження нових технологій М. Свон вважає одноранговий “піринговий” обмін основою для технології “блокчейна” [19, с. 3]. Погоджуючись із цим, слід зазначити, що іншою технічною проблемою, яка вирішена, є проблема захисту інформації від впливу, тобто криптозахисту на рівні кожної операції обміну інформацією. Хоча дослідники фіксують випадки заволодіння інформацією, але успішний електронний вплив з метою її зміни відбувається на рівні програмного забезпечення кінцевого користувача, а не на рівні обміну даними [7 с. 1, 7-9] На сьогодні саме такий захист зумовив надзвичайну популярність криптовалют в інвесторів, насамперед інформаційної сфери, оскільки криптозахист зробив з таких валют по суті “цифрове золото”, не дарма саме таку назву для своєї книги, присвяченій історіям ключових постатей біткойн-індустрії обрав репортер-розслідувач Н. Поппер.

Не вдаючись в технічні тонкощі, можливо стверджувати, що сутність DL-технології полягає у відсутності якогось одного фізичного носія інформації (сервера чи системи серверів), що зберігає усю інформацію, або її частину. Інформація, яка зберігається, перебуває одночасно у всіх учасників системи, при цьому жоден з них не контролює ані усю інформацію, ані якусь критично важливу частину. Саме таке розуміння суті технології вбачається критично важливим для правового погляду на суспільні відносини в цій сфері з метою вирішення проблем юридичного характеру.

Звичайно існують різні технічні рішення зазначеного вище завдання щодо розподіленої інформації. З огляду на критичну важливість для такої системи проблеми захисту інформації перспективними для прикладного використання поза сферою наукових обчислень є системи, які використовують криптографічний захист і конструювання блоків. Зрозуміло, що поштовх для безперешкодного розвитку таких засобів було закладено “поразкою” держави при вирішенні проблем обмеженості криптографічного захисту, відомих в літературі під назвою “крипто-війни” початку 1990-х років, що відбувалась у США, які здебільшого закінчились загальним ослабленням державного регулювання у сфері експорту технологій, які використовували криптографію [20]. Врешті-решт вирішення різних аспектів проблеми закінчилось створенням нової технології, яка спочатку була задумана як альтернатива глобальному грошовому обігу.

Зазначена технологія наразі відома як “блокчейн” (від англomовного терміну block chain – ланцюг блоків) і використовується насамперед як розподілена система даних, що закладена в основу криптовалют (віртуальних валют, які не мають фізичного аналогу і, як правило, одного емітента, а здобуваються шляхом використання обчислювальних можливостей учасників системи), найвідомішою з яких на сьогодні є система “Біткойн”.

На сьогодні досить часто у популярній літературі та засобах масової інформації ці поняття використовують як синоніми. Хоча, звичайно, увага суспільства (а останнього часу і держав в особі їх органів) більше зосереджена на “біткойні”, оскільки цифрові

показники є більш ніж красномовними. Починаючи з січня 2017 року капіталізація “біткойн”-індустрії збільшилась вдвічі і станом на травень поточного року становить близько 35 мільярдів доларів США [21]. І хоча таке зростання дозволяє деяким аналітикам зробити висновки про спекулятивний характер торгівлі “біткойн” і її розуміння як чергової інвестиційної “мильної бульбашки”, яка неодмінно закінчиться падінням та кризою [22], економічне значення введення і розповсюдження грошової одиниці, яка не емітується централізовано, але є об’єктом для вільної торгівлі на біржах і обміну на інші валюти, важко переоцінити.

В основі сприйняття “біткойн”-індустрії знаходяться багато факторів – як економічних, так і геополітичних. Наприклад, окремі дослідники приділяють значну увагу ролі Китаю на глобальних ринках “біткойн” та взаємозв’язку характеру внутрішніх китайських ринків із ціною криптовалюти. З іншого боку “біткойн” став трендом і породив певну суспільну субкультуру, нерідко і без якогось економічного підґрунтя. Розповсюдження таких технологій в нашій державі та її вплив на політичні рішення буде висвітлено дещо нижче.

Як вбачається з самого терміну “криптовалюта”, в основі її існування знаходиться безпека. Попри досить невелику історію використання криптовалют, з часу впровадження їх вільного обміну на звичайні грошові кошти та введення котирування на деяких валютних біржах, різного роду атаки на систему є постійними. Особливо коли вартість одного біткойну стала перевищувати 1 000 доларів США.

Звичайно, більшість кібератак спрямовано на викрадення криптовалют. Такі атаки бувають і успішними у випадках, коли об’єктом є не уся система або її частина під час функціонування, а конкретний визначений користувач, що “зберігає криптовалюту” (яка так би мовити “існує” тільки у віртуальному вигляді) на власних носіях інформації. Іншою метою атак є намагання встановити контроль над емісією криптовалют одним користувачем (або групою, що об’єднана змовою). Зазначені випадки мали місце шляхом змови великих груп, які займаються здобуванням “біткойну”, але успішними не були завдяки закладеним в алгоритм системи запобіжникам.

Оскільки в основі системи є розподілення інформації та криптографічний захист усіх транзакцій на усіх етапах система є стійкою за умови, якщо електронно-обчислювальні машини, які її складають, продовжують роботу. У випадку, якщо система створена і використовується для обігу криптовалют, її робота зумовлена необхідністю здобування нових одиниць криптовалюти, яка виробляється внаслідок проведення обчислювальних операцій учасниками усієї системи. Таким чином учасників системи тримає у ній їх власний економічний інтерес. Слід зазначити, що кількість криптовалют, які є альтернативою “біткойн”, уже обчислюється сотнями. Серед них є і валюти з різними видами підтримки державами, а також ті, які покращили алгоритм програми таким чином, що виключають генерацію у промислових масштабах. Наприклад, капіталізація другої і третьої за обсягами індустрії криптовалют (Ethereum та DASH) перевищує 1 мільярд доларів по кожній [23].

Як вбачається з аналітичних оглядів, підготовлених фахівцями у сфері фінансів та регулювання [7; 11 – 15], попри нібито мінімальність державного впливу в цій сфері і, навіть, практичну неможливість статутного правового регулювання таких суспільних відносин [9, с. 82], основними проблемами вбачаються такі:

1. Необхідність ліцензування (або будь-якого іншого дозволу з боку держави в особі її уповноважених органів) для такої діяльності взагалі. У демократичних державах усяка діяльність приватних осіб, що не порушує закон, є легальною. Таким чином, відповідні операції з криптовалютами (купівля-продаж та інші угоди) ніяких дозволів не

потребують, оскільки здійснюються між приватними особами. У цьому разі виникає питання юрисдикції їх цивільно-правових спорів. Але на сьогодні в юридичному плані воно залишається більш теоретичним аніж практичним, і буде вирішене у подальшому, швидше за все шляхом правового прецеденту. Водночас, ліцензування діяльності з емісії криптовалют, обігу на біржах та обміну на іншу (емітовану державою) валюту, потребує державного впливу. Метою зазначеної діяльності державних органів є протидія вчиненню злочинів (насамперед, шахрайства) щодо приватних осіб, а також легалізації доходів, отриманих злочинним шляхом, фінансуванню тероризму, ухиленню від сплати податків. Основним проблемним питанням для правової регламентації цих відносин є необхідність дотримання правил про так звану банківську ідентифікацію вкладників, що не завжди можливо в умовах проведення операції з криптовалютою. Зазначена проблема визначена в іноземній правовій літературі як така, що потребує вирішення [8, с. 590].

2. Оподаткування операцій з криптовалютами. Безумовно, що під час проведення операцій отримується прибуток, який підлягає оподаткуванню. При цьому такий прибуток може виникнути і як пасивний дохід внаслідок збільшення вартості криптовалюти по відношенню до валюти, емітованої державою, протягом часу. У деяких державах існують також окремі податки на майно, до складу якого також можуть бути віднесені криптовалюти внаслідок наявності у них відповідної вартості. На сьогодні у більшості держав із розвинутою фінансовою системою та деталізованим податковим законодавством, проблема належної правової регламентації оподаткування таких операцій та вдосконалення відповідного законодавства є актуальним [24, с. 532-533].

3. Також важливим питанням є визначення статусу криптовалют саме як грошей. Ще два роки тому щодо криптовалют застосовувався термін “сурогат грошей”. А в деяких державах були підготовлені законодавчі пропозиції стосовно заборони таких “сурогатів”. На сьогодні з різних причин криптовалюти (або окремі види) заборонені у деяких країнах (Бангладеш, Болівія, В’єтнам, Таїланд), проте операції з ними не криміналізовано, а ці обмеження стосуються адміністративних заборон у діяльності банків та інших фінансових установ. Така заборона пов’язана, як правило, з іншими численними забороняючими та регламентуючими вимогами. Інші випадки (Ісландія, Гонконг) стосувались досить складної державної політики та наявності певних преференцій у цій сфері. Як правило, спірні питання виникають в першу чергу при валютообмінних операціях (з огляду на відсутність централізованого емітента, криптовалюта розглядається як аналог дорогоцінного металу, а операції юридично вважаються бартерними), а також при використанні криптовалют як засобу платежу за товари чи послуги (при цьому невирішеними залишаються спірні питання у цивільно-правовому статусі такої угоди і оподаткуванні відповідної операції).

4. Необхідність дотримання вимог міжнародно-правових актів по боротьбі з тероризмом та легалізацією доходів, отриманих злочинним шляхом. Імплементация зазначених положень у національне законодавство викликає правову колізію з огляду на зазначені вище властивості криптовалюти. У літературі звернуто увагу на можливість використання криптовалют для фінансування тероризму та іншої протиправної діяльності [8, с. 571-572; 10, с. 49-58; 25, с.13-15]. При цьому дослідники проблематики протидії фінансуванню тероризму та іншої протиправної діяльності зазвичай розглядають криптовалюти як аналог історичних систем безготівкових операцій з веденням децентралізованого обліку. У такому разі виникає необхідність у вжитті відповідних заходів щодо застосування визначених міжнародно-правовими актами механізмів насамперед у питанні ідентифікації в режимі реального часу не тільки

суб’єктів проведення операцій, а і всіх транзакцій. Пов’язаним із цим питанням є необхідність дотримання вимог законодавства щодо обмеженості використання криптографії недержавними органами та приватними особами, що до цього часу існує в США та деяких інших країнах. Така обставина може впливати на правове регулювання використання криптовалюти, оскільки використання криптографічних методів її захисту є неодмінною властивістю криптовалюти.

І нарешті, проблемним питанням, що неодмінно виникає, є захист персональних даних у випадку, якщо держава захищає зазначену інформацію. Річ у тім, що технологія блокчейн не забезпечує анонімізацію, навпаки – для участі у системі необхідна цифрова ідентифікація користувача, яка розповсюджується на усі його дії. У випадку поєднання такої технології зі сферою “Інтернет речей” можлива повна ідентифікація дій особи, фіксація інформації стосовно таких дій, а також вплив на ці дії зовні. До речі на двоякий характер технології і здатність використання її ідентифікаційних можливостей в інтересах правоохоронної діяльності вже звернуто увагу дослідників [26].

На нашу думку питання правового регулювання суспільних відносин, які виникають у ході обігу криптовалют, мають розглядатись у контексті реалізації функцій держави, що знаходить свій прояв у відповідному впливі та правовій регламентації. У правовій регламентації обігу криптовалют реалізується економічна функція держави, яка зумовлена потребами ринкової економіки. Інша річ – це застосування технології “блокчейн” у тих напрямках життєдіяльності, що прямо не пов’язані із обігом криптовалют.

За останні два роки зазначений вид технологій розподіленої обробки даних став дуже популярним, переважно в сфері вітчизняних мас-медіа. З огляду на таку популярність, імідж “блокчейн” став використовуватись у політичних цілях та у рекламній компанії деяких продуктів, у т.ч. ніяк не пов’язаних з цими технологіями.

Особливим напрямом є застосування технологій розподіленої обробки даних в системах електронного урядування та ведення державних реєстрів. Це зумовлено вимогами боротьби з корупцією, що досягається прозорістю дій держави [16; 17].

Використання “блокчейн” та інших подібних DL-технологій для ведення державних реєстрів та у діяльності державних органів визнане перспективним фахівцями з державного стратегічного планування провідних країн світу [11]. Починаючи з 2016 року, у пресі згадувалось принаймні про два проекти застосування технології “блокчейн” саме для ведення різного роду державних реєстрів України. Попри досить активну кампанію в ЗМІ саме на підтримку “блокчейн”-технології, ще ніде в світі не реалізовано в рамках більш-менш великого проекту у сфері державних реєстрів. Значна популярність ідеї застосування “блокчейн”-технології для державних реєстрів зумовлена насамперед недовірою суспільства до діяльності державних органів, а також іншими соціальними факторами впливу (медійна популярність теми, недовіра до закритості інформації, приналежність активної частини користувачів соціальних мереж і ЗМІ до субкультури “блокчейну” та криптовалют, лібертаріанські ідеї тощо).

### **Висновки.**

На наш погляд, при використанні сучасних технологій розподіленої обробки даних (DLT, блокчейн) у сферах державного регулювання та державної реєстрації інформації неодмінно рано чи пізно доведеться вирішити ряд проблем правового характеру, до числа яких слід віднести питання:

- відповідальності держави за функціонування системи (у випадку класичної “блокчейн”-технології ніхто не контролює всю систему),
- стимулів для підтримки функціонування системи користувачами (у випадку криптовалют таким стимулом є економічний);



- захищеності інформації (насамперед від втрати і спотворення та забезпечення довготривалого (практично довічного) зберігання у відкритому для користування стані).

У будь-якому разі впровадження технологій розподіленої обробки даних для потреб управління державою потребуватиме значного оновлення законодавства і вирішення дуже серйозних правових проблем.

### Використана література

1. Johnson's English Dictionary. – Boston : Published by Perkins and Marvin, 1830. – 1156 p.
2. Merriam Webster Dictionary Online. – Режим доступу : <https://www.merriam-webster.com/dictionary/ledger>. – Назва з екрана. – Дата звернення : 27.05.2017 p.
3. Cambridge Dictionary Online. – Режим доступу : <http://dictionary.cambridge.org/dictionary/english/ledger?q=Ledger>. – Назва з екрана. – Дата звернення : 27.05.2017 p.
4. Dictionary of English Etymology by Hensleigh Wedgwood. Second Edition / Hensleigh Wedgwood. – London : Trubner & Co, 1872. – 746 p.
5. Kshemkalyani Ajay. Distributed Computing. Principles, Algorithms And Systems / Ajay D. Kshemkalyani, Mukesh Singhal. – Cambridge : University Press, 2008. – 756 p.
6. Distributed Systems : Concepts and Design. Fifth Edition / George Coulouris, Jean Dollimore, Tim Kindberg, Gordon Blair. – Boston : Pearson-Addison-Wesley, 2012. – 1008 p.
7. Bitcoin : Questions, Answers and Analysis of Legal Issue. Report by Congressional Research Service. October, 13.2015 / Edward V. Murphy, Maureen Murphy, Michael V. Seitzenger. – Washington : US Congress Research Service. – 2015. – 36 p.
8. Kiviat Trevor. Beyond Bitcoin: Issues In Regulating Blockchain Transactions / Trevor I. Kiviat // Duke Law Journal. – 2015. – Vol. 65 (569). – P. 569-608.
9. Shcherbak Sergii. How Should Bitcoin be Regulated? / Sergii Shcherbak // European Journal Of Legal Studies. – 2014. – Vol. 7. – No 1. – P. 42-83.
10. Singh Kavid. The New Wild West: Preventing Money Laundering in the Bitcoin Network / Kavid Singh // Northwestern Journal of Technology and Intellectual Property. – 2015 – Vol. 13, Issue 3. – P. 38-64.
11. Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser. December 2015 / Mark Walport. – Режим доступу : [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf) – Назва з екрана. – Дата звернення : 27.05.2017 p.
12. Whitepaper On Distributed Ledger Technology. Commissioned by Hong Kong Monetary Authority. – Режим доступу : [http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper\\_On\\_Distributed\\_Ledger\\_Technology.pdf](http://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf). – Назва з екрана. – Дата звернення : 27.05.2017 p.
13. Distributed ledger technology in payments, clearing, and settlement / David Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahu, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird. – Режим доступу : <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>. – Назва з екрана. – Дата звернення : 27.05.2017 p.
14. Casey Michael. Blockchain Technology: Redefining Trust for a Global Digital Economy / Michael Casey, Mariana Dahan. – Режим доступу : <https://medium.com/mit-media-lab-digital-currency-initiative/blockchain-technology-redefining-trust-for-a-global-digital-economy-1dc869593308>. – Назва з екрана. – Дата звернення : 27.05.2017 p.
15. Virtual Currencies and Beyond : Initial Consideration. Prepared by International Monetary Fund Staff Team / Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, and Concepcion Verdugo-Yepes. – Режим доступу : <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>. – Назва з екрана. – Дата звернення : 27.05.2017 p.

16. Kim Kibum. Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology. Paper for 2017 OECD Global Anti-Corruption & Integrity Forum / Kibum Kim, Taewon Kang. – Режим доступу : <https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology.pdf>. – Назва з екрана. – Дата звернення: 27.05.2017 р.

17. Konashevych O.. The Use Of Blockchain Technology for the Development Of Electronic Democracy And Electronic Governance/O. Konashevych // Часопис Національного університету “Острозька академія”. – 2015. – № 1. – (Серія “Право”). – Режим доступу : <http://lj.oa.edu.ua/articles/2015/n1/15koiaeg.pdf>. – Назва з екрана. – Дата звернення : 27.05.2017 р.

18. Правовое регулирование криптовалютного бизнеса : отчет Axon Partners и ForkLog Researchers, февраль 2017. – Режим доступу : <http://axon.partners/wp-content/uploads/2017/02/Global-Issues-of-Bitcoin-Businesses-Regulation.pdf>. – Назва з екрана. – Дата звернення : 27.05.2017 р.

19. Swan Melanie. Blockchain: Blueprint for a New Economy / Melanie Swan - Sebastopol CA : O'Reilly Media, 2015. – 152 p.

20. Levy Steven. CRYPTO: How the Code Rebels Beat the Government? Published 2001/Steven Levy. – Режим доступу : <http://www.nytimes.com/books/first/l/levy-crypto.html>. – Назва з екрана. – Дата звернення : 27.05.2017 р.

21. Market Capitalization. The total USD value of bitcoin supply in circulation. Chart. – Режим доступу : <https://blockchain.info/en/charts/market-cap>. – Назва з екрана. – Дата звернення : 27.05.2017 р.

22. Rich Bryan. Is Bitcoin A Bubble? 2017, May 25 / Bryan Rich. – Режим доступу : <https://www.forbes.com/sites/bryanrich/2017/05/25/why-the-bitcoin-bubble-could-be-dangerous/#3ed400111bd9>. – Назва з екрана. – Дата звернення : 27.05.2017 р.

23. Капіталізація DASH и Ethereum Classic превысила \$ 1 млрд. – 24.05.2017. – Режим доступу : <http://forklog.com/kapitalizatsiya-dash-i-ethereum-classic-prevysila-1-mlrd>. – Назва з екрана. – Дата звернення : 27.05.2017 р.

24. Hughes Sara. Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries / Sara Hughes, Stephen Middlebrook // Yale Journal on Regulation. – 2015. – Vol. 32. – P. 496-559.

25. Brill Alan. Cryptocurrencies: The Next Generation of Terrorist Financing? / Alan Brill, Lonnie Keene // Defence Against Terrorism Revue. – 2014. – Vol. 6. – No 1. – P. 7-30.

26. Everdell Christian. The Promise of Blockchain Technology To Combat Money Laundering / Christian Everdell, Daniel Mandell // New York Law Journal. – 2017. – Vol. 257. – No 62. – Режим доступу : [https://www.cohengresser.com/assets/publications/070041703\\_Cohen\\_Gresser.pdf](https://www.cohengresser.com/assets/publications/070041703_Cohen_Gresser.pdf). – Назва з екрана. – Дата звернення : 27.05.2017 р.

~~~~~ \* \* \* ~~~~~

УДК 342.951:351.82

ТАРАСЮК А.В., аспірант, Національний університет
біоресурсів і природокористування України

ВІДКРИТІ ДАНІ ТА ІНШІ ДАНІ У ПУБЛІЧНОМУ ДОСТУПІ: ПРАВОВІ АСПЕКТИ

***Анотація.** Стаття присвячується правовим аспектам використання публічної інформації у формі відкритих даних та іншої інформації, що є у публічному доступі у мережі Інтернет у комерційних та некомерційних проектах.*

***Ключові слова:** інформаційне право, відкриті дані, публічні дані, дані у відкритому доступі, великі дані, приватність.*

***Аннотация.** Статья посвящается правовым аспектам использования публичной информации в форме открытых данных и другой информации, представляемой в открытом доступе в сети Интернет в коммерческих и некоммерческих проектах.*

***Ключевые слова:** информационное право, открытые данные, публичные данные, данные в открытом доступе, большие данные, приватность.*

***Summary.** The article is devoted to legal aspects of usage of public information in a form of open data and other information with open access at the Internet in commercial and non-commercial projects.*

***Keywords:** informational law, open data, public data, open access data, big data, privacy.*

Постановка проблеми. Інформація є необхідним ресурсом для компаній в їхній діяльності. Її актуальність, достовірність та якість багато в чому визначають успіх підприємства. Фактично, дані стають сировиною, необхідною для функціонування суб'єктів господарювання та некомерційних проектів. Відкриті дані та інші дані, що є у відкритому доступі на тих чи інших підставах в мережі Інтернет, можна вважати частиною “Великих даних” (англ. – Big Data).

Результати аналізу наукових публікацій. Правовими аспектами збору та аналізу таких даних, розміщених на різноманітних приватних веб-сайтах займалися іноземні правники, зокрема Т. Клаузнер (Т. Klausner) [1]. В Україні питання загроз приватному життю при застосуванні технологій “Великих даних” досліджувались, зокрема, С.А. Серьогіним [2] та іншими науковцями, про результати робіт яких йдеться у [3, с. 58-60, 62-67]. Проте юридичні питання використання публічної інформації у формі відкритих даних та іншої інформації у публічному доступі продовжують знаходитися у сфері правових дискусій та на початковому етапі пошуку шляхів їх вирішення.

Метою статті є розробка практичних правових підходів щодо легального використання відкритих даних та іншої публічної інформації, що є у відкритому доступі в мережі Інтернет, з точки зору можливості використання такої інформації в діяльності підприємств, стартап-проектів та організацій, у тому числі і завдяки комбінуванню такої інформації в рамках проектів українських компаній та організацій, а також нерезидентів.

Виклад основного матеріалу. Визначення поняття “відкритих даних” тією чи іншою мірою наведено в ст. 10¹ Закону України “Про доступ до публічної інформації” [4]. Зокрема вказано, що “публічною інформацією у формі відкритих даних – є публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання”.

Ще одне визначення поняття “відкритих даних”, яке є корисним в рамках цієї статті, наводить Л. Джеймс (L. James), а саме: “Відкриті дані представляють собою дані, які можуть бути вільно використані, розповсюджені та комбіновані будь-ким, будь-де, з будь-якою метою” [5]. Таке визначення наводиться як суть більш широкої дефініції відкритих даних, запропонованих Фондом відкритих знань [6]. Отже, відкритими є дані, що надають інформацію, яка може бути використана будь-ким, у тому числі з комерційною метою, якщо це передбачено законом. Держава може надавати у відкритий доступ публічну інформацію у вигляді відкритих даних, встановлюючи категорії такої інформації та певні обмеження, наприклад, щодо персональних даних.

У багатьох країнах та окремих містах створено веб-портали, на яких розміщено публічну інформацію у вигляді відкритих даних та умови використання такої інформації. Як приклад, можна навести відповідний ресурс в США – <https://www.data.gov> [7] та Великій Британії – <https://data.gov.uk> [8].

Наступною категорією в рамках цієї статті є “інші дані”, що перебувають у “відкритому доступі”. До таких даних автор відносить будь-яку інформацію в мережі Інтернет, до якої можна отримати доступ за визначеною адресою. Під умовною назвою – “інші дані у відкритому доступі” автор має на увазі будь-яку інформацію, у більшості своїй у текстовій формі, яка розміщена на різноманітних веб-сайтах, та доступ до якої може отримати фактично кожен, хто має доступ до мережі Інтернет. Проте, умови можливого використання таких даних часто значною мірою відрізняються від відповідних правових можливостей роботи з ними. Компанії та окремі фізичні особи у своїй діяльності можуть плутати ці поняття, та, як наслідок, допускати порушення прав третіх осіб під час комбінування, комерційного використання публічної інформації у вигляді відкритих даних та інших даних у відкритому доступі, що знаходяться на різноманітних Інтернет-ресурсах.

Правова природа відкритих даних. Відкриті дані є доступними на певній правовій підставі. Оскільки у питанні концепції відкритих даних Україна перейняла досвід провідних країн світу щодо їх правового регулювання, вважаємо за доцільне проаналізувати деякі з документів, за якими відкриті дані стають відкритими у інших країнах.

Як вказувалось вище, у Великій Британії, основним порталом відкритих даних є ресурс <https://data.gov.uk>, завдяки якому дані розповсюджуються (якщо тільки в самому масиві даних не вказано інше) на підставі ліцензії, яка надається всім бажаючим. Така ліцензія має назву – “Відкрита урядова ліцензія для інформації публічного сектору” (Open government license for public sector information) [9].

В ліцензії вказано, що її утримувач може використовувати інформацію, що є доступною, вільно та у гнучкій манері, але за деяких умов. Вона поширюється у всьому світі, є безкоштовною та не ексклюзивною. В рамках нормативного упорядкування відносин, ліцензія надає можливість використання інформації у контексті наступних видів дій: копіювання, публікування, поширювання і передавання інформації, її адаптування та експлуатування на комерційній основі, але не шляхом наприклад, об’єднання її з іншою інформацією, або включивши її в свій власний продукт або додатки.

Таким чином, утримувачу ліцензії надаються правомочності для обробки та використання відповідної інформації, у тому числі з комерційною метою з можливістю комбінування з іншою інформацією.

Умовою такого використання є зазначення джерела такої інформації. Наприклад, в продукті, який містить такі відкриті дані, має бути вказано, що в ньому містяться відкриті публічні дані. Ще однією умовою є те, що особа, яка буде використовувати таку інформацію в своєму продукті, не може стверджувати, що є офіційним представником державних органів тощо.

Варто зауважити, що відкриті дані у Великій Британії можуть також поширюватись і за іншими ліцензіями, зокрема згідно “Некомерційної урядової ліцензії на інформацію в публічному секторі” (Non-commercial government license for public sector information) [10]. Ключовою відмінністю цієї ліцензії є пряма заборона на використання відповідної інформації у комерційних цілях, а саме – “утримувачу ліцензії заборонено реалізовувати будь-які з прав, отриманих за цією ліцензією будь-яким способом, який насамперед призначений для або спрямований в бік комерційної вигоди або приватної грошової компенсації”. Таким чином, надаються права:

- копіювати, публікувати, розповсюджувати, передавати інформацію;
- адаптувати інформацію;
- комбінувати інформацію з іншою інформацією.

Головною умовою реалізації таких прав є некомерційне використання отриманої інформації.

Отже, відкриті дані можуть надаватись державою у користування на різних умовах і, перш ніж включати такі дані до свого комерційного продукту, необхідно визначити чи отримано таке право за відповідною ліцензією.

Повертаючись до регулювання відкритих даних в Україні, необхідно більш детально проаналізувати ст. 10¹ Закону України “Про доступ до публічної інформації” Зокрема, в частині 2 вищевказаної статті зазначено, що “Публічна інформація у формі відкритих даних є дозволеною для її подальшого вільного використання та поширення” [4].

Будь-яка особа може копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов’язковим посиланням на джерело отримання такої інформації.

Як ми можемо бачити, правове регулювання відкритих даних багато в чому є аналогічним з регулюванням цієї категорії інформації у Великій Британії. Важливо зазначити про майже повну свободу дій для особи, що використовує таку інформацію щодо цих даних. Також варто відмітити, що інформація надається “як є”, тобто щодо її точності та актуальності не надається гарантій.

Важливим є те, що є винятки з інформації, на яку не поширюється ліцензія, зокрема персональні дані. В Україні також існують обмеження щодо персональних даних, які викладені у частині 3 статті 10¹ вищевказаного закону України [4]. В частині 4 вказаної статті зазначено, що перелік наборів даних, що підлягають оприлюдненню у формі відкритих даних визначає Кабінет Міністрів України. Державні органи, на які покладено обов’язок оприлюднити відповідні відкриті дані роблять це у тому числі і на порталі <http://data.gov.ua> [11] – єдиному державному порталі відкритих даних України.

Правові аспекти практичного використання відкритих даних. Відкриті дані надаються урядами різних країн у користування утримувачам відкритих даних – будь-яким юридичним чи фізичним особам або організаціям на підставі рішення відповідних державних органів та ліцензій. При цьому обсяг прав, які надаються утримувачам таких відкритих даних, може відрізнятися в залежності від обсягу прав, який надається у конкретній країні та щодо конкретних даних.

Візьмемо випадок, коли компанія прагне використати у своєму продукті, який планує розповсюджувати з комерційною метою, відкриті дані різних країн, наприклад, щодо екологічного стану річок в цих країнах. Продуктом такої компанії може бути мобільний додаток, в якому буде показано стан річок з застосуванням різних елементів інформаційної графіки та корисних розробок для користувача, що будуть створені

компанією самостійно. У цьому випадку відкриті дані про стан річок компанія зможе взяти з відкритих баз даних, які розповсюджуються як відкриті дані відповідно до законів цих країн (якщо, звісно, такі дані там є). Попередньо необхідно буде провести правове дослідження щодо можливості:

- отримання таких даних з відкритих реєстрів;
- можливості використання таких даних у комерційних цілях та комбінування з іншими даними;
- можливості комерційного використання таких даних. В цьому випадку відкриті дані з декількох країн фактично стають безкоштовною сировиною для комерційного продукту.

Концепція відкритих даних набирає дедалі більшого поширення у Європі та світі. Проекти, що націлені на глобальний ринок та в основі яких лежать інновації роблять величезні масиви відкритих даних доступними, корисними та зручними у використанні компаніям та людям. Одним з місць створення та просування таких проектів є Європейський інкубатор відкритих даних [12]. Одним з проектів, що є резидентом інкубатора на момент написання цієї статті, є сайт – <https://openlaws.com> [13]. Він оприлюднює відомості щодо конвенцій, директив та інші правові документи Європейського союзу. Таким чином, використовуючи відкриті дані щодо правового регулювання в Європейському союзі, було створено продукт, який дозволяє отримувати доступ до цих нормативних актів у зручному режимі, у тому числі на платній основі.

Повертаючись до правових аспектів використання відкритих даних в Україні, зазначимо, що перелік відкритих даних, що підлягає оприлюдненню в Україні вказаний, зокрема, в “Положенні про набори даних, які підлягають оприлюдненню у формі відкритих даних”, затвердженого постановою Кабінету Міністрів України від 21.10.15 р. № 835 [14]. Серед інших, в цьому переліку містяться дані про перелік потенційних об’єктів оренди державного майна, єдиний державний реєстр судових рішень, та інші.

Український проект, який хотілося б виділити в рамках цієї статті, – це <https://opendatabot.com> [15]. В рамках проекту можна отримати серед інших сервісів інформацію про реєстраційні дані юридичних та фізичних-осіб підприємців в Україні а також дані з реєстру судових рішень. Такі дані є відкритими згідно вищевказаного Положення Кабінету Міністрів України. З правової точки зору є можливість надання повного доступу до своїх даних іншим компаніям, а також самі умови користування сервісом, зокрема застереження щодо відсутності відповідальності компанії за будь-які рішення, які були прийняті користувачами, ґрунтуючись на даних з веб-сайту.

Таким чином, використання відкритих даних у комерційних проектах з правової точки зору можливе та практикується. В рамках реалізації таких проектів доцільно аналізувати правові підстави отримання відкритих даних, а також розробити відповідні правила користування продуктами, які б максимально виключали відповідальність компанії за неточності у інформації, що була одержана як відкриті дані, а також за наслідки використання такої інформації користувачами.

Інші дані у відкритому доступі. Відкриті дані є відкритими на певній правовій підставі. На різноманітних веб-сайтах, у тому числі в соціальних мережах, користувачі добровільно розміщують особисту інформацію про себе, а компанії – інформацію про свою діяльність. Така інформація фактично є відкритою для обробки третіми особами. При цьому, при завантаженні такої інформації, особа, яка завантажує її до соціальної мережі, робить це на певних правових підставах, а саме – у відповідності до правил користування відповідним сервісом. Сервіс же розміщує таку інформацію на своєму ресурсі у межах згоди, отриманої від особи та на умовах, знову ж таки, викладених у

відповідних правилах користування сервісом, які визначають правомочності третіх осіб для обробки такої інформації. В самих же правилах такого сервісу (terms of use) такий механізм закріплюється дозволом (ліцензією), яку надає особа, при завантаженні своїх даних або контенту, що нею створюється, компанії, і навпаки, ліцензією (дозволом), в якому компанія, отримавши ліцензію від користувачів, надає доступ до такої інформації на певних умовах третім особам – користувачам сайту. Приклад такої правової конструкції можна знайти, зокрема, в правилах користування всесвітньо відомими сервісами, такими як //www.linkedin.com [16] та //www.facebook.com [17]. З правової точки зору, правила LinkedIn залишають користувача власником всього контенту (інформації), яку він завантажує до сервісу і може самостійно розповсюджувати її в подальшому, а компанія лише отримує невиключну ліцензію.

З іншого боку, в контексті використання самого LinkedIn, в своїх правилах, компанія вказує на пряму заборону [18]:

- проглядати (scrape) чи копіювати інформацію про профілі користувачів а також іншу інформацію на ресурсі будь-якими технічними чи ручними засобами;
- збирати, використовувати, копіювати або передавати будь-яку інформацію, отриману на LinkedIn, без згоди LinkedIn;
- копіювати, використовувати та вивчати інформацію, з конкурентною метою.

Перелік не є виключним, але можна зробити висновок, що LinkedIn максимально блокує можливості щодо автоматичного чи ручного аналізу, копіювання чи відтворення інформації, що розміщена на ресурсі, окрім як її використання користувачами в дозволених межах правилами платформи.

Ще однією умовною категорією даних, що є у відкритому доступі в мережі Інтернет, яку можна виділити окремо, це дані, які надаються на різноманітних ліцензіях Creative commons [19] та інших. В цьому випадку, використання таких даних визначається умовами відповідної ліцензії.

Інформація, яка розміщена в мережі Інтернет може містити об'єкти авторського права і для використання таких об'єктів необхідно мати правову підставу – дозвіл (ліцензію) від власника виключних майнових авторських прав або підставу, визначену відповідним законом. У будь-якому випадку, таке використання може бути здійснене в межах відповідних ліцензій або в межах норм, що визначають умови добросовісного використання (fair use) щодо конкретних об'єктів та на інших правових підставах, що визначені в законодавстві відповідної держави.

Повертаючись до питання автоматизованого зчитування (споглядання) та аналізу інформації на веб-сайтах за допомогою роботів (ботів) та інших технічних способів, доцільно визначити, чи є такі дії правомірними.

Можна виділити два аспекти, в рамках яких власник веб-сайту може повідомити особу, що бажає здійснити автоматизоване зчитування його ресурсу про дозвіл чи заборону такого зчитування. Перший аспект – технічний. Стандарт виключень для роботів [20], що був прийнятий World Wide Web Consortium 30 січня 1994 року [21], регламентує використання файлу robots.txt власниками веб-сайтів. В цьому файлі вказується інформація щодо можливості автоматизованого зчитування даних з конкретних сторінок веб-сайту. Використання стандарту є добровільним, але на сьогодні він став правилом і його порушення можна вважати порушенням волі сторони – володільця веб-сайту щодо обробки. Другий аспект – юридичний, а саме встановлення відповідних обмежень та застережень щодо заборони обробки та зчитування інформації з веб-сайту технічними засобами в умовах користування відповідним ресурсом.

Можна виділити деякі тези, які характерні для правового регулювання автоматизованого зчитування даних з веб-сайтів в цілому. В статті “Crawling for Data: Best Practices for Mitigating Legal and Compliance Risks for Hedge Fund Managers Utilizing Web Crawling Technology for Investment Research” [2], Е. Кілдаф – керівник, засновник компанії з аналізу даних та Т. Клауснер – партнер юридичної фірми Wilson, Sonsini, Goodrich & Rosati, розкрили правові аспекти автоматизованого зчитування даних з веб-сайтів при проведенні інвестиційних досліджень менеджерами хедж-фондів.

Зокрема, Т. Клауснер наводить тези, які могли б бути додані покупцем інформації, яка є зібраною автоматизованим способом з веб-сайтів. При зборі інформації, збирач гарантує наступне:

- дотримання всіх вимог, відповідно до відомостей з файлів robots.txt;
- автоматизоване зчитування, що не перевантажує сервери веб-ресурсів;
- отримана інформація не містить контенту, що захищений авторським правом;
- інформація, що зчитується, є публічно доступною та не є захищеною паролями;
- дані не збираються в обхід будь-яких технічних обмежень;
- отримана інформація не була отримана після одержання спеціальних інструкцій щодо заборони автоматичної обробки.

Таким чином, можемо зробити висновок, що інформація, що зібрана шляхом автоматизованого зчитування веб-сайтів, може бути правомірно використана за умов дотримання певних умов. Зокрема, вона має бути зібрана без порушень відповідних застережень та/або приписів законів і використовується не порушуючи відповідні права третіх осіб чи вимоги нормативно-правових актів.

Отже, інші дані у відкритому доступі є неоднорідною базою інформації, а складним правовим феноменом. Можливість використання такої інформації необхідно визначати окремо в кожному конкретному випадку в залежності від суб'єкта, що планує їх використовувати, а саме – згідно правомірності способу отримання та використання, в межах умов, за яких вони можуть бути використані.

Висновки.

Відкриті дані та інші дані у відкритому доступі є неоднорідними з правової точки зору та в контексті можливості їх обробки, копіювання, передачі та використання. Правові підстави для таких дій щодо відкритих даних визначаються законодавчими актами відповідних країн, що оприлюднюють публічну інформацію у формі відкритих даних.

Правові підстави та межі дій для інших даних, що є у відкритому доступі в мережі Інтернет визначають власники відповідних ресурсів або особи, що володіють такими даними. Такі дані можуть бути використані і на інших підставах, встановлених законами в межах і в спосіб, що будуть визначені у таких законах.

Створення комерційних продуктів, які використовують як відкриті дані з різних джерел (оприлюднені в рамках різних юрисдикцій), так і інші дані у відкритому доступі, у тому числі, отримані шляхом автоматизованого збору, є можливим з правової точки зору за умов правомірності їх збирання, використання, обробки та передачі.

В умовах комбінування такого неоднорідного масиву даних необхідною є перевірка правових підстав, що дають можливість використовувати їх бажаним способом щодо кожного окремого масиву даних, що комбінується, та врахування правових вимог щодо його використання, зокрема, але не виключно – можливості використовувати в комерційних проектах, необхідності надання посилань, правомірності збирання шляхом автоматизованої обробки тощо. На сьогодні відкриті дані та інші дані у публічному доступі є фактично сировиною для використання за умов дотримання всіх правових вимог.

Перспективою подальших досліджень цього напрямку є створення дорожніх карт, які б визначали конкретні правові шляхи для використання тих чи інших даних для комерційних установ, які практикують використання цього ресурсу в своїй діяльності.

Використана література

1. Klausner T.O. Crawling for Data : Best Practices for Mitigating Legal and Compliance Risks for Hedge Fund Managers Utilizing Web Crawling Technology for Investment Research / Hedge Fund Legal & Compliance Digest, 2016. – Режим доступу : [//www.wsgr.com](http://www.wsgr.com)
2. Серєгин В.А. “BIG DATA” : Новая угроза для прайвеси в условиях информационного общества // Науковий вісник Ужгородського національного університету. – 2015. – № 35. – С. 93-97. – (Серія Право. – Ч. 1. – Т. 1).
3. Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах // Інформація і право. – № 1(20)/2017. – С. 51-67. – Режим доступу : [//www.ippi.org.ua/zhurnal-informatsiya-i-pravo](http://www.ippi.org.ua/zhurnal-informatsiya-i-pravo)
4. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI // Відомості Верховної Ради України (ВВР). – 2011. – № 32. – Ст. 314.
5. James L. Defining Open Data / Open knowledge international blog, 2013. – Режим доступу : [//www.blog.okfn.org](http://www.blog.okfn.org)
6. The Open Data Hendbook / Open Knowledge International. – Режим доступу : <http://openhdatahandbook.org>
7. The Home of the U.S.Government’s Open Data. – Режим доступу : [//www.data.gov.ua](http://www.data.gov.ua)
8. DATA.GOV.UK. Opening up Government. – Режим доступу : [//www.data.gov.ua](http://www.data.gov.ua)
9. Open Government License for public sector information. / The National Archives. – Режим доступу : [//www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)
10. Non-Commercial Government License for public sector information / The National Archives. – Режим доступу : [//www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)
11. Єдиний державний веб-портал відкритих даних в Україні DATA.GOV.UA. – Режим доступу : [//www.data.gov.ua](http://www.data.gov.ua)
12. Open data incubator Europe ODINE. – Режим доступу : [//www.opendataincubator.eu](http://www.opendataincubator.eu)
13. EU Project openlaws.eu. – Режим доступу : [//www.info.openlaws.com](http://www.info.openlaws.com)
14. Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : Постанова Кабінету Міністрів України від 21.10.15 р. № 835. – Режим доступу : [// www.kmu.gov.ua](http://www.kmu.gov.ua)
15. OpenDataBot – сервіс моніторингу реєстраційних даних українських компаній та судового реєстру для захисту від рейдерських захоплень і контролю контрагентів. – Режим доступу : [//www.opendatabot.com](http://www.opendatabot.com)
16. Linkedin. – Режим доступу : [//www.linkedin.com](http://www.linkedin.com)
17. Facebook. – Режим доступу : [//www.facebook.com](http://www.facebook.com)
18. Пользовательское соглашение Linkedin. – Режим доступу : [//www.linkedin.com](http://www.linkedin.com)
19. Публічні ліцензії Creative commons / Creative commons Ukraine. – Режим доступу : [//www.creativecommons.org.ua](http://www.creativecommons.org.ua)
20. Koster M. Robot exclusion standard. – Режим доступу : [//www.en.wikipedia.org](http://www.en.wikipedia.org)
21. World Wide Web Consortium (W3C). – Режим доступу : [//www.w3.org](http://www.w3.org)

~~~~~ \* \* \* ~~~~~

УДК 340:004.7:001.8

ЛАНДЕ Д.В., доктор технічних наук, старший науковий співробітник,  
НДІ інформатики і права НАПрН України  
ФУРАШЕВ В.М., кандидат технічних наук, доцент, старший науковий  
співробітник, НДІ інформатики і права НАПрН України

## ТЕРМІНОЛОГІЧНА МЕРЕЖЕВА МОДЕЛЬ ЯК ВІДОБРАЖЕННЯ ПРОЦЕСІВ ДЕНЦЕНТРАЛІЗАЦІЇ ВЛАДИ В УКРАЇНІ

**Анотація.** У роботі наводиться алгоритм побудови моделей термінологічних мереж з предметної області “децентралізація” на базі автоматизованого моніторингу і аналізу контенту мережі Інтернет. Терміни природної мови, що відображають поняття, склад і зміст яких динамічно змінюється, утворюють мережі. Дослідження цих мереж у динаміці дозволяє визначати нові аспекти у процесах децентралізації, спостерігати зміну пріоритетів, визначати напрямки соціально-правової активності. На прикладах показана адекватність підходу, що пропонується, а також, що кластери в термінологічних мережах можуть розглядатися як основа для визначення окремих наукових напрямків.

**Ключові слова:** модель предметної області, термінологічна база, контент-моніторинг, зв’язки понять, децентралізація.

**Аннотация.** В работе приводится алгоритм построения моделей терминологических сетей в предметной области “децентрализация” на базе автоматизированного мониторинга и анализа контента сети Интернет. Термины естественного языка, отражающие понятия, состав и содержание которых динамично изменяется, образуют сети. Исследование этих сетей в динамике позволяет определять новые аспекты в процессах децентрализации, наблюдать изменение приоритетов, определять направления социально-правовой активности. На примерах показана адекватность предлагаемого подхода, а также то, что кластеры в терминологических сетях могут рассматриваться как основа для определения отдельных научных направлений.

**Ключевые слова:** модель предметной области, терминологическая база, контент-мониторинг, связи понятий, децентрализация.

**Summary.** The algorithm of creation of models of subject domains on decentralization on the basis of computer aided data analysis and Internet content monitoring is offered in the article. Terms of natural language reflecting concepts, composition and content of which change dynamically, form networks. The study of these networks in dynamics allows us to define new aspects in the processes of decentralization, observe changes in priorities, and determine the directions of social and legal activity. Adequacy of the approaches offered is shown by example, and also the fact that clusters of terminological networks can be considered as a basis for detection of certain scientific directions.

**Keywords:** subject domain model, terminology-oriented database, content monitoring, links of concepts, decentralization.

**Постановка проблеми.** Децентралізація влади – це процес перерозподілу або диспергування функцій, повноважень, людей або речей від центрального управління [1]. Децентралізація влади (далі – децентралізація) здійснюється шляхом передання повноважень на прийняття рішень з головного органу будь-якої галузі уряду до органів нижчих рівнів. Тобто при цьому частина функцій центральної влади переходить до органів самоврядування; скасування або послаблення централізації. Цей процес який було названо “новим державним управлінням”, описаний як децентралізація, предметне управління, конкуренція урядової і місцевої координації [2].

Відповідно до Європейської Хартії Місцевого Самоврядування від 15 жовтня 1985 року., зміст місцевого самоврядування полягає у гарантованому державою праві та реальній здатності самих територіальних спільнот громадян (територіальних колективів) та сформованих ними органів самостійно та під свою відповідальність вирішувати окрему частину публічних справ, діючи в межах конституції та законів відповідної держави. Органи місцевого самоврядування визнано однією з головних підвалин будь-якого демократичного режиму.

Децентралізація в Україні має давню історію, що була започаткована ще у Конституції Української Народної Республіки (1918 р.). На цей час в Україні здійснюються процеси децентралізації – передачі значних повноважень та бюджетів від державних органів органам місцевого самоврядування. Вважається, що необхідно, щоб більше повноважень мали ті органи, які ближче до людей, де такі повноваження реалізуються успішніше.

Децентралізація являє собою динамічний процес, що охоплює всі ланки суспільно-правового поля країни. На різних етапах цього процесу застосовуються різні підходи, іноді правильні, іноді хибні. На цей час актуальною є проблема дослідження цих підходів, побудова моделей, що дозволяють вивчати процеси децентралізації, створення інструментальних засобів для підтримки прийняття рішень щодо процесів децентралізації особами, що приймають ці рішення.

**Метою статті** є опис термінологічної мережевої моделі на базі моніторингу мережевих ЗМІ, що відображає динаміку процесів децентралізації в Україні.

**Виклад основного матеріалу.** Як вважаємо, зазначена вище модель має застосовуватися як інструментальна база для підтримки прийняття рішень щодо процесів децентралізації особами, що приймають ці рішення. На цей час на веб-сайтах та у соціальних мережах в Інтернеті публікуються сотні тисяч повідомлень, що репрезентативно відображають стан соціально-правових процесів. На базі цієї інформації можлива побудова термінологічних мереж, що відбивають найважливіші поняття з предметних областей і семантичні зв'язки між ними [3]. За допомогою побудови і подальшого дослідження цих мереж можна визначати найбільш важливі і актуальні поняття, а також зв'язки між ними, динаміку їх застосувань у часі. Виявлення груп найбільш близьких за деякими змістовими характеристиками понять (кластерів) дозволяє визначати нові принципи класифікації процесів, що досліджуються, спостерігати зміну пріоритетів, визначати напрямки соціально-правової активності. Побудовані термінологічні мережі можуть бути розвинуті до рівня сучасних онтологій [4], когнітивних карт [5], що можуть ставати основою сценарного аналізу, відпрацювання соціально-правових процесів в предметній області (децентралізації), сюжетів майбутніх змін.

#### **Методика побудови моделі.**

На першому етапі побудови термінологічної моделі процесів децентралізації необхідно сформулювати репрезентативний текстовий корпус. Для цього авторами було застосовано систему контент-моніторингу InfoStream [6], за допомогою якої за запитом: *(децентралізац|деконцентрац|диспергуванн|делегуван|діволюц)&(влад)|(державн~управл інн)|самоврядуван)* було отримано 457 документів з україномовних веб-сайтів мережі Інтернет за визначеною тематикою за 1 – 12 червня 2017 року (Рис. 1).

На другому етапі здійснюється екстрагування термінів (окремих слів – уніграм, пари слів – біграм, і трійки – триграм) із відібраного на першому етапі текстового корпусу. Для підвищення точності термінів (міри їх відповідності тематиці децентралізації) до розгляду із текстового корпусу розглядаються лише абзаци, що відповідають первинному запиту.

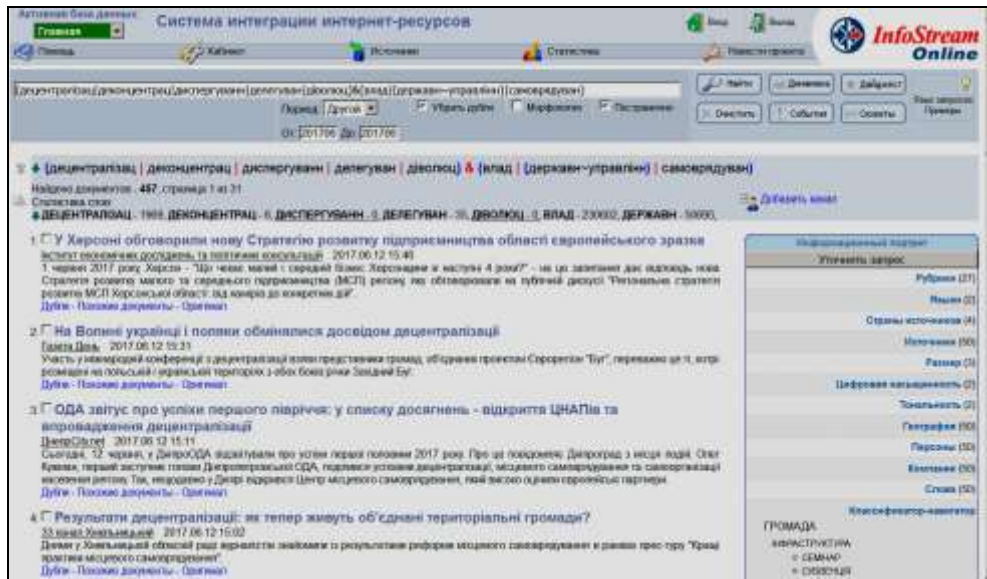


Рис.1 – Інтерфейс системи контент-моніторингу InfoStream

Витяг найбільш релевантних термінів здійснюється за дисперсійною моделлю [7]. Як міра важливості (ваги) термінів розглядається оцінка нерівномірності її входження у тексти. Для цього використовується така оцінка дискримінантної ваги терміна:

$$\sigma_i = \frac{\sqrt{\langle d^2 \rangle - \langle d \rangle^2}}{\langle d \rangle}$$

де:  $\langle d \rangle$  – середнє значення послідовності  $d_1, d_2, \dots, d_n$ ,  $n$  – кількість появ терміна  $t_i$  в інформаційному масиві. Тут  $d_k$  – відстань між появами терміна в тексті. Якщо позначити координати (номери) входження слова  $t_i$  в інформаційний масив як  $e_1, e_2, \dots, e_n$ , то  $d_k = e_k - e_{k-1}$  ( $e_0 = 0$ ).

На цьому етапі кожному окремому слову, словосполученню із двох слів (біграм) та із трьох слів (триграм) з текстового корпусу, що аналізується, ставиться у відповідність дисперсійна оцінка  $\sigma_i$ . Після цього всі терміни (окремо уніграми, біграми і триграми) сортуються за вагою і вибирається визначена експертами кількість найбільш вагомих цих термінів. Крім того, експерти додатково здійснюють візуальну фільтрацію слів, вилучаючи “зайві”, явно не релевантні тематиці.

На третьому етапі із відібраних термінів формується термінологічна мережа. Відомо декілька підходів до побудови мереж з текстів і різні способи інтерпретації вузлів і зв’язків, що призводить, відповідно, до різних видів представлення таких мереж. Вузли можуть бути сполучені між собою, якщо відповідні їм слова стоять поряд у тексті, належать до одного речення або абзацу, сполучені синтаксично або семантично [8].

**Термінологічна мережа.**

Традиційно розрізняють чотири різновиди мереж мови (просторів):

1. *L*-простір. Зв’язуються сусідні слова (терміни), які належать до одного речення. Кількість сусідів для кожного слова (вікно слова) визначається радіусом взаємодії  $R$ , найчастіше розглядається випадок  $R = 1$ .



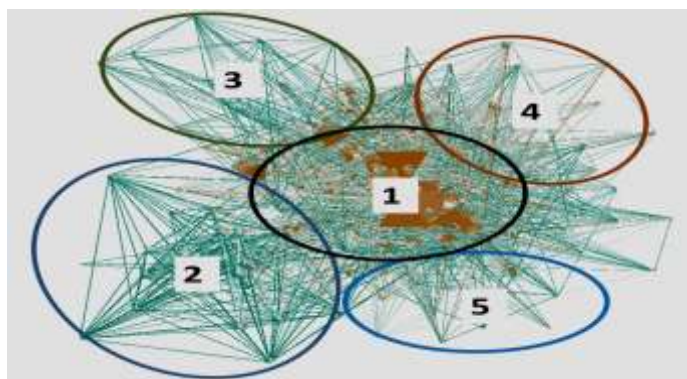


Рис. 3 – Кластерна структура мережі

Шляхом аналізу складу кластерів визначено такі основні напрямки термінології, що визначають процеси децентралізації в Україні на початок червня 2017 р.:

|          |                                         |                                       |
|----------|-----------------------------------------|---------------------------------------|
| <b>1</b> | <b>Загальні питання децентралізації</b> | УКРАЇНА                               |
|          |                                         | ДЕЦЕНТРАЛІЗАЦІЯ                       |
|          |                                         | ПРОЕКТ                                |
|          |                                         | ПРОЕКТ ДЕЦЕНТРАЛІЗАЦІЇ                |
|          |                                         | СТРАТЕГІЯ ОБ'ЄДНАННЯ                  |
|          |                                         | ПРОЕКТ РЕГІОНАЛЬНОГО РОЗВИТКУ         |
|          |                                         | СУСПІЛЬСТВО                           |
|          |                                         | ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО              |
|          |                                         | ЗМІНИ КОНСТИТУЦІЇ УКРАЇНИ             |
| <b>2</b> | <b>Місцеве самоврядування</b>           | ГРОМАДА                               |
|          |                                         | ГРОМАДИ УКРАЇНИ                       |
|          |                                         | РОЗВИТОК МІСЦЕВОГО САМОВРЯДУВАННЯ     |
|          |                                         | ОТГ                                   |
|          |                                         | ОЧІЛЬНИК                              |
|          |                                         | МЕР                                   |
|          |                                         | ФІНАНСУВАННЯ                          |
|          |                                         | МІСЬКИЙ ГОЛОВА                        |
| <b>3</b> | <b>Правове забезпечення</b>             | НОРМАТИВНО-ПРАВОВІ АКТИ               |
|          |                                         | ПРАВОВІ АКТИ                          |
|          |                                         | АДМІНІСТРАТИВНО-ТЕРИТОРІАЛЬНА РЕФОРМА |
| <b>4</b> | <b>Державні органи, посадові особи</b>  | ВЕРХОВНА РАДА                         |
|          |                                         | КОМІТЕТ                               |
|          |                                         | АГРАРНИЙ КОМІТЕТ                      |
|          |                                         | ПРЕМ'ЄР ВОЛОДИМИР ГРОЙСМАН            |
|          |                                         | АНДРІЙ ПАРУБІЙ                        |
| <b>5</b> | <b>Європейський вибір</b>               | ЄВРОПЕЙСЬКІ КРАЇНИ                    |
|          |                                         | ОФІС РАДИ ЄВРОПИ                      |
|          |                                         | ЄВРОПЕЙСЬКА ІНТЕГРАЦІЯ                |

**Висновки.**

Децентралізація – складний, багатогранний процес, який визначає не лише перерозподіл владних повноважень по всій ієрархії системи державного управління, а й перерозподіл сфер обов’язків та відповідальності, фінансових і інформаційно-правових потоків. В цих умовах, особливо з огляду на суттєву трансформацію суспільних відносин, дуже велику роль відіграють саме інформаційно-правові потоки, питання запобігання та своєчасного усунення реальних та потенційних колізій у правовому полі, що стрімко буде розширюватися.

Децентралізація являє собою динамічний процес, що охоплює всі ланки суспільно-правового поля країни. На різних етапах цього процесу застосовуються різні підходи, іноді правильні, іноді хибні.

У роботі запропоновано і реалізовано алгоритм формування моделей предметних областей шляхом автоматизованого аналізу контенту мережі Інтернет. Від статичних моделей предметних областей таких підхід відрізняється урахуванням динамічної зміни контенту бази даних цього сервісу, урахуванням нових понять, феноменів, що з’являються, зокрема в юридичній області, що розглядається.

Процеси децентралізації знаходять своє відображення у мовному середовищі. Терміни природної мови, що відображають поняття, склад і зміст яких динамічно змінюється, утворюють мережі. Дослідження цих мереж у динаміці дозволяє визначити нові аспекти у процесах децентралізації, спостерігати зміну пріоритетів, визначити напрямки соціально-правової активності.

Запропонована модель, що базується на моніторингу і подальшому аналізі мережевого контенту, має застосовуватися як інструментальна база для підтримки прийняття рішень щодо процесів децентралізації особами, що приймають ці рішення.

**Використана література**

1. Definition of decentralization, TheFreeDictionary.com, accessed February 4, 2013.
2. Managing Decentralisation : A New Role for Labour Market Policy, Organisation for Economic Co-operation and Development, Local Economic and Employment Development (Program), OECD Publishing, 2003. – P. 135.
3. Ландэ Д.В., Снарский А.А., Путятин В.Г. Построение терминологической сети предметной области // Реєстрація, зберігання і обробка даних. – 2014. – Т. 14. – № 2. – С. 114-121.
4. Ландэ Д.В., Снарский А.А. Автоматическое построение терминологических онтологий // Proceedings of the XX-th International Conference Knowledge-Dialogue-Solution 2014, Kyiv, Ukraine. – Pp. 28-71.
5. Кузнецов О.П. Когнитивное моделирование слабо структурированных ситуаций / О.П. Кузнецов. – М. : Политехнический музей, 2006. – С. 86-100.
6. Ланде Д.В. Программно-апаратний комплекс інформаційної підтримки прийняття рішень : науково-методичний посібник / Д.В. Ланде, В.М. Фурашев, О.М. Григор’єв. – К. : Іжніринг, 2006. – 48 с.
7. Ortuño M., Carpena P., Bernaola P., Muñoz E., Somoza A.M. Keyword detection in natural languages and DNA // Europhys. Lett., 2002. – 57. – P. 759-764.
8. Ланде Д.В. Элементы компьютерной лингвистики в правовой информатике. – К.: НДПП НАПрН України, 2014. – 168 с.

~~~~~ \* \* \* ~~~~~

УДК 342.53:004

ДОРОГИХ С.О., старший науковий співробітник
НДІ інформатики і права НАПрН України

МОДЕЛЬ НАЦІОНАЛЬНОЇ СИСТЕМИ ПРАВОВОЇ ІНФОРМАЦІЇ В УКРАЇНІ

Анотація. До питання моделі побудови національної системи правової інформації.

Ключові слова: Електронний парламент, Парламент, Верховна Рада України, Національна система правової інформації.

Аннотация. К вопросу модели построения национальной системы правовой информации.

Ключевые слова: Электронный парламент, Парламент, Верховная Рада Украины, Национальная система правовой информации.

Summary. To the question of building a model of the national system of legal information.

Keyword: Electronic parliament, Parliament, Verkhovna Rada of Ukraine, National system of legal information.

Постановка проблеми. Євроінтеграційний рух та процеси демократизації, що відбуваються в країні, порушують питання як щодо покращення рівня прийнятих законів та інших нормативних актів, так і щодо збільшення прозорості діяльності органів влади, залучення громадян до законотворчого та нормотворчого процесів. У той же час процес децентралізації владних повноважень в країні у найближчому майбутньому створить розгалужену систему місцевих баз правової інформації, до яких необхідно встановити доступ для усіх громадян, які проживають чи працюють у цій місцевості.

Вирішення поставлених питань буде відбуватися, на нашу думку, й завдяки впровадженню Національної системи правової інформації.

Метою статті є представлення моделі Національної системи правової інформації.

Виклад основного матеріалу. Першою спробою створення Національної системи правової інформації була Постанова Президії Верховної Ради України “Про організацію роботи по формуванню єдиної системи правової інформації в Україні” від 26 грудня 1994 р. № 308/94-ПВ [1], яка зокрема містила положення про необхідність створення загальнодержавної системи правової інформації в Україні з метою підвищення рівня правотворчої і правозастосувальної діяльності органів державної влади, а також створення найбільш сприятливих умов користування правовою інформацією громадянам, установам, організаціям і суб’єктам підприємницької діяльності в Україні.

На виконання Постанови 308/94-ПВ була розроблена Концепція правової інформатизації [2, с. 49]. Важливою складовою правової інформатизації були запропоновані у Концепції інформатизована система правового забезпечення України та розподілений банк правових документів.

Ядром інформатизованої системи правового забезпечення України планувався розподілений банк правових документів. За задумом розподілений банк являв собою сукупність баз даних правових документів органів, які є джерелами правової інформації, об’єднаних каналами зв’язку та апаратурою передавання даних. Поступово кожний з органів державної влади, що видає нормативно-правові документи, формував би власну базу даних нормативних документів. В подальшому ці бази об’єднувались би у одну загальнодержавну базу, доступ до якої мали б усі органи влади, та окремі громадяни [2].

5 липня 2012 року була прийнята Програма інформатизації законотворчого процесу у Верховній Раді України на 2012 – 2017 роки, яка ставила за мету досягнення максимально можливої автоматизації інформаційно-організаційних процесів у діяльності депутатського корпусу загалом, у тому числі комітетів Верховної Ради України, депутатських фракцій, а також Апарату Верховної Ради України шляхом створення сучасних систем управління законотворчим процесом та документообігом у парламенті; оперативне інформаційно-аналітичне забезпечення народних депутатів України, помічників-консультантів народних депутатів України, фахівців Апарату Верховної Ради України; створення нової автоматизованої системи обробки вхідних, вихідних, внутрішніх інформаційно-документальних потоків та контролю за виконанням доручень, оперативне формування аналітично-звітної та довідкової документації; технічне удосконалення систем зв'язку для забезпечення оперативності у роботі народних депутатів України, комітетів Верховної Ради України, Апарату Верховної Ради України, у тому числі щодо питань, пов'язаних з діяльністю органів виконавчої влади, органів місцевого самоврядування, інформуванням громадян [3].

Пріоритетним завданням Програми планувалося створення інтегрованої електронної інформаційно-аналітичної системи “Електронний парламент”. Аналізуючи даний проект, можна зауважити, що в разі побудови такого інформаційного комплексу на базі Верховної Ради України була би побудована потужна система, яка би стала ядром майбутньої Національної системи правової інформації та могла в подальшому бути інтегрованою з інформаційними системами інших органів влади.

3 липня 2015 р. Головою Верховної Ради України Володимиром Гройсманом та Президентом Європейського парламенту Мартіном Шульцем було підписано Меморандум про взаєморозуміння між Верховною Радою України та Європейським парламентом про спільні рамки парламентської підтримки та підвищення інституційної спроможності.

З метою сприяння впровадженню положень Меморандуму, Європейським парламентом було започатковано роботу Місії з оцінки потреб, яку очолив колишній президент Європейського парламенту Пет Кокс. Метою Місії було визначити, у співпраці з представниками Верховної Ради України, напрями посилення українського парламенту як ефективної демократичної інституції. Результатом цієї роботи стала Доповідь та Дорожня карта, висновки якої покликані покращити результати законодавчої роботи Верховної Ради та її інституційну ефективність.

Програма передбачає, що створена система забезпечить не лише повну автоматизацію етапів законотворчого процесу, а й інформаційну взаємодію Верховної Ради України з іншими органами державної влади та органами місцевого самоврядування, громадянами, юридичними особами за допомогою сучасних інформаційно-комунікаційних технологій із застосуванням високих стандартів доступу до інформаційних ресурсів парламенту [4]. В той же час Дорожня карта рекомендує посилити координацію між ініціаторами законодавства у Кабінеті Міністрів України, Адміністрації Президента України та Верховній Раді України та створити спільну систему електронного документообігу (так званий “законотворчий трикутник”).

Отже на основі попередніх концепцій ми пропонуємо наступну схему моделі Національної системи правової інформації (див. Рис.).

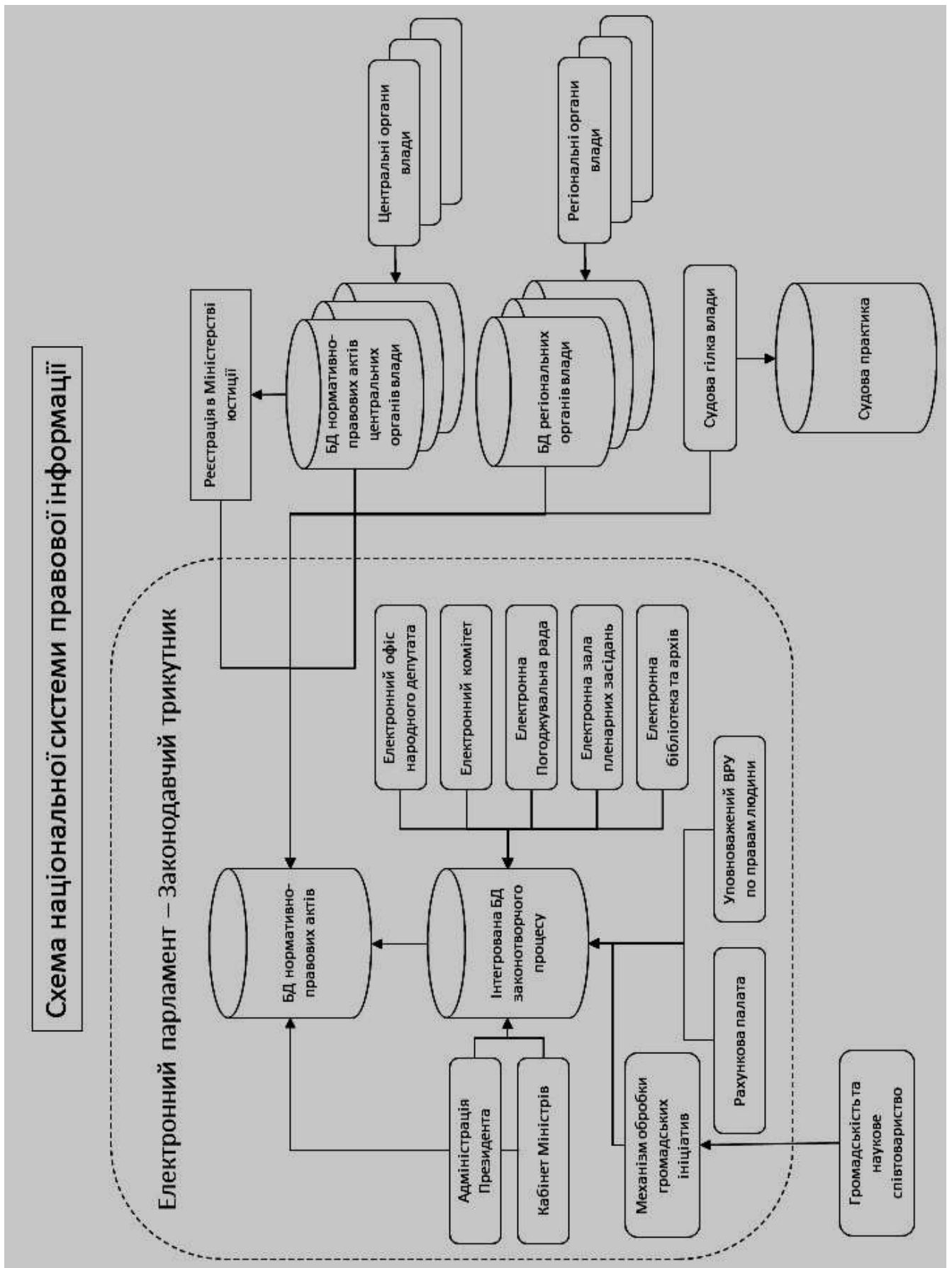


Рис. Схема моделі Національної системи правової інформації

В основі моделі знаходяться два основних елемента: інтегрована база даних законотворчого процесу та база даних нормативно-правових актів (далі – БД НПА). Схема побудована з урахуванням впровадження рекомендацій місії Пета Кокса щодо поєднання електронного документообігу та інформаційних систем “законодавчого трикутника”. Ядро системи пов’язано з іншими елементами системи – інформаційними системами центральних органів влади та інформаційними системами місцевих органів влади. В подальшому до системи можуть бути підключені інформаційні системи судової гілки влади або, навіть, інформаційні системи наукових та навчальних установ, які працюють у галузі права.

Інтегрована база даних законотворчого процесу (далі – ІБД ЗП) передбачається як один з головних елементів “Електронного парламенту”. За задумом авторів Програми інформатизації законотворчого процесу у Верховній Раді України на 2012 – 2017 роки вона повинна бути пов’язана зі всіма підсистемами “Електронного парламенту”, такими як “Електронний офіс народного депутата”, “Електронний комітет”, “Електронна погоджувальна рада” та ін. На нашу думку вона також повинна бути пов’язана й з інформаційними системами Рахункової палати та Уповноваженого Верховної Ради України з прав людини.

Важливою частиною ІБД ЗП є механізм обробки громадських ініціатив. Наразі є питання залучення громадянського суспільства та наукового співтовариства до законотворчого процесу. Розглядаються різні форми такого залучення – від подання народних петицій, проведення громадських слухань, участі представників громадськості у роботах робочих груп комітетів Верховної Ради або спеціальних дорадчих консультативних органів і до публікації зауважень до законопроектів безпосередньо у ІБД ЗП.

На початку роботи з утворення механізму обробки громадських ініціатив може виникнути проблема з порівняно низьким рівнем якості поданих громадських проектів, проте в подальшому автори, що подають ґрунтовні та професійні пропозиції можуть бути виявлені та включені до робочих груп. На думку автора, особливо важливим є врахування зауважень наукового співтовариства та публікація їх аналітичних матеріалів щодо законопроектів та практики застосування чинних нормативно-правових актів. Відповідно до ІБД ЗП зможуть надходити матеріали, які можуть бути використані народними депутатами при створенні законопроектів.

База даних нормативно-правових актів повинна зберігати всі видані в Україні нормативно-правові акти та, за нашою думкою, бути офіційним джерелом публікації нормативно-правових актів в електронному вигляді. Документи Верховної Ради України, Президента України та Кабінету Міністрів надходять безпосередньо до бази даних нормативно-правових актів (Закони України після проходження через інтегровану базу даних законотворчого процесу). Документи центральних органів влади потрапляють до БД НПА з власних баз даних після реєстрації у Міністерстві юстиції або відразу (для документів, що не потребують такої реєстрації). Також до БД НПА надходять документи судової гілки влади.

На сьогодні БД НПА створена на базі Верховної Ради України й вже знаходиться у вільному доступі на офіційному веб-порталі парламенту, проте відсутність прийнятих єдиних технічних форматів створення, збереження та обміну нормативно-правовими документами у електронній формі між різними органами влади призводить до зайвих витрат держави, повторного введення одного й того ж самого нормативно-правового документа в різних державних базах даних, зниження актуальності при публікації роз’яснень та інших документів органів влади, які не реєструються у Міністерстві

юстиції України. Це є однією з головних проблем для створення й функціонування Національної системи правової інформації. Саме відсутність таких стандартів не дає можливості інтегрувати інформаційні системи різних органів влади на всіх рівнях.

Відзначимо, що на кожному рівні (від законотворчого процесу у парламенті до вирішення питань на рівні окремої громади) системи повинна бути реалізована система залучення громадськості до нормотворчого процесу.

Висновки.

Побудова Національної системи правової інформації дозволяє створити не лише інтегровану систему нормативно-правових ресурсів усіх органів влади (починаючи від центральних і закінчуючи рівнем громад), але й впровадити механізми участі громадян у законотворчому та нормотворчому процесах, а також забезпечити вільний доступ до всього масиву нормативно-правових документів на всій території країни та публічної інформації щодо діяльності органів влади на всіх рівнях.

В її основі знаходяться як бази нормативно-правових документів, так і елементи залучення громадян до участі у прийнятті рішень, законотворчому та нормотворчому процесах.

Обов'язковою передумовою існування такої системи є впровадження єдиних стандартів (бажано відкритих) створення, збереження та обміну інформацією між усіма елементами системи.

На нашу думку, побудова Національної системи правової інформації може бути розпочата з системи “Електронного парламенту” Верховної Ради України, а у разі виконання Дорожньої карти щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України – з інтегрованої системи “законодавчого трикутника” (інформаційних систем Верховної Ради, Адміністрації Президента та Кабінету Міністрів України).

У своєму кінцевому результаті впровадження Національної системи правової інформації спрямоване на покращення якості створюваних законопроектів та побудови громадянського суспільства, котре бере активну участь в управлінні країною.

Використана література

1. Про організацію роботи по формуванню єдиної системи правової інформації в Україні : Постанова Президії Верховної Ради України від 26.12.94 р. № 308/94-ПВ. – Режим доступу : <http://zakon.rada.gov.ua>

2. Інформатизація законотворчої, нормотворчої, правозастосовної та правоосвітньої діяльності : посібник / [Л.Є. Горьовий, М.Я. Швець, Т.Г. Дрогаль та ін.]. – К. : Парламентське видавництво, 1999. – 199 с.

3. Про затвердження Програми інформатизації законотворчого процесу у Верховній Раді України на 2012 – 2017 роки : Постанова Верховної Ради України від 05.07.12 р. № 5096-VI. – Режим доступу : <http://zakon.rada.gov.ua>

4. Доповідь та дорожня карта щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України. – (Підготовлена Місією Європейського парламенту з оцінки потреб під головуванням Пета Кокса, Президента Європейського парламенту 2002 – 2004 рр., вересень 2015 – лютий 2016 рр. – Режим доступу : <http://www.europarl.europa.eu/resources/library/media/20160301RES16508/20160301RES16508.pdf>

~~~~~ \* \* \* ~~~~~

**Інформаційна і національна безпека**

УДК 328.185:342:351.746

**СКУЛИШ Є.Д.**, доктор юридичних наук, професор,  
**ІРХА Ю.Б.**, науковий консультант судді Конституційного Суду України

**ВЗАЄМОЗВ'ЯЗОК КОРУПЦІЇ ТА ЕКСТРЕМІЗМУ:  
ПРОБЛЕМИ ПРОТИДІЇ**

**Анотація.** У статті висвітлено існуючі взаємозв'язки між проявами корупції та екстремізму. Наголошено, що корупція стала фактором формування та діяльності організованої злочинності, у тому числі міжнародної. Звертається увага на суттєве сприяння корупції в організації різноманітної екстремістської діяльності та її впливу на формування екстремістської поведінки та мислення у деяких громадян. У результаті дослідження виокремлено два основних напрями впливу корупції на появу та поширення екстремізму у суспільстві.

**Ключові слова:** корупція, екстремізм, міжнародна і національна безпека, організована злочинність, порушення прав і свобод людини

**Аннотация.** В статье освещены существующие взаимосвязи между проявлениями коррупции и экстремизма. Отмечено, что коррупция стала фактором формирования и деятельности организованной преступности, в том числе международной. Обращается внимание на существенное содействие коррупции в организации разнообразной экстремистской деятельности и ее влияния на формирование экстремистского поведения и мышления некоторых категорий граждан. В результате исследования выделены два основных направления влияния коррупции на появление и распространение экстремизма в обществе.

**Ключевые слова:** коррупция, экстремизм, международная и национальная безопасность, организованная преступность, нарушение прав и свобод человека

**Summary.** The article highlights the existing relationship between acts of corruption and acts of extremism. Authors emphasize that corruption has become a factor of formation and activities of organized crime, including international. Attention is drawn to the significant corruption facilitation in the organization of various extremist activity and its influence on the formation of extremist thinking and behavior in some people. The study singled out two main areas of impact of corruption on the appearance and spread of extremism in the society.

**Keywords:** corruption, extremism, international and national security, organized crime, violation of rights and freedoms.

**Постановка проблеми.** Поява та розвиток у державі кампаній громадянської непокори (протестів, мітингів, пікетів, страйків, перекриття транспортних магістралей, захоплення адміністративних будинків тощо), а також проявів екстремізму та тероризму завжди пов'язане із наявністю у суспільстві суттєвих політичних, релігійних, соціально-економічних та інших протиріч. Перехід громадян до активної протестної діяльності, у тому числі протиправної, відбувається, як правило, у разі невчасного виявлення та/або невдалого врегулювання органами публічної влади відповідного конфлікту інтересів між різними категоріями осіб. Радикалізація громадян, використання ними екстремістських та терористичних методів і способів відстоювання своїх поглядів та цінностей, захисту прав, свобод та інтересів, як законних, так і вигаданих ними, вказують на невирішені системні проблеми у соціумі, до яких належить, зокрема, корупція.

На нашу думку, корупція не є основною детермінантою екстремізму і його крайньої форми – тероризму, однак вона суттєво сприяє організації різноманітної екстремістської діяльності. За певних умов корупція може мати вплив на формування екстремістських установок у деяких громадян, особливо соціально вразливих.

**Результати аналізу наукових публікацій.** Дослідження корупції, особливостей її проявів, наслідків та механізмів протидії здійснюється на міжнародному та національному рівні. Цими питаннями займаються універсальні та регіональні міжнародні організації, різноманітні громадські організації, вчені та фахівці з різних галузей знань. Серед вітчизняних вчених-юристів ґрунтовні наукові розробки цих проблем здійснювали Л. Багрій-Шахматов, В. Гарашук, О. Дудоров, О. Калиновський, В. Клименко, М. Коржанський, М. Мельник, В. Навроцький, Є. Невмержицький, В. Сташис, М. Хавронюк, В. Шакур, О. Ярмиш та інші.

У процесі опрацювання наукових робіт, присвячених проблемам протидії корупції, ми виявили недостатнє наукове опрацювання питання впливу корупції на появу та поширення екстремізму у суспільстві. Саме тому це питання і стало предметом нашого наукового пошуку.

**Метою статті** є висвітлення взаємозв'язку корупції та екстремізму.

Для реалізації вказаної мети необхідно: з'ясувати сутність корупції, виявити зв'язок між корупцією та екстремістською діяльністю; проаналізувати вплив корупції на формування екстремістських установок у індивідів; розробити пропозиції щодо вдосконалення механізмів протидії екстремізму та корупції.

**Виклад основного матеріалу.** Корупційні прояви відомі з давніх часів. У межах різних історичних епох протидія корупції відбувалася у різних формах – від насильницьких (жорстоких) до ліберальних (гуманних), однак люди досі не перестали вчиняти корупційні правопорушення. Більше того, в окремих державах корупція стала “національною особливістю” як державного управління, так і міжособистісних відносин. Корупція становить загрозу для стабільності, розвитку й безпеки суспільства і держави. Її прояви зсередини підривають існуючі демократичні здобутки, етичні та моральні цінності, руйнують засади ринкової економіки, а також перешкоджають ефективній реалізації та захисту прав і свобод людини і громадянина.

У Кодексі поведінки посадових осіб органів правопорядку, затвердженому Резолюцією Генеральної Асамблеї Організації Об'єднаних Націй від 17 грудня 1979 року № 34/169, зазначено, що поняття “корупція” охоплює, зокрема, скоєння певних дій при виконанні обов'язків або у зв'язку з цими обов'язками в результаті прийнятих подарунків, обіцянок чи стимулів або їх незаконне одержання кожного разу, коли має місце така дія або бездіяльність (стаття 7) [1].

Відповідно до Закону України “Про запобігання корупції” від 14 жовтня 2014 року № 1700-VII корупція визначається як використання особою, уповноваженою на виконання функцій держави або місцевого самоврядування, наданих їй службових повноважень чи пов'язаних з ними можливостей з метою одержання неправомірної вигоди або прийняття такої вигоди чи прийняття обіцянки/пропозиції такої вигоди для себе чи інших осіб або відповідно обіцянка/пропозиція чи надання неправомірної вигоди особі, уповноваженій на виконання функцій держави або місцевого самоврядування, або на її вимогу іншим фізичним чи юридичним особам з метою схилити цю особу до протиправного використання наданих їй службових повноважень чи пов'язаних з ними можливостей [2].

На думку П. Добродумова, корупція – це симптом того, що в системі державного управління існують серйозні дефекти. Державні інститути, створені для регулювання

взаємовідносин між громадянином і державою, замість цього використовуються для особистого збагачення і надання пільг корумпованим господарюючим суб'єктам. Ціновий механізм, який повинен бути джерелом економічної ефективності, стимулятором економічного зростання, може – у формі хабара – підірвати легітимність і ефективність державної влади.

Дослідник справедливо наголошує, що корупція як соціальне явище притаманна усім без винятку державам світу, вона є невід'ємним атрибутом публічної влади. Це явище існувало, існує і буде існувати, доки існує держава та публічна влада. Відмінність різних держав полягає не у наявності чи відсутності корупції як такої, а в її масштабах, характері корупційних проявів, впливу корупції на економічні, політичні, правові та інші соціальні процеси [3, с. 51-52].

За твердженнями професора М. Мельника корупція, характеризує основні соціальні процеси, які відбуваються в державі та суспільстві і відображає найбільш значущі для держави й суспільства проблеми. У корупції проявляється неефективність влади й економіки, недосконалість найбільш важливих державних та суспільних інститутів. У країнах, де корупція набуває значного поширення і суттєвого впливу на соціально-економічні процеси, вона із соціальної аномалії (патології) поступово перетворюється на звичайний спосіб вирішення проблем, стає нормою функціонування влади і стилем життя значної частини громадян. Корупція як соціальне явище існує в певних інституціональних рамках, у яких відбувається взаємовплив між нею та економічними, політичними, правовими, соціальними процесами [4, с. 10].

Виникнення і зростання корупції, як вважає В. Мартиновський, відбувається в певному соціальному середовищі, що створює для неї сприятливі умови. Загальною умовою її розвитку є перебування держави в перехідному етапі, що являє собою якісні зміни соціальних, політичних та економічних інститутів і зв'язків. Зміна пріоритетів, норм і цінностей, що виступають у ролі критеріїв оцінки будь-якого соціального явища чи поведінки членів суспільства, призводить до формування в суспільстві різних точок зору. Влада як засіб управління переходить від однієї керівної соціальної групи до іншої, між ними виникає боротьба за панівне соціальне становище. Державна влада і право стають для керівників засобом нав'язування власної волі. У зв'язку з цим, такі риси перехідного періоду, як слабкість державної влади та соціального контролю, загострене соціальне протистояння, відсутність ефективної правової системи якісно характеризують середовище, де виникає і розвивається корупція [5, с. 52].

Загальновідомо, що на сьогодні корупція вже давно вийшла за межі державних кордонів, вона почала суттєво впливати на міжнародні та міждержавні відносини, спотворюючи їх сутність. В окремих випадках корупція відіграє значну роль у сприянні в організації, скоєнні та приховуванні різних злочинів. Крім того, корупція стала фактором формування та діяльності організованої злочинності, у тому числі міжнародної.

Наведене не могло залишитися без уваги та реагування з боку міжнародних організацій, які сформувавши універсальні антикорупційні стандарти з метою захисту прав і свобод людини і громадянина, а також найважливіших людських здобутків і цінностей.

Так, Організація Об'єднаних Націй (далі – ООН) від 31 жовтня 2003 року ухвалила Конвенцію проти корупції, в якій закріпила, що кожна Держава-учасниця, згідно з основоположними принципами своєї правової системи, розробляє й здійснює або проводить ефективну скоординовану політику протидії корупції, яка сприяє участі суспільства і яка відображає принципи правопорядку, належного управління

державними справами й державним майном, чесності й непідкупності, прозорості й відповідальності (стаття 5) [6].

Генеральна асамблея ООН Резолюцією від 17 грудня 1979 року № 34/169 затвердила Кодекс поведінки посадових осіб органів правопорядку, Резолюцією від 12 грудня 1999 року № 51/59 схвалила Міжнародний кодекс поведінки державних посадових осіб, а Резолюцією від 16 грудня 1996 року № 51/191 – Декларацію про боротьбу з корупцією та хабарництвом у міжнародних комерційних операціях. Крім того, на VIII Конгресі ООН з запобігання злочинності було ухвалено Резолюцію “Практичні заходи боротьби з корупцією” від 7 вересня 1990 року.

У межах Ради Європи прийнято Кримінальну конвенцію про боротьбу з корупцією від 27 січня 1999 року, Додатковий протокол до Кримінальної конвенції про боротьбу з корупцією від 15 травня 2003 року та Цивільну конвенцію про боротьбу з корупцією від 4 листопада 1999 року, в якій закріплено що “корупція” означає прямі чи опосередковані вимагання, пропонування, дачу або одержання хабара чи будь-якої іншої неправомірної вигоди або можливості її отримання, які порушують належне виконання будь-якого обов’язку особою, що отримує хабара, неправомірну вигоду чи можливість мати таку вигоду, або поведінку такої особи (стаття 2) [7].

До того ж, під егідою Ради Європи у 1998 році утворено Групу держав по боротьбі з корупцією (GRECO), метою діяльності якої є удосконалення компетентності її членів у боротьбі з корупцією для вжиття заходів через динамічний процес спільного оцінювання методів проведення та однакового впливу згідно з їхніми зобов’язаннями в цій сфері.

Незважаючи на загально визнану необхідність запобігання корупційним правопорушенням, створення національних та міжнародних механізмів боротьби з ними, у багатьох державах масштаби корупції суттєво не зменшились. Прояви політичної, ділової, соціальної та побутової корупції не зустрічають дієвих контрзаходів. Значна кількість пересічних громадян, підприємців, чиновників, політиків публічно засуджують ці прояви, однак у повсякденному житті їм реально важко відмовитись від переваг, які вони отримують завдяки корупційним діям.

У 2016 році у Великій Британії (м. Лондон) відбувся антикорупційний саміт, на якому було ухвалено Декларацію по боротьбі з корупцією та відповідне комюніке, в якому зазначено, що корупція є джерелом багатьох світових проблем. Вона підриває довіру суспільства до державної влади, нівелює принцип верховенства права, а також може призвести до невдоволення суспільства на політичному й економічному ґрунті, яке, у поєднанні з іншими факторами, може стати поштовхом до насильницького екстремізму [8].

Генеральний Секретар ООН Пан Гі Мун, представляючи на Генеральній Асамблеї ООН свій “План дій щодо попередження войовничого екстремізму”, підкреслив, що войовничий екстремізм, як правило, процвітає в умовах відсутності демократії, неефективного управління, корупції та безкарності держави або її представників у випадку протиправної поведінки [9]. За даними Агентства США з міжнародного розвитку повсюдна корупція і безкарність еліт є однією із семи політичних умов, які зумовлюють екстремізм [10, с. 27].

На нашу думку, можна виокремити два основних напрями впливу корупції на появу та поширення екстремізму у суспільстві.

По-перше, корупційні прояви руйнують мораль, породжують соціальну нерівність та несправедливість. Бажання відновити і захистити зневажені цінності є рушійною силою для використання окремими особами, як правило молоддю, насильницьких, у тому числі екстремістських, способів і методів боротьби з корупціонерами та



корупційним політичним режимом, особливо у випадках неефективності систем державного управління і правосуддя, занедбаності соціальної інфраструктури, низьких соціальних стандартів, відсутності прозорих та зрозумілих соціальних ліфтів, моделей успішного будівництва своєї кар’єри тощо.

Британські експерти у своїх дослідженнях наголошують, що системна корупція, кумівство і патримоніальне управління є основою багатьох соціально-економічних і політичних чинників екстремізму, зокрема у країнах Північно-Східної Африки. Фахівці зазначають, що у державах цього регіону відбувається підрив розвитку національної економіки через істотне розкрадання або нецільове використання бюджетних коштів. Внаслідок корупції мільйони людей щоденно стикаються з насиллям, дискримінацією та несправедливістю, відбуваються обмеження (де-юре і де-факто) громадянських і політичних прав і свобод, процвітає безкарність та асиметричність влади держави та політичної еліти.

У державах, де обмежено або заборонено громадянську і політичну активність суспільна напруженість буде знаходити своє зовнішнє вираження в інших формах, які спричинятимуть як насильницькі, так і ненасильницькі наслідки. Експерти стверджують, що соціально-політична маргіналізація, безправність, обмежена економічна мобільність, відносна депривація, систематична корупція та обмежені можливості для правового захисту (політичного чи інституційного) не є достатніми факторами для поширення насильницького екстремізму на індивідуальному рівні у країнах Північно-Східної Африки.

Агресивна (екстремістська) поведінка особи обумовлена поєднанням її індивідуальних особливостей, здібностей, психологічних схильностей, взаємовідносин з соціальними, політичними та економічними чинниками. При цьому вирішальною умовою такої поведінки є ступінь наблизеності індивіда до екстремістів та їх угруповань. Люди, які поділяють певну екстремістську ідеологію, можуть відгукнутися на заклики екстремістів щодо насильницького способу досягнення соціальних і політичних цілей. Крім того, вербування нових членів відбувається на основі соціальних, фінансових і матеріальних стимулів, які щедро надаються або обіцяються лідерами екстремістів [11, с. 10].

Екстремістська діяльність, зумовлена обуренням корупцією і безкарністю корупціонерів, може бути спрямована проти: конкретних осіб або груп, які розглядаються як символи існуючої корупції; чиновників чи органів публічної влади, яких звинувачують у власних етичних недоліках та/або у тому що вони не хочуть протидіяти корупції; проти суспільства, яке вважається корумпованим і причетним до збереження несправедливості; держав, цивілізацій (Захід, США, Європа), які розглядаються як такі, що підтримують корумповану систему і є частково відповідальними за усвідомлений моральний занепад системи [10, с. 39].

По-друге, толерантне становлення людей до корупції у поєднанні з різноманітними факторами, які сприяють появі та поширенню корупції у суспільстві, дозволяє екстремістам, їх угрупованням користуватись послугами корупціонерів для приховування своєї протиправної діяльності, зміцнення інституційної спроможності, а також зайняття посад в органах державної влади, органах місцевого самоврядування, чи іншого проникнення у легальні сфери суспільного життя.

У таких випадках екстремістські угруповання набувають ознак, які притаманні організованій злочинності, більше того, вони можуть поєднувати екстремістську діяльність із скоєнням злочинів загально кримінальної спрямованості. Існує інформація, що окремі екстремістські угруповання володіють сучасними засобами зв’язку та

шифрування передачі даних, спеціальними технічними засобами негласного отримання інформації, застосовують у своїй роботі агентурні і контрагентурні методи, знайомі із особливостями оперативно-розшукової та контррозвідувальної діяльності тощо. Наведене, у поєднанні з “корупційним прикриттям”, суттєво ускладнює здійснення ефективних антиекстремістських заходів, а в деяких випадках взагалі зводить все нанівець.

За твердженнями С. Грачова та А. Морозової, корупція в органах державної влади, особливо у правоохоронних структурах, є сприятливим середовищем для розвитку екстремізму. З одного боку, корупція є причиною виникнення екстремізму, а з іншого – невід’ємною умовою його існування. Дослідники звертають увагу на те, що, не подолавши корупцію, неможливо очікувати серйозних успіхів у справі боротьби з екстремізмом та тероризмом [12, с. 20].

Прояви корупції в органах публічної влади, як слушно зазначає М. Каратаєв, є фактичним перенесенням ринкових механізмів у сферу державного управління, що є неприпустимим як по суті, так і відповідно до закону. В умовах, коли повноваження окремих чиновників (військових, депутатів чи суддів) на ухвалення владно-управлінських рішень купуються і продаються, як звичайний товар, навіть ідеально організована система безпеки не гарантуватиме ефективного захисту від загроз екстремістського й терористичного характеру [13, с. 11].

Вже ні для кого не є таємницею, що екстремістські угруповання, особливо міжнародні, мають у своєму розпорядженні достатні фінансові ресурси, акумульовані внаслідок привласнення чужого майна, незаконної торгівлі зброєю, наркотиками, людьми, а також природними ресурсами. Крім того, частина коштів надходить від “податків і зборів” з населення на підконтрольних територіях, законних операцій, а також від “благодійників”. Отримані кошти вони спрямовують на різні цілі, у тому числі на налагодження корупційних зв’язків з “потрібними” людьми.

Ми вважаємо, що лідери екстремістських організацій через різні корупційні схеми мають можливість організувати “співпрацю” з окремими представниками органів державної влади та органів місцевого самоврядування, у тому числі співробітниками і керівниками правоохоронних органів, суддями, працівниками апаратів судів, а також із лідерами та членами політичних партій, громадських організацій, керівниками і працівниками підприємств, установ, організацій різної форми власності тощо.

Результатом налагодження екстремістами корупційних зв’язків з представниками правоохоронних і контролюючих органів є те, що останні “заплющують очі” на порушення національного законодавства у сферах дозвільної, міграційної, митної, податкової, регуляторної, реєстраційної політики тощо. У такий спосіб екстремісти полегшують собі шляхи переходу через державні кордони, придбання зброї, боєприпасів, вибухових речовин, транспортних засобів, об’єктів нерухомості, іншого майна, здійснення підприємницької діяльності, а також отримання послуг, необхідних для здійснення різних екстремістських та/або терористичних актів.

Існують випадки, коли за матеріальну винагороду лобіюються інтереси екстремістів під час законодавчої, нормотворчої та правозастосовної діяльності. Крім того, їм може незаконно надаватися інформація з обмеженим доступом (секретна, службова, конфіденційна), що дає їм можливість більш якісно планувати свою протиправну діяльність, уникати юридичної відповідальності чи ухилятися від переслідувань з боку судових та правоохоронних органів.

Завдяки корупційній складовій екстремістські організації мають можливість знаходити підтримку своїх дій в засобах масової інформації, політичних партіях, як

правило тих, які не представлені у парламенті, та громадських організаціях. Це робиться з метою розширення соціальної бази екстремістів, посилення їх політичного впливу на місцевому та загальнодержавному рівні, формування майбутнього електорату.

Вважаємо за необхідне звернути увагу на те, що необхідність боротьби з корупцією використовується екстремістськими організаціями, особливо релігійними, для пропаганди своїх деструктивних ідеологій.

Так, в багатьох економічно нерозвинутих країнах Африки та Близького Сходу корупція є надзвичайно поширеною, що стало головною причиною фрустрації арабської спільноти. Радикальні екстремісти, у тому числі з “Аль Каїди”, використовують заклики до боротьби з корупцією для того щоб поставити під сумнів існуючу державну владу та захопити її у відповідних країнах [14, с. 306]. Самопроголошена “Ісламська держава” у такий спосіб набирає новобранців та збільшує кількість своїх прихильників в Іраку, Пакистані, Центральній Азії, зоні “Сахелю”, Західній Африці. Представники радикального ісламістського угруповання “Боко Харам” у своїй агітації стверджували, що їхня конституція базуватиметься на ісламській системі цінностей, тому корупція зникне, а суспільство буде правовим і справедливим [15]. Згідно соціологічних опитувань у Нігерії, саме корупція сприяє “Боко Харам” вербуванню послідовників та радикалізації громадян. Про це стверджували 70 % опитаних у штаті Сокото, та 67 % респондентів у штаті Кано. Духовні лідери екстремістів у своїх проповідях наголошують на значній корумпованості влади та її небожественному походженні. Зазначене знаходить підтримку у збіднілої, відчуженої і безробітної північної мусульманської молоді [16, с. 5].

У Дагестані та інших республіках Північного Кавказу Російської Федерації, як зазначають В. Дзидзоев та Н. Левченко, у пострадянський час набули широкого поширення серйозні і небезпечні негативні явища, проти яких рішуче почали боротися ваххабіти. На тлі масового зубожіння значної частини населення цих республік, жадібності багатьох керівників, які розбагатіли в результаті “прихватизації”, корупції в усіх ешелонах влади, наркоманії, пияцтва, проституції, явного порушення соціальної гармонії, масового безробіття та інших негативних явищ, вчення “ваххабізму” знайшло чимало своїх прихильників [17, с. 154].

У середині 1990-х років лідери “Талібану” використовували гасла, що вони незаплямовані корупцією та можуть забезпечити законність, порядок і фізичну безпеку громадян. На тлі багаторічного грабування та експлуатації афганського населення військовими та чиновниками це спрацювало. Талібам вдалося взяти під контроль значну частину території Афганістану. Аналогічно відбулося і в Сомалі, де “Союз ісламських судів” отримав підтримку у населення, яке було виснажене багатьма роками війни, корумпованістю польових командирів і прагнуло безпеки і справедливості [10, с. 40-41].

Взаємозв'язок корупції та екстремізму простежується не тільки у нерозвинутих країнах Африки чи Близького Сходу.

За твердженнями експертів, теракти, які були скоєні у Бельгії у 2016 році, підтвердили, що терористичні мережі глибоко прижилися у цій країні. Це стало можливим через існуючі системні проблеми державного управління, зокрема: 1) корупцію і непотизм у державній службі, які призвели до відсутності довіри до поліції і судової системи; 2) фрагментацію поліції та муніципальної влади; 3) толерантність до дрібної злочинності. Тривала напруженість між різними мовними групами (більше 30 років) та необхідність знаходження компромісу виснажили центральну владу. Брюссель не в змозі на достатньому рівні профінансувати заходи щодо недопущення ісламської радикалізації, наприклад у тюрмах [18].

Експерти Фонду Карнегі встановили взаємозв’язок між корупцією та насильство на підставі аналізу Індексів поширення цих явищ у світі (див. Рис. 1 та 2). Вони дійшли висновку, що держави, де процвітає корупція, страждають від соціальних конфліктів та кризи державного управління. Дослідники звертають увагу на те, що двадцять п’ять країн, які займають останні місця у Індексі сприйняття корупції, становлять серйозну загрозу для міжнародної безпеки. Це зумовлено зокрема тим, що ці держави є ареною заколотів, а на їх території знайшли притулок різні екстремістські угруповання [19].

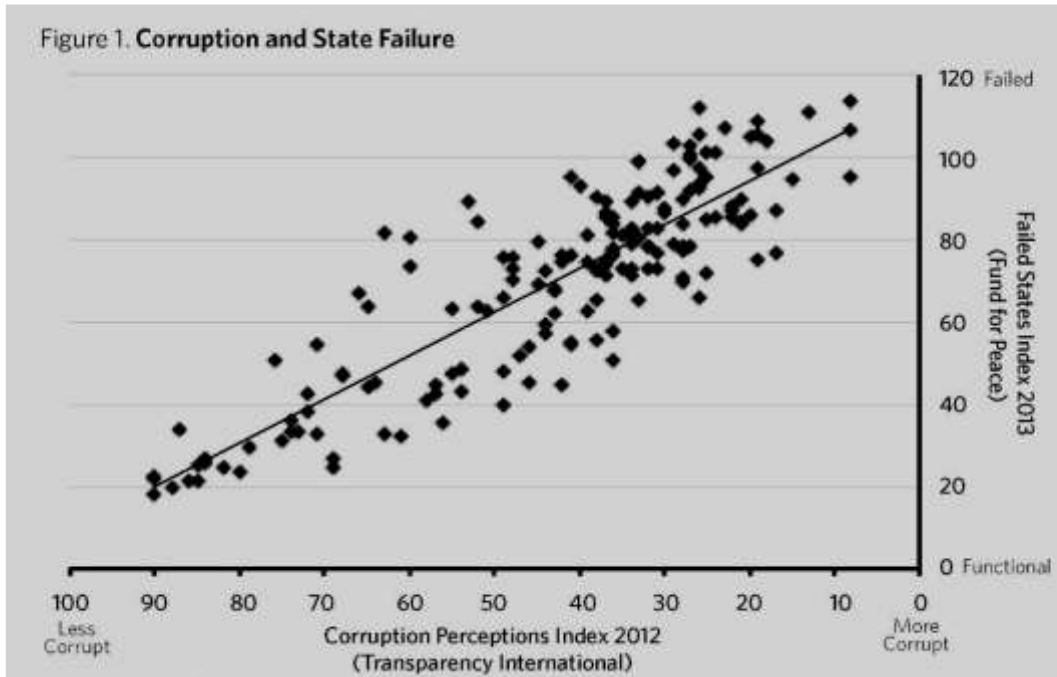


Рис. 1

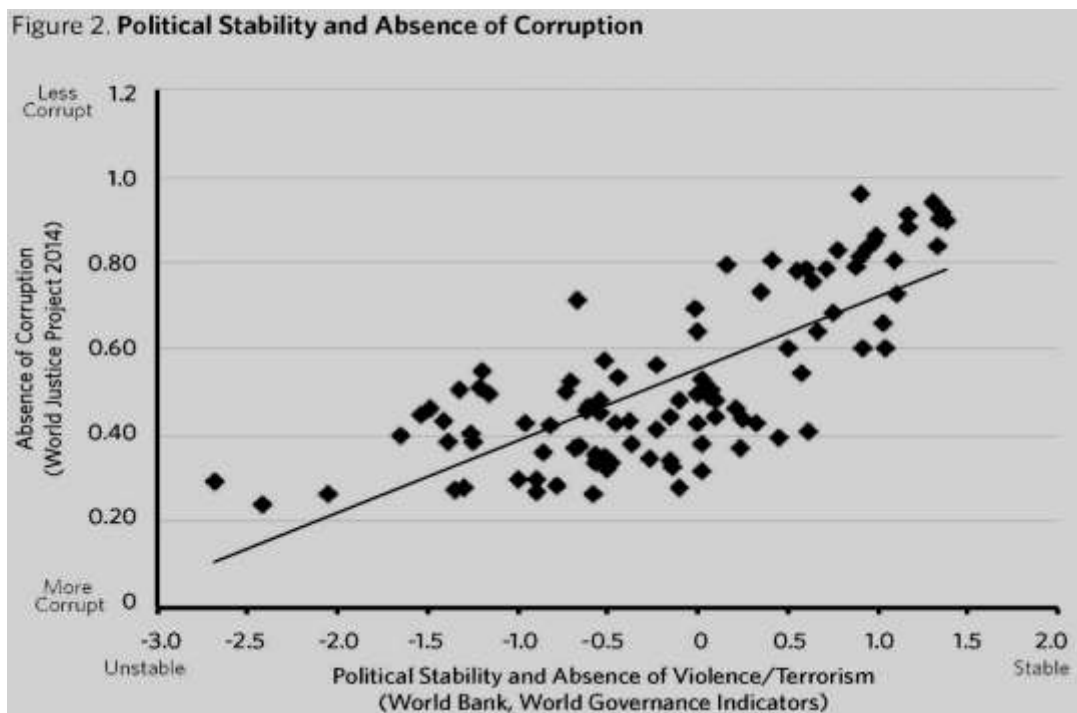


Рис. 2

Проблеми поширення корупції та екстремізму актуальні для всіх без винятку держав. У світі не існує універсальних механізмів протидії цим негативним явищам. У кожній державі корупція та екстремізм, поряд із загальними ознаками, мають національні особливості, які зумовлені історичним розвитком відповідного суспільства. Ми переконані, що протидія корупції та екстремізму має здійснюватися за такими основними напрямками:

1) перегляд та удосконалення законодавства з метою створення належних умов для функціонування механізму держави, відновлення або збільшення довіри громадян до органів публічної влади, їх посадових та службових осіб. Громадяни мають бути впевнені, що держава забезпечить всебічний захист та відновлення їх прав, свобод та законних інтересів, у випадках будь-яких порушень чи протиправних посягань;

2) усунення адміністративних бар'єрів та створення фінансово-економічних умов для реалізації економічно-активним населенням на практиці своїх здібностей, знань, вмінь, навичок у різних сферах суспільного життя;

3) розробка та впровадження загальнодержавних, регіональних та місцевих програм по зменшенню безробіття, а також фізичного, інтелектуально-творчого і духовно-морального розвитку представників різних соціальних груп. Вироблення дієвих механізмів державного та громадського контролю за виконанням цих програм;

4) виділення достатніх кадрових, матеріально-технічних і фінансових ресурсів для суб'єктів протидії корупції та екстремізму з метою розроблення сучасних методик пошуку, виявлення, фіксації та нейтралізації відповідних правопорушень;

5) посилення прикордонного та міжнародного співробітництва з метою обміну досвідом та недопущення утворення транскордонних організованих злочинних угруповань.

На нашу думку, протидію корупції та екстремізму необхідно здійснювати з урахуванням демократичних норм та принципів. При цьому силові та несилові методи і способи боротьби мають застосовуватися до всіх суб'єктів права без винятку. У разі вибіркового переслідування винних осіб, призначення окремим з них надто м'яких покарань, що не відповідають тяжкості скоєних правопорушень, поганій профілактики правопорушень та некваліфікованого правового виховання населення, особливо молоді, досягнути бажаних результатів буде неможливо.

Наприкінці дослідження вважаємо за необхідне звернути увагу на проблему корупції в Україні. Відповідно до “Індексу сприйняття корупції 2016”, підготовленого Міжнародною неурядовою організацією Transparency International, Україна, поряд з Казахстаном, Іраном, Непалом та Росією, посідає 131 місце з 176 за рівнем корупції [20].

Вивчення проблем корупції дало змогу В. Гаращуку здійснити узагальнену класифікацію негативних наслідків цього явища для України, а саме 1) неефективне використання державних коштів та ресурсів; 2) неефективна зовнішня і внутрішня економічна політика; 3) втрата податків, інших надходжень до державного бюджету (шляхом їх прямого розкрадання або “узгодженого” недоотримання); 4) гальмування шляхом установа надуманих перешкод розвитку бізнесу; 5) уповільнення ефективності роботи державного апарату в цілому; 6) неефективне використання знань та умінь людини, які замість того, щоб займатися справою, вимушені долати штучні бюрократичні перешкоди; 7) зниження якості управлінських послуг (у тому числі навмисне, задля провокування сплати за безоплатну послугу); 8) зниження інвестицій, уповільнення економічного зростання; 9) розорення приватних підприємців; 10) посилення організованої злочинності, яка часто “кришується” корумпованими високопосадовцями; 11) зростання соціальної нерівності; 12) зuboжіння населення;

13) зменшення народжуваності через матеріальні й інші складнощі у вихованні дітей;  
14) деформація суспільної моралі [21, с. 35-36].

Очевидно, що суттєві проблеми, які існують у суспільстві та у державному управлінні внаслідок корупції, створюють сприятливі умови для зародження чи інспірування серед українського населення екстремістських ідеологій та активізації екстремістської діяльності. Ми вважаємо, що протидія корупції та екстремізму в Україні має відбуватися комплексно із поєднанням можливостей держави та громадянського суспільства. При цьому суб'єктам боротьби з цими явищами необхідно враховувати факт збройної агресії проти України, анексію Автономної Республіки Крим та міста Севастополь, і тимчасову окупацію окремих районів Донецької та Луганської областей. Заходи щодо протидії корупції та екстремізму мають відбуватися у межах єдиного стратегічного задуму щодо відновлення суверенітету та територіальної цілісності України.

### **Висновки.**

Загальновідомо, що неможливо побудувати суспільство в якому люди не вчинятимуть правопорушень. Прояви корупції та екстремізму будуть завжди мати місце у житті людства. У зв'язку з цим дуже важливо, щоб їх масштаби були незначними і не підтримувались домінуючою частиною населення. В еліти, середнього класу та незаможних верств населення мають виробитися внутрішні установки на засудження і відторгнення корупційної та екстремістської діяльності. Люди мають бути впевнені, що їхня безпека та благополуччя можуть бути досягнуті у законний спосіб без зловживання владою та службовим становищем, неправомірним застосування насилля до інших. Саме на досягнення такого результату необхідно спрямовувати зусилля під час протидії корупції та екстремізму.

### **Використана література**

1. Кодекс поведінки посадових осіб органів правопорядку : Резолюція Генеральної Асамблеї Організації Об'єднаних Націй від 17.12.79 р. № 34/169. – Режим доступу : [http://zakon4.rada.gov.ua/laws/show/995\\_282](http://zakon4.rada.gov.ua/laws/show/995_282)
2. Про запобігання корупції : Закон України від 14.10.14 р. № 1700-VII. – Режим доступу : <http://zakon5.rada.gov.ua/laws/show/1700-18/print1456324320008262>
3. Добродумов П.О. Корупція як явище соціально-політичного життя історії / П.О. Добродумов / Аспекти регіональної модернізації : медіа, громадські ініціативи, приватний сектор. – Суми : ВАТ “Сумська обласна друкарня”, видавництво “Козацький вал”, 2005. – С. 51-58.
4. Мельник М.І. Кримінологічні та кримінально-правові проблеми протидії корупції : автореф. дис. на здобуття наук. ступеня д-ра юрид. наук : 12.00.08 / М.І. Мельник. – К., 2002. – 31 с.
5. Мартиновський В.В. Причини та умови виникнення корупції в державному механізмі / В.В. Мартиновський / Корупція в Україні : питання протидії ; за заг. ред. В.М. Гаращука. – Х.: ФОП Панов А.М., 2015. – С. 41-54.
6. Проти корупції : Конвенція Організації Об'єднаних Націй від 31.10.03 р. – Режим доступу : [http://zakon5.rada.gov.ua/laws/show/995\\_c16/print1445948204946821](http://zakon5.rada.gov.ua/laws/show/995_c16/print1445948204946821)
7. Про боротьбу з корупцією : Цивільна Конвенція Ради Європи від 04.11.99 р. – Режим доступу : [http://zakon5.rada.gov.ua/laws/show/994\\_102/print1445948204946821](http://zakon5.rada.gov.ua/laws/show/994_102/print1445948204946821)
8. Anti-Corruption Summit London 2016 : Communiqué 12 May. – Режим доступу : [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/522791/FINAL\\_-\\_AC\\_Summit\\_Communique\\_-\\_May\\_2016.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/522791/FINAL_-_AC_Summit_Communique_-_May_2016.pdf)

9. Пан Ги Мун представил Генеральной Ассамблее ООН “План действий по предупреждению воинствующего экстремизма”. – Режим доступа : <http://www.un.org/russian/news/story.asp?NewsID=25249#.WDSH1TtHx>

10. Guide to the drivers of violent extremism. – Режим доступа : [http://pdf.usaid.gov/pdf\\_docs/pnadt978.pdf](http://pdf.usaid.gov/pdf_docs/pnadt978.pdf)

11. Eelco Kessels, Tracey Durner, Matthew Schwartz. Violent Extremism and Instability in the Greater Horn of Africa. An Examination of Drivers and Responses, April 2016. – Режим доступа : [http://www.globalcenter.org/wp-content/uploads/2016/05/GCCS\\_VIOLENT-XTREMISM\\_low\\_3.pdf](http://www.globalcenter.org/wp-content/uploads/2016/05/GCCS_VIOLENT-XTREMISM_low_3.pdf)

12. Грачев С.И., Морозова А.С. Детерминирующие факторы в превенции коррупции, терроризма и экстремизма среди студенческой молодежи на протяжении новейшей истории // Вестник ННГУ им. Н.И. Лобачевского. – 2015. – № 2. – С. 18-22.

13. Каратаев М.В. Коррупция как причина, условие и сопутствующий фактор российского терроризма / Дайджест-финансы. – 2012. – № 7. – С. 9-18.

14. J. Scott Carpenter, Matthew Levitt, and Michael Jacobson. Confronting the Ideology of Radical Extremism. – Режим доступа : <http://www.washingtoninstitute.org/uploads/Documents/ope ds/4aca6941f0ec7.pdf>

15. Sarah Chayes. Corruption : Violent Extremism, Kleptocracy, and the Dangers of Failing Governance. – Режим доступа : <http://carnegieendowment.org/2016/06/30/corruption-violent-extremism-kleptocracy-and-dangers-of-failing-governance-pub-63982>

16. Freedom C. Onuoha. Why Do Youth Join Boko Haram?. – Режим доступа : [http://www.usip.org/sites/default/files/SR348-Why\\_do\\_Youth\\_Join\\_Boko\\_Haram.pdf](http://www.usip.org/sites/default/files/SR348-Why_do_Youth_Join_Boko_Haram.pdf)

17. Дзидзоев В.Д. Сепаратизм, терроризм и экстремизм на Северном Кавказе : политико-правовой анализ / В.Д. Дзидзоев, Н.Н. Левченко. – Владикавказ : Ир, 2008. – 288 с.

18. Tim King. Brussels attacks: Belgium, corrupt and fragmented, is a breeding ground for extremism. – Режим доступа : <http://www.telegraph.co.uk/news/worldnews/europe/ belgium/12201246/Brussels-attacks-Belgium-corrupt-and-fragmented-is-a-breeding-ground-for-extremism.html>

19. CORRUPTION The Unrecognized Threat to International Security / Carnegie Endowment for International Peace, 2014. – Режим доступа : [http://carnegieendowment.org/files/corruption\\_and\\_security.pdf](http://carnegieendowment.org/files/corruption_and_security.pdf)

20. CORRUPTION PERCEPTIONS INDEX 2016 / Transparency International. – Режим доступа : [https://www.transparency.org/news/feature/corruption\\_perceptions\\_index\\_2016](https://www.transparency.org/news/feature/corruption_perceptions_index_2016)

21. Гаращук В.М. Становлення корупційних відносин в Україні / В.М. Гаращук / Корупція в Україні : питання протидії ; за заг. ред. В.М. Гаращука. – Х. : ФОП Панов А.М., 2015. – С. 8-40.

~~~~~ \* \* \* ~~~~~

УДК 338.46:002+343.627

РАДЗІЄВСЬКА О.Г., старший науковий співробітник
НДІ інформатики і права НАПрН України

ПРАВОВІ ЗАСАДИ ТА ПРІОРИТЕТИ РОЗВИТКУ ПРОТИДІЇ НЕГАТИВНИМ ІНФОРМАЦІЙНИМ ВПЛИВАМ НА ДІТЕЙ

***Анотація.** Стаття присвячена аналізу сучасного стану і наукових поглядів на проблему правового регулювання протидії негативним інформаційним впливам на дітей та дослідженню пріоритетних напрямів розвитку системи правового регулювання щодо забезпечення їх інформаційної безпеки в Україні.*

***Ключові слова:** інформаційна безпека дитини, загрози інформаційній безпеці, уразливість дитини в інформаційній сфері, негативні інформаційні впливи.*

***Аннотация.** Статья посвящена анализу современного состояния и научных взглядов на проблему правового регулирования противодействия негативным информационным воздействиям на детей и исследованию приоритетных направлений развития системы правового регулирования по обеспечению их информационной безопасности в Украине.*

***Ключевые слова:** информационная безопасность ребенка, угрозы информационной безопасности, уязвимость ребенка в информационной сфере, негативные информационные воздействия.*

***Summary.** The article is devoted to the analysis of the current state and scientific views on the problem of legal regulation of counteraction to negative informational influences on children and research of priority directions of development of the legal regulation system in order to ensure their information security in Ukraine.*

***Keywords:** information security of the child, threats to information security, child's vulnerability in the information sphere, negative informational influences.*

Постановка проблеми. Трансформаційні процеси, що відбуваються у сучасному суспільстві, мають значний вплив на формування дитини. Розвиток інформаційно-комунікаційних технологій сприяє її активному інтелектуальному і духовному розвитку. Проте надто швидке їх впровадження та неконтрольований обіг інформації може становити загрозу психологічному та психофізичному здоров'ю і життю дитини. Система правового та організаційного убезпечення дитини в інформаційному просторі наразі лише формується і нездатна комплексно протидіяти інформаційним викликам та ефективно захищати дитину від небезпек в інформаційній сфері. Динамічність розвитку інформаційних викликів та загроз в сучасному світі, суб'єктивізм та відсутність єдиного бачення в оцінці небезпек а також міждисциплінарність окресленої проблеми вимагають комплексного наукового дослідження негативного впливу інформаційного середовища на свідомість дитини. Актуальним постає питання теоретичного переосмислення вказаної проблеми та пошуку найбільш ефективних шляхів протидії негативним інформаційним впливам та забезпечення інформаційної безпеки дитини.

Результати аналізу наукових публікацій. Проблемами регулювання суспільних відносин в інформаційній сфері та убезпечення особи в інформаційному просторі займалися ряд українських та зарубіжних науковців, зокрема І. Арістова, О. Баранов, І. Бачило, К. Беляков, В. Брижко, В. Богущ, І. Боднар, О. Довгань, А. Качинський, А. Ковальчук, І. Корж, Б. Кормич, А. Кузьменко, А. Литвинюк, І. Манжул., А. Марущак,

М. Медвідь, О. Нестеренко, О. Олійник, В. Остроухов, В. Пилипчук, В. Петрик, А. Погребняк, Н. Савінова, Є. Скулиш, О. Соснін, О. Тихомиров, В. Фурашев, О. Юдін та інші. Окремих аспектів інформаційної безпеки дитини торкались такі вчені як О. Золотар, Г. Красноступ, О. Петрунько, О. Яременко. Проте наразі не існує комплексного дослідження проблеми протидії негативним інформаційним впливам на дітей та їх убезпечення в інформаційному просторі, з урахуванням особливостей сприйняття інформації дитиною та специфіки і механізмів дії інформаційних впливів на її свідомість. Тому науковий пошук у цьому напрямку є надзвичайно важливим та актуальним, оскільки стосується безпеки дитини та майбутнього держави.

Метою статті є аналіз законодавства з питань протидії негативним інформаційним впливам на дітей та визначення пріоритетних напрямів розвитку системи правового регулювання щодо забезпечення інформаційної безпеки дитини в Україні.

Виклад основного матеріалу. Відповідно до статті 3 Конституції України “...життя і здоров’я, честь і гідність, недоторканність і безпека людини в Україні визнаються найвищою соціальною цінністю”. Обов’язком держави є утвердження та забезпечення прав і свобод людини. Забезпечення “...інформаційної безпеки є однією з найважливіших функцій держави та справою усього Українського народу” як зазначено в ст. 17 Конституції України [1]. Згідно з положеннями Закону України “Про основи національної безпеки України” інформаційна безпека громадянина відноситься до сфери національної безпеки і є пріоритетним напрямом державної політики [2]. Іншими словами, держава гарантує кожній людині безпеку і захист при одночасному дотриманні всіх прав і свобод, у тому числі й в інформаційній сфері. Тобто держава гарантує, що система протидії загрозам в інформаційному просторі, зокрема й протидія негативним інформаційним впливам на будь-якого громадянина, у тому числі на дитину, працюватиме ефективно для реалізації однієї з найважливіших своїх функцій по забезпеченню інформаційної безпеки.

Дитина є особливим суб’єктом суспільних відносин, що відповідно до національного законодавства та міжнародного права потребує особливого захисту та піклування з боку держави та основних її інститутів. На інститути держави покладено функції забезпечення найкращих інтересів дитини, направлених на задоволення її індивідуальних потреб відповідно до віку, статі, стану здоров’я, особливостей розвитку, життєвого досвіду, родинної, культурної та етнічної належності, а також вжиття заходів, спрямованих на забезпечення повноцінного життя, всебічного виховання, розвитку та захисту її прав (ст. 1 Закону України “Про охорону дитинства”) [3].

Убезпечення дитини в інформаційному просторі при одночасному дотриманні її прав і свобод, гарантованих національним та міжнародним правом, потребує ефективного функціонування у державі системи правових й організаційних заходів. Необхідним також є врегулювання механізмів взаємодії державного та приватного секторів, які мусять діяти в окресленому правовому полі в рамках законодавчо визначеної інформаційної політики та пріоритетних напрямків розвитку нашої держави. Для створення ефективної системи протидії негативним інформаційним впливам на дітей та забезпечення їх інформаційної безпеки потрібно чітко усвідомлювати загрози, механізми їх дії на свідомість дитини та наслідки, до яких може призвести їх дія (ступінь шкоди для суб’єкта інформаційних відносин).

Діти практично не усвідомлюють ступінь загроз, які існують в сучасному інформаційному середовищі, зокрема у медійному телерадіопросторі та у соціальних мережах. Переважно, вони схильні довіряти інформації, отриманій через будь-які засоби її поширення. За даними соціологічних досліджень, до основних джерел отримання

інформації 38 % українських дітей у віці 7 – 14 років відносять телебачення, 18 % – комп’ютер (DVD, ігри тощо) і 44 % – Інтернет. На питання про те, яким джерелам для отримання знань вони надають перевагу: телебаченню, Інтернету або інформації, що подається на уроках, учні відповіли таким чином: телебачення – 38 %, Інтернет – 49 %, інформація, отримана на уроках, – 13 % [4]. Це означає, що вплив медійного продукту на дитину є надзвичайно великим. Українські науковці встановили, що “маленький” українець має змогу споглядати жорстокі сцени на телеекрані кожні 6 хвилин [5]. Доведено, що у пересічній телепередачі міститься до 6 жорстоких сцен насилля, а у прайм-тайм обсяг насильства зростає на всіх каналах кабельного та ефірного телебачення. До 60 % телепередач містять насильство, переважна більшість з яких представлена як буденна і значно “прикрашена” [6] і лише 26 % ефірного часу припадає на поточну і пізнавальну інформацію [7, с. 5]. За результатами дослідження “Телевізор і дитина”, проведеного британськими та бельгійськими вченими у 35 країнах світу, українські діти дивляться телевізор найбільше – 3,7 год. на добу [6]. А за результатами досліджень, проведених у різний час та в різних країнах, психологи стверджують про існування причинно-наслідкових зв’язків між переглядом сцен насилля і подальшою агресивною поведінкою та поглядами дитини [8, с. 193-214, 237-254.].

Медіанасилля, як вид негативного інформаційного впливу – це несиловий вплив (дія) на ментальну сферу, що може корегувати закономірність перебігу подій [9]. Він може бути як прямим, так і непрямим (опосередкованим); коротко- та довготривалим. Психологічний вплив медіанасилля, як і будь-який негативний інформаційний вплив, може проявлятися на трьох рівнях: на рівні *поведінки* (копіювання насилля) – коли перегляд сцен насилля впливає на поведінку телеглядача; на *емоційному рівні* (страх, агресія, збудженість, чи навпаки загальмованість) – коли перегляд сцен насилля викликає швидко, чи довготривалу емоційну реакцію та *когнітивному рівні* (реальний світ здається більш жорстоким, ніж є насправді) – коли перегляд сцен насилля впливає на сприйняття реального світу. Сприйняття ж продукту ЗМІ та реакція аудиторії на нього залежить від індивідуальних особливостей, психологічних факторів, факторів зовнішнього середовища та характеристик соціальних груп [8, с. 78]. Вирізняють *фізіологічну* (негативний вплив від поєднання кольорів, підбору музики, ефекту 25-го кадру) та *психологічну* (страх, розлади, негативна інформація) форми медіанасилля [10].

За даними дослідження найефективніше впливає на свідомість дитини телебачення. Поєднання картинки і звукового супроводу дає видовищність та повноту образу ілюзорного світу, чим прив’язує дитину до екрану, веде до формування потреби включатись у віртуальну реальність телебачення, яке повсякденно впливає на образи, смаки, коригує моду, формує мову, стиль і лексику [11]. Кліпова зміна кадрів викликає залежність, а образи насилля діють на дитячу психіку як сильний наркотик, від якого тяжко позбавитись. Швидка зміни кадрів призводить до дефіциту уваги у школі та синдрому гіперактивності.

Тому правомірним є припущення, що шкідливий аудіовізуальний контент може мати суттєвий негативний вплив на психофізичний стан дитини, стати причиною відхилень у її індивідуальному і суспільному становленні та розвитку, деформувати світогляд та підмінити систему цінностей дитини [12, с. 53-55].

Вплив – це дія, яку певна особа чи предмет або явище виявляє стосовно іншої особи чи предмета [13, с. 751], а інформаційний – той, що стосується інформації чи містить інформацію [14, с. 42]. Тому можемо сказати, що інформаційний вплив – це дія

інформації або за допомогою інформації, яку певна особа чи предмет або явище виявляє стосовно іншої особи чи предмета.

Якщо розглянути негативну дію інформаційного впливу з позиції інформаційної безпеки особи, представленої у Законі України “Про основні засади розвитку інформаційного суспільства на 2007 – 2015 роки” [15], то під негативним інформаційним впливом слід розуміти такий вплив, що може становити загрозу важливим інтересам людини, суспільства, держави.

Сучасна військова наука визначає інформаційну безпеку особи як стан захищеності “психіки та свідомості людини від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукання до девіантної поведінки” [16, с. 11].

Фахівці з інформаційно-психологічного протиборства визначають інформаційний вплив як “організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення деструктивних змін у свідомість особистості, соціальних груп чи населення (корекція поведінки), в інформаційно-технічну інфраструктуру об’єкта впливу та (чи) фізичний стан людини” [17, с. 10].

Підсумовуючи викладене та опираючись на раніше проведене власне дослідження [18], під негативним інформаційним впливом, на наш погляд, слід розуміти таку дію інформації або за допомогою інформації, з використанням спеціальних засобів і технологій, яку певна особа чи предмет або явище виявляє стосовно іншої особи чи предмета, що загрожує інформаційній безпеці особи, суспільства, держави, становить небезпеку для індивідуальної або суспільної свідомості, завдає шкоди фізичному чи психічному здоров’ю людини, або спонукає її до девіантної поведінки.

С. Янковський вважає, що в широкому розумінні у контексті теорії інформації інформаційний вплив визначається як будь-яка взаємодія між суб’єктами, у процесі якого один набуває певну субстанцію (інформацію), а інший її втрачає [19].

Тобто інформаційний вплив може становити загрозу для психофізичного здоров’я дитини, як суб’єкта інформаційних відносин, під час взаємодії з іншим суб’єктом інформаційних відносин. Суб’єктами інформаційних відносин відповідно до ст. 4 Закону України “Про інформацію” є фізичні та юридичні особи, об’єднання громадян і суб’єкти владних повноважень [20]. Взаємодія між суб’єктами інформаційних відносин може відбуватися як у симплексному, так і в дуплексному режимах. Тобто дитина, як суб’єкт інформаційних відносин, може отримувати і споживати інформацію, не маючи зворотного зв’язку (симплексний режим взаємодії в інформаційній сфері) та за можливості зворотно реагувати і впливати на джерело інформації (дуплексний режим взаємодії в інформаційній сфері). Прикладом першого режиму взаємодії є телебачення та нові медійні платформи, коли дитина є пасивним отримувачем інформації. Дуплексна взаємодія в інформаційній сфері яскраво представлена в соціальних мережах. Тут дитина не лише отримує інформацію, але й має можливість реагувати на неї, створюючи та розповсюджуючи власний контент, тим самим чинячи вплив на іншого суб’єкта інформаційних відносин. Для цих двох способів взаємодії між суб’єктами інформаційних відносин характерним є відповідний розподіл соціальних функцій. Для телебачення (симплексного режиму взаємодії) притаманні інформаційно-пізнавальна та розважальна соціальна функція, а для соціальних мереж (дуплексного режиму взаємодії) основною соціальною функцією є комунікаційно-інформаційна. Розглядаючи інформаційні відносини з позиції форми взаємодії між суб’єктами можемо стверджувати, що кожному із них будуть притаманні певні виклики та загрози, а методи протидії їм носитимуть окремий характер і потребуватимуть системи різних організаційно-правових заходів.

При симплексному споживанні інформації дитина не має можливості впливати на її джерело. Наприклад, у дитини, як і у будь-якого громадянина, що не має владних повноважень, нема й можливості змінювати інформаційне наповнення (контент) телерадіопростору України. Вона є пасивним суб'єктом інформаційних відносин і може визначатися лише у тому, споживати надану інформацію чи ні. Інша справа при дуплексному режимі інформаційної взаємодії в соціальних мережах. Тут у дитини як у суб'єкта інформаційних відносин з'являється можливість реагувати на інформацію, створювати власний контент, розповсюджувати конфіденційну інформацію про себе чи інших, намагатися чинити власний інформаційний вплив, чи не робити нічого із перерахованого, або робити це частково, чи в рамках правових та морально-етичних норм. Тому система протидії негативному впливу на дитину при різних способах інформаційної взаємодії буде різнитися.

Очевидно, що система протидії негативним інформаційним впливам на дитину з метою забезпечення її інформаційної безпеки повинна враховувати як систематизацію та класифікацію інформаційних загроз, так і відмінності у інформаційних взаємовідносинах між суб'єктами.

Наприклад, при симплексному режимі інформаційної взаємодії держава повинна взяти на себе відповідальність за забезпечення інформаційної безпеки дитини. Повинна працювати чітка система регулювання та контролю з боку держави за дотриманням законодавчо закріплених правових норм щодо створення та обігу медійного контенту та запобігання поширення матеріалів, що можуть зашкодити психофізичному здоров'ю дитини, у телерадіопросторі країни. Відповідальність за недотримання вимог чинного законодавства покладається на виробника та поширювача медійного продукту. Проте, функції держави та її інституцій також полягають у контролі за дотриманням правових норм суб'єктами інформаційних відносин.

Нині нормативно-правове регулювання у сфері убезпечення дітей від негативних впливів в інформаційному середовищі телерадіопростору України представлене переважно у контексті загальних прав і свобод дитини [1; 21; 22] та у Законі України “Про основи національної безпеки України” [2]. Ці акти, декларативно торкаються зазначеної проблеми. Утім, згідно зі статтею 52 Конституції України – “Діти рівні у своїх правах... Будь-яке насильство над дитиною та її експлуатація переслідуються за законом” [1]. Це положення деталізовано у п. 4 ст. 20 Закону України “Про охорону дитинства”: “Пропагування у ЗМІ культу насильства і жорстокості, розповсюдження порнографії та інформації, що зневажає людську гідність і завдає шкоди моральному благополуччю дитини” заборонено [22]. Також серед положень вітчизняних законодавчих актів, що спрямовані на убезпечення дітей від негативних інформаційних впливів є: ст. 5, 7 Закону України “Про захист суспільної моралі” [23], ст. 62 Закону України “Про телебачення і радіомовлення” [24], ст. 3 Закону України “Про друковані засоби масової інформації (пресу) в Україні” [25], ст. 20, п. 3 ст. 22 Закону України “Про рекламу” [26]. Але і вони носять переважно декларативний характер.

При дуплексному режимі інформаційної взаємодії багато суб'єктів суспільних відносин одночасно вступають в інформаційні відносини і мають можливість здійснювати цілий спектр дій з інформацією (створювати, передавати, приймати, трансформувати і т.д.). Тому в цьому випадку потрібна комплексна модель забезпечення інформаційної безпеки дитини.

У Законі України “Про основні засади розвитку інформаційного суспільства на 2007 – 2015 роки” інформаційна безпека характеризується станом захищеності “важливих інтересів людини, суспільства, держави, при якому запобігається завдання

шкоди через негативний інформаційний вплив” [15]. Виходячи із змістовної частини визначення інформаційної безпеки, що на правовому рівні надається у Законі України “Про основи національної безпеки України” [2], можемо зробити висновок, що для її забезпечення державі необхідно застосувати комплексну систему захисту у трьох основних напрямках:

- захист інформації, інформаційних ресурсів та забезпечення надійного функціонування інформаційно-комунікаційних систем, у тому числі систем критичної інфраструктури суспільства;

- забезпечення ефективної системи виявлення та протидії новітнім викликам і загрозам в інформаційному суспільстві, у тому числі й системі протидії негативним інформаційним та інформаційно-психологічним впливам на індивідуальну і колективну свідомість у суспільстві, недопущення впливу на неї через маніпулювання з інформацією;

- виховання в особи навичок та умінь убезпечувати власний інформаційний простір з метою підвищення її інформаційної безпеки та рівня інформаційної грамотності.

Такої ж думки притримується й О. Пучков, вивчаючи філософські аспекти інформаційних небезпек, притаманних сучасному суспільству [27, с. 240].

Очевидно, що усі перераховані вище пункти так чи інакше є важливими у системі протидії негативним інформаційним впливам свідомість дитини.

Вільний та безпечний доступ до інформаційних ресурсів, відсутність інформації, що може зашкодити інтелектуальному та духовному розвитку дитини, а також завдати шкоди її психологічному та психофізичному здоров'ю поряд з вмінням самої дитини ефективно шукати, аналізувати, трансформувати та використовувати інформацію разом з її теоретичними знаннями та практичними навичками убезпечувати власний інформаційний простір є основоположними умовами забезпечення її інформаційної безпеки у новому суспільстві.

За даними соціологічних опитувань, проведених ЮНЕСКО, в Україні переважна більшість дітей (96 %) не обізнані про небезпеки, які існують в соціальних мережах: 44 % дітей знаходиться в потенційній небезпеці, оскільки регулярно розміщує персональні дані, кожен п'ятий неповнолітній, а у віковій групі 15 – 17 років – до 60 %, вже опинявся в небезпечних ситуаціях, маючи безпосередній контакт зі зловмисниками і лише 25 % зізналися згодом батькам про такі зустрічі [28]. Понад 28 % опитаних дітей готові надіслати свої фотокартки незнайомцям у мережі. 17 % повідомляли інформацію про себе і свою родину незнайомцям, що свідчить про незнання елементарних правил безпечної поведінки [29, с. 10-11].

Поширення дітьми персональних даних у соціальних мережах створює передумови не лише для інформаційних загроз, але й фізичних. Захист персональних даних регламентований ст. ст. 31, 32 Конституції України [1], Законом України “Про захист персональних даних” [30], а відповідальність за порушення порядку використання персональних даних встановлена ст. 182 КК України [31]. Проте, “викладаючи” інформацію про себе, особа робить її “загальнодоступною”, тому її убезпечення від поширення є практично неможливим. Конфіденційність інформації, розміщеної у соціальних мережах, не може гарантувати її убезпечення від використання іншими особами: на веб-ресурсі лишаються “цифрові сліди”, “цифрові тіні” [32, с. 146, 147], створюється загроза використання цих відомостей у протиправних діях у майбутньому. Неконтрольоване поширення персональних даних може стати причиною залякування, погроз, шахрайства, шантажу, крадіжок особистого майна, а також маніпулювання та впливу на прийняття рішень як самої дитини, так і її рідних. Особливої небезпеки для

дитини набувають ті персональні дані, які були викладені в соціальних мережах, що контролюються та куруються спеціальними службами іншої держави, зокрема тієї, що перебуває в стані протистояння з нашою. Ці дані можуть стати інструментами інформаційного або збройного протистояння, інформаційно-психологічного протиборства і спеціальних інформаційних операцій.

Нова Стратегія Ради Європи з прав дитини (2016 – 2021 рр.) серед п'яти пріоритетних напрямків діяльності для гарантування прав дитини відповідно до викликів сьогодення визначила забезпечення прав дитини в цифровому середовищі [33]. Відповідно, з метою імплементації європейських стандартів та підходів у забезпеченні прав дитини в Україні, основні напрямки реалізації яких окреслено Стратегією Ради Європи з прав дитини, 5 квітня 2017 року розпорядженням Кабінету Міністрів України № 230-р було затверджено Концепцію Державної соціальної програми “Національний план дій щодо реалізації Конвенції ООН про права дитини” на період до 2021 року [34]. В рамках даного документу серед інших основоположних принципів забезпечення прав дитини передбачено й всебічний доступ дитини до інформації і знань, необхідних для її розвитку з використання досягнень сучасних інформаційно-комунікаційних технологій, відсутність дискримінації в інформаційній сфері, захист від усіх видів насильства, у тому числі і психологічного, а також створення безпечного інформаційного простору для дітей, а саме:

- забезпечення захисту персональних даних дитини та іншої конфіденційної інформації про неї, забезпечення безпеки дітей в інформаційному просторі;
- формування політики запобігання проявам радикалізму, расизму, ксенофобії та іншим формам екстремізму у дітей в умовах стрімкого розвитку інформаційних технологій;
- внесення до освітніх програм для дітей віком від 7 до 14 років та програм підвищення кваліфікації вчителів питань безпеки дітей в інформаційному просторі;
- впровадження системи соціально-педагогічної роботи з батьками з питань безпеки дітей в інформаційному просторі.

В рамках розроблення Державної соціальної програми “Національний план дій щодо реалізації Конвенції ООН про права дитини” на період до 2021 року, що покладено на Міністерство соціальної політики разом з іншими заінтересованими центральними органами виконавчої влади, на наш погляд було б доречно розробити Концепцію інформаційної безпеки дитини, яка була б відповіддю на інформаційні виклики і загрози для дитини в інформаційному просторі та основою плану дій щодо реалізації її захисту в інформаційному суспільстві та забезпечення дотримання основних її прав і свобод, гарантованих національним та міжнародним правом, зокрема, ст.ст. 34, 52, 53 Конституції України [1], принципом 7 Декларації прав дитини [35], ст. 2, пп. d п. 1, п. 3 ст. 28 та ст. 17 Конвенції про права дитини [21].

Висновки.

Підсумовуючи викладене, слід зауважити, що задекларовані та законодавчо закріплені основні права і свободи дитини в інформаційному просторі, у тому числі і гарантії інформаційної безпеки, потребують розроблення нових механізмів та способів для їх реалізації. Протидія негативним інформаційним впливам на свідомість дитини стає дедалі актуальнішою проблемою у системі забезпечення її інформаційної безпеки. Розробка механізмів протидії негативному впливу інформації на дитину повинна враховувати новітні глобальні інформаційні загрози та орієнтуватись на прогресивні світові методи їх запобігання.

При розробленні плану дій щодо реалізації Конвенції ООН про права дитини на період до 2021 року пропонується розглянути наступні пропозиції:

1. Для забезпечення прав дитини в інформаційній сфері та формування ефективної системи протидії негативним інформаційним впливам на її свідомість в умовах поширення інформаційної агресії і насилля в ході розвитку національного законодавства передбачити:

– впровадження і правове закріплення шкільних освітніх програм з медіаграмотності та інформаційної безпеки, покликаних навчати дітей убезпеченню власного інформаційного простору;

– підвищення ефективності моніторингу медіаконтенту і механізмів протидії загрозам інформаційній безпеці дитини в медіапросторі та в мережі Інтернет, формування системи превентивних заходів убезпечення дитини від небезпек в інформаційному просторі, що ґрунтується на моделюванні потенційних інформаційних загроз;

– заохочення суб’єктів надання інформаційних послуг до саморегуляції та самоочищення власного медіапростору від матеріалів, що становлять загрозу моральному і психологічному здоров’ю дитини, а також стимулювання до створення в Україні інформаційного продукту, який би базувався на загальнолюдських і національних духовних, культурних та історичних цінностях;

– посилення відповідальності суб’єктів надання інформаційних послуг за розміщення матеріалів, що містять небезпечний контент (насилля, жорстокість, порнографія тощо) або інформацію маніпулятивного характеру, яка може завдати шкоди моральному чи психічному здоров’ю дитини;

– запровадження заборони на продаж в Україні аудіовізуальних відтворюючих пристроїв без вмонтованої системи “батьківського контролю”, та розроблення правових механізмів контролю;

– розроблення правових механізмів для врегулювання суспільних відносин, що виникають у соціальних мережах та Інтернет-спільнотах у контексті безпеки дитини і захисту її персональних даних, а також впорядкування суспільних відносин щодо залучення дітей до Інтернет-комерції;

– запровадження юридичної відповідальності за доведення особи до самогубства або до замаху на самогубство через маніпулювання її свідомістю з використання сучасних інформаційно-комунікаційних технологій. Частину першу статті 120 Кримінального кодексу України [31] пропонується викласти у такій редакції:

Доведення особи до самогубства або до замаху на самогубство, що є наслідком жорстокого з нею поводження, шантажу, маніпулювання з її свідомістю через використання інформаційно-комунікаційних технологій, примусу до протиправних дій або систематичного приниження її людської гідності, – карається обмеженням волі на строк до трьох років або позбавленням волі на той самий строк;

– підвищення юридичної відповідальності за незаконне збирання, зберігання і поширення конфіденційної інформації про дитину. Для цього, у статті 182 Кримінального кодексу України [31] пропонується визнати неповнолітнього суб’єктом особливого захисту, а частину другу цієї статті викласти у такій редакції:

Ті самі дії, вчинені повторно, або щодо неповнолітнього, або якщо вони заподіяли істотну шкоду охоронюваним законом правам, свободам та інтересам особи, караються арештом на строк від трьох до шести місяців або обмеженням волі на строк від трьох до п’яти років, або позбавленням волі на той самий строк;

– врегулювання механізмів обігу ігрового контенту, у тому числі в мережі Інтернет, та доступу до мережевих ігор з урахуванням вікового цензу;

– проведення віктимологічних профілактик злочинності в інформаційній сфері серед дітей різних вікових категорій;

2. У контексті розбудови в Україні орієнтованого на інтереси громадян інформаційного суспільства з метою імплементації європейських стандартів та підходів у забезпеченні прав дитини в Україні, основні напрямки реалізації яких окреслено Стратегією Ради Європи з прав дитини (2016 – 2021 рр.) розробити Державну цільову освітню програму “Освіта майбутнього” на період до 2021 року, у якій передбачити:

– створення рівних можливостей у доступі до інформації і знань для усіх дітей, незалежно від місця проживання і соціального статусу, що дозволить позбутися в Україні цифрової нерівності серед дітей та наслідків, до яких вона могла б призвести;

– підвищення рівня правосвідомості, правової та інформаційної культури у дітей шляхом імплементації у навчальний курс “Правознавство” основ інформаційного права та правових механізмів регулювання суспільних відносин в інформаційній сфері;

– впровадження у навчальний процес дисципліни “Інформаційна безпека”, як окремого предмета, або його викладання у складі дисципліни “Основи життєдіяльності”;

– модернізації методик викладання курсу “Інформатика” у шкільній програмі для підвищення комп’ютерної та інформаційної грамотності дітей з урахуванням сучасних викликів і загроз в інформаційній сфері;

– облаштування бібліотек безпечним широкосмуговим з’єднанням із мережею Інтернет з метою розширення можливостей доступу дітей до національних духовних, культурних та історичних цінностей, досягнень світової культури і науки відповідно до статті 20 Закону України “Про охорону дитинства” [3];

– створення у комп’ютерних класах навчальних закладів достатньої кількості робочих місць, обладнаних сучасною технікою і програмним забезпеченням із безпечним широкосмуговим доступом до мережі Інтернет, для оволодіння новими технологіями і здобуття навичок їх практичного використання у процесі пізнання й накопичення знань;

– проведення заходів національного і патріотичного виховання молоді в контексті протидії маніпулятивним інформаційно-психологічним впливам на дітей.

3. В умовах стрімкого зростання інтенсивності інформаційних обмінів та обсягів доступної для дітей інформації, у тому числі шкідливої або небезпечної для їх морального і психічного здоров’я, запровадити практику оцінки психофізичного стану під час проведення обов’язкових медичних профілактичних оглядів учнів загальноосвітніх навчальних закладів.

У зв’язку з цим пункт 5 Порядку здійснення медичного обслуговування учнів загальноосвітніх навчальних закладів, затвердженого Постановою Кабінету Міністрів України від 08.12.09 р. № 1318 [36] викласти у такій редакції:

Під час обов’язкових медичних профілактичних оглядів лікарі оглядають учнів та проводять обстеження, роблять висновки про стан їх фізичного і психічного здоров’я, визначають групу для занять фізичною культурою, дають рекомендації щодо додаткових обстежень, лікування (за наявності показань), профілактичних щеплень, режиму, харчування та здійснення інших заходів.

4. З метою моніторингу рівня інформаційно-психологічних впливів на індивідуальну та суспільну свідомість у навчальних закладах пропонується запровадити періодичний контроль морально-психологічного стану методом опитування і тестування, з подальшим аналітичним опрацюванням результатів, що дасть можливість

виявляти потенційно можливі загрози для інформаційної безпеки дитини та прогнозувати їх системність, направленість та подальшу динаміку.

5. У зв'язку із підвищенням інформаційно-психологічного навантаження на дитину в інформаційному суспільстві пропонується переглянути статус шкільного психолога та його роль у протидії негативним інформаційним впливам на дитину у процесі забезпечення її інформаційної безпеки.

6. З урахуванням кардинального зростання ролі інформаційної складової в усіх сферах життєдіяльності людини, суспільства і держави, а також тенденцій розвитку і наявного правового поля в інформаційній сфері, підготувати нову редакцію Національної програми правової освіти населення на заміну затвердженій Указом Президента України від 18 жовтня 2001 року № 992/2001 [37]. Заходи із забезпечення виконання цієї програми у новій редакції повинні враховувати тенденції розвитку суспільства з врахуванням існуючих та потенційно можливих викликів.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
2. Про основи національної безпеки України : Закон України від 19.06.03 р. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/964-15>
3. Про охорону дитинства : Закон України від 26.04.01 р. № 2402-III. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/2402-14>
4. Іванов В.Ф., Іванова Т.В. Медіакомпетентність та медіаграмотність як основні компетентності сучасного педагога // Інформаційне суспільство. – 2014. – № 20. – С. 96-99.
5. Дроздов О.Ю. Телебачення, як джерело впливу на соціальну спрямованість молоді : матеріали методологічного семінару АПН України [“Психолого-педагогічна наука і суспільна ідеологія”], (Київ, 12 листопада 1998 р.). – К., 1998. – 485 с.
6. Потятиник Б.В. Екранна агресія : знати, щоб вберегтися. – Режим доступу : http://www.lnu.edu.ua/mediaeco/ndch/potjt_ekran_agr.htm
7. Пацлаф Р. Застывший взгляд : физиологическое воздействие телевидения на развитие детей / Р. Пацлаф. – М. : Evidentis, 2003. – 224 с.
8. Брайант Д.. Основы воздействия СМИ / Д. Брайант, С. Томпсон. – М. – К., 2004. – 424 с.
9. Данильян О.Г., Дзьобань О.П. Інформаційне насильство : сутнісні проблеми. – Режим доступу : http://www.rusnauka.com/3_ANR_2011/Philosophia/2_78843.doc.htm
10. Алдер Х. НЛП : современные психотехнологии / Х. Алдер. – СПб. : Питер, 2000. – 160 с.
11. Безрукова О.М. Аналіз впливу ЗМІ на особистість підлітків : за матеріалами VI Міжнародної науково-практичної конференції [“Наукова молодь : досягнення та перспективи”] // Вісник ЛНУ ім. Тараса Шевченка. – 2010. – № 8(195). – С. 81-84. – (Педагогічні науки).
12. Савінова Н.А. Кримінально-правова політика та убезпечення інформаційного суспільства в Україні : монографія. – К. : Ред. журн. “Право України”. – Х. : Право, 2013. – 292 с.
13. Словник української мови : в 11 т. ; редкол. : І. К. Білодід (голова) та ін. – (Акад. наук Укр. РСР, Ін-т мовознавства ім. О.О. Потебні). – К. : Наук. думка, 1970 – 1980 рр. – Т. 1. – 1970. – 799 с.
14. Там само. – Т. 4. – 1973. – 840 с.
15. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/537-16>
16. Прибутько П.С. Інформаційні впливи : роль у суспільстві та сучасних воєнних конфліктах / П.С. Прибутько, І.Б. Лук'янець. – К. : ПАЛИВОДА А.В., 2007. – 252 с. – С. 11.
17. Інформаційно-психологічне протиборство (еволюція та сучасність) : монографія / [Я.М. Жарков, В.М. Петрик, М.М. Присяжнюк та ін.]. – К. : ПАТ “Віпол”, 2013. – 248 с.

18. Радзівська О.Г. Проблеми негативних інформаційних впливів на дитину в Україні в умовах збройного протистояння // Науковий вісник Ужгородського національного університету. – 2017. – № 42. – С. 197-200. – (Серія “Право”).

19. Янковський С.Я. Концепции общей теории информации. – Режим доступу : <http://n-t.ru/t/p/ng/oti.htm>

20. Про інформацію : Закон України від 02.10.92 р. № 2657-ХІІ. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/2657-12>

21. Про права дитини : Конвенція ООН від 20 листопада 1989 г. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_021.

22. Про охорону дитинства : Закон України від 26.04.01 р. № 2402-ІІІ. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/2402-14>

23. Про захист суспільної моралі : Закон України від 20.11.03 р. № 1296-ІV. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/1296-15>

24. Про телебачення і радіомовлення : Закон України від 21.12.93 р. № 3759-ХІІ. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/3759-12>

25. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16.11.92 р. № 2782-ХІІ. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/2782-12>

26. Про рекламу : Закон України від 03.07.96 р. № 270/96-ВР. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80>

27. Пучков О.О. Інформаційна безпека у контексті сьогоденних реалій : філософський аспект // Гуманітарний вісник ЗДІА. – 2015. – Вип. 60. – Ст. 240.

28. Чачанидзе І. ИНТЕРНЕТ: Правила безопасности. – Режим доступу : // <http://www.my-baby.info/news/view/323.html>

29. Діти в Інтернеті : як навчити безпеці у віртуальному світі : посібник для батьків / [І. Литовченко, С. Максименко, С. Болтівець та ін.]. – К. : ТОВ “Видавничий будинок “Аванпост-Прим”, 2010. – 48 с.

30. Про захист персональних даних : Закон України від 1.06.10 р. № 2297-ІV. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2297-17>

31. Кримінальний кодекс України : Закон України від 1.09.01 р. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2341-14/page>

32. Конкурентная разведка в компьютерных сетях / [А.Г. Додонов, Д.В. Ландэ, В.В. Прищеп, В.Г. Путятин]. – К. : ИПРИ НАН Украины, 2013. – 248 с.

33. Council of Europe Strategy for the rights of the child 2016 – 2021 : Council of Europe; Strasbourg, 6 November 2015. – Режим доступу : <https://rm.coe.int/168048dee3>

34. Про схвалення Концепції Державної соціальної програми “Національний план дій щодо реалізації Конвенції ООН про права дитини” на період до 2021 року : Розпорядження Кабінету Міністрів України від 5.04.17 р. № 230-р. – Режим доступу : <http://www.kmu.gov.ua/control/uk/cardnpd?docid=249890555>

35. Декларація прав дитини : Декларація ООН від 20 листопада 1959 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_384

35. Про затвердження Порядку здійснення медичного обслуговування учнів загальноосвітніх навчальних закладах : Постанова Кабінету Міністрів України від 08.12.09 р. № 1318. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1318-2009-%D0%BF>

36. Про Національну програму правової освіти населення : Указ Президента України від 18.10.01 р. № 992/2001. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/992/2001>

~~~~~ \* \* \* ~~~~~

УДК 343.9

**ГУЦАЛЮК М.В.**, кандидат юридичних наук, с.н.с., доцент,  
Міжвідомчий науково-дослідний центр з проблем боротьби  
з організованою злочинністю при РНБО України

## **ВДОСКОНАЛЕННЯ ЧИННОГО ЗАКОНОДАВСТВА З ПИТАНЬ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ**

***Анотація.** В статті досліджуються питання інформаційної безпеки та протидії кіберзлочинності. Пропонуються напрями вдосконалення чинного законодавства у даній галузі та запровадження безпечного сегменту Інтернет – ID-web.*

***Ключові слова:** кіберзлочинність, кібербезпека, міжнародне співробітництво, ID-web.*

***Аннотация.** В статье исследуются вопросы информационной безопасности и противодействия киберпреступности. Предлагаются направления совершенствования действующего законодательства в данной сфере и внедрения безопасного сегмента Интернет – ID-web.*

***Ключевые слова:** киберпреступность, кибербезопасность, международное сотрудничество, ID-web.*

***Summary.** The article deals with the issues of cybersecurity and cybercrime. The improvement of the legislation in this area and the introduction of safe ID-web Internet are proposed.*

***Keywords:** cybercrime, cybersecurity, international cooperation, ID-web.*

**Постановка проблеми.** Поява інформаційно-комунікаційних технологій (далі – ІКТ) спричинила істотний вплив на розвиток як світової економіки, так і міжнародної безпеки. Ці технології дають змогу отримувати величезні економічні та соціальні вигоди. Разом з цим, вони також можуть використовуватися в цілях, несумісних з підтриманням безпеки, внаслідок чого в останні роки помітно підвищився рівень ризику щодо вчинення злочинів із використанням ІКТ.

**Результати аналізу наукових публікацій.** Експерти Всесвітнього економічного форуму в Давосі підготували та у січні 2017 року опублікували щорічну доповідь про глобальні ризики у світі під назвою “Global Risks Report 2017”. Виходячи з її концептів, на третьому місці за важливістю для світової спільноти перебувають технологічні ризики – крадіжки персональних даних, махінації з ними, масштабні кібератаки та кіберзлочинність [1].

Згідно зі звітом “2016 Norton Cyber Security Insights Report” американської компанії Symantec, світового лідера в галузі рішень інформаційної безпеки, у 2016 році тільки з 21-єї країни зазнали загроз від кіберзлочинності 689 мільйонів чоловік. Це явище стало настільки поширеним, що багато людей однаково побоюються он-лайн і реальних ризиків. Відповідно до досліджень Європолу, втрати держав-членів ЄС від кіберзлочинності складають 265 мільярдів євро в рік, а для світової економіки ця цифра становить близько 900 мільярдів євро. І це тільки фінансовий бік проблеми [2].

Виходячи із сучасних реалій, заслуговує на увагу позиція колишнього помічника генпрокурора з питань національної безпеки в Міністерстві юстиції США Джона Карліна, що однією із тенденцій поширення кіберзагроз у майбутні 3 – 5 років стануть саме кіберзлочини за підтримки урядів, а також атаки, що можуть здійснюватися урядовими кібершпигунами заради отримання фінансової вигоди [3]. Це підтвердив і Генеральний секретар НАТО Йенс Столтенберг, який повідомив під час прес-конференції в Брюсселі

15 лютого 2017 року, що Альянс стикається з серйозними кібератаками, за якими стоять хакери, які діють не тільки у власних інтересах, а також й держави-агресора [4]. Це особливо небезпечно для України, яка стала своєрідним полігоном для відпрацювання таких атак. Наприклад, тільки протягом двох місяців наприкінці 2016 року було скоєно понад 6,5 тисячі кібератак на об'єкти п'яти відомств і 31 державного інформаційного ресурсу, багато з яких організовані зі сторони РФ [5].

Особливе занепокоєння сьогодні викликає можливість вчинення терористичних актів за допомогою ІКТ на об'єктах критичної інфраструктури. У 2015 та 2016 роках на енергетичний та фінансовий сектор України було здійснено низку потужних кібератак, які призвели до значних шкідливих наслідків. Питання забезпечення безпеки на об'єктах критичної інфраструктури розглянуте 13 лютого 2017 року під час головування України в Раді Безпеки ООН, де була прийнята відповідна Резолюція № 2341 (2017). У документі зазначено, що Рада Безпеки ООН рекомендує посилити інформованість про проблеми, які створюють терористичні атаки на об'єкти критичної інфраструктури, і закликає всі країни удосконалювати стратегії зменшення ризиків таких нападів; зміцнювати міжнародні партнерські відносини із зацікавленими сторонами, як державними, так і приватними, з метою обміну інформацією та досвідом для відновлення після заподіяної ними шкоди. Також усі держави, які в змозі робити це, повинні сприяти в забезпеченні ефективного нарощування потенціалу, професійної підготовки, технічної допомоги, передачі технологій і реалізації програм з тим, щоб всі держави могли досягти захисту критично важливих об'єктів інфраструктури від терористичних нападів [6].

В зв'язку з зазначеним сьогодні в Україні разом з докорінними змінами у зовнішньому та внутрішньому безпековому середовищі, появою нових викликів та загроз в умовах гібридної війни активно реформується сектор безпеки і оборони з урахуванням специфіки кіберпростору. Так, Указом Президента України від 26 травня 2015 року № 287/2015 затверджено Стратегію національної безпеки України, якою визначені основні пріоритети забезпечення кібербезпеки в державі.

З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави окремим документом розроблена і затверджена Указом Президента України від 15 березня 2016 року № 96/2016 Стратегія кібербезпеки України.

Указом Президента України від 13 лютого 2017 року № 32/2017 затверджено Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, у якому визначені термінові та короткострокові завдання Кабінету Міністрів України, правоохоронним органам щодо захисту інформації в інформаційно-телекомунікаційних системах, та зокрема на об'єктах критичної інфраструктури.

Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська, П.Д. Біленчук., К.І. Беляков, В.М. Бутузов, В.Д. Гавловський, М.А. Погорецький, В.Г. Хахановський, В.П. Шеломенцев, О.М. Юрченко та інші. Проте стрімкий розвиток інформаційних технологій та способів і методів протиправної діяльності у кіберпросторі спонукає для подальших досліджень.

**Метою статті** є продовження дослідження щодо протиправної діяльності в глобальній мережі Інтернет та надання пропозицій для удосконалення системи безпеки в українському сегменті глобальної мережі Інтернет.

**Виклад основного матеріалу.** Враховуючи зростаючі масштаби кіберзлочинності, з метою розробки юридичних механізмів протидії загрозам у комп'ютерних мережах у травні 2011 року Міжнародний союз електрозв'язку і Управління ООН з наркотиків та

злочинності підписали угоду про боротьбу з кіберзлочинністю. Для прийняття конкретних заходів, спрямованих на обмеження комп'ютерних загроз, ООН розробила Глобальну програму кібербезпеки, в якій визначено п'ять основних напрямів [7]:

- 1) правові заходи;
- 2) технічні та процедурні заходи;
- 3) організаційні структури;
- 4) програма підвищення компетентності;
- 5) міжнародне співробітництво.

У зв'язку з тим, що основною ознакою кіберпростору є відсутність міждержавних кордонів, особливого значення набуває правове регулювання суспільних відносин, які виникають під час виявлення та розслідування протиправної діяльності в ньому. Зловмисник може знаходитися в одній державі, активувати кібератаку з інформаційного ресурсу, розташованого в іншій, а збитки будуть завдані фізичній чи юридичній особі, яка знаходиться в третій державі. При цьому шкідливі програми можуть перетинати ще низку кордонів, ніяк не повідомляючи про це уповноважені державні органи.

Сьогодні можна виділити п'ять груп міжнародних і регіональних нормативно-правових актів, які регулюють суспільні відносини у сфері протидії кіберзлочинності. В них входять документи, розроблені під егідою:

- Ради Європи Європейського союзу,
- Співдружності Незалежних Держав або Шанхайської організації співпраці,
- міждержавних африканських організацій,
- Ліги арабських держав і (V) Організації Об'єднаних Націй.

Існують і інші теоретичні підходи щодо регулювання проблем кіберпростору. Так, науковець Джон Перрі Барлоу ще у 1996 році запропонував розробити та прийняти Женевську декларацію незалежності кіберпростору, яка б передбачала функціонування Міжнародного суду у зв'язку тим, що кіберпростір не належить до жодної країни і є інтернаціональним. Проте цей документ так і не був прийнятий [8].

Серед основних міжнародних нормативно-правових документів щодо протидії кіберзлочинності, у тому числі організованої, слід виокремити такі:

– Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності (United Nations Convention against Transnational Organized Crime), підписана у м. Палермо 12 грудня 2000 року та ратифікована із застереженнями і заявами Законом України від 04.02.04 р. № 1433-IV [9];

– Європейська конвенція про взаємну допомогу у кримінальних справах (European Convention on Mutual Assistance in Criminal Matters), підписана у м. Страсбурзі 20 квітня 1959 року та ратифікована із заявами і застереженнями Законом України від 16.01.98 р. № 44/98-ВР [10];

– Конвенція про кіберзлочинність (Convention on Cybercrime), підписана 23 листопада 2001 року в м. Будапешті і ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV [11].

Поряд з нормативно-правовим забезпеченням, заходи боротьби з кіберзлочинністю повинні також супроводжуватися середньостроковими і довгостроковими стратегічними цілями, спрямованими на захист інформаційних ресурсів і притягнення розробників злочинних схем до відповідальності.

Більшість країн розробили та затвердили відповідні нормативно-правові документи (стратегії), в яких визначаються напрями протидії загрозам в інформаційній сфері. До таких країн, зокрема, належать США, Франція, Німеччина, Великобританія, Канада, Японія та інші.

Надзвичайно великого значення захисту кіберпростору надає Організація Північноатлантичного договору (НАТО). У країнах Альянсу, економіка яких розвивається у складному середовищі, кіберзагрози стають усе більш поширеними, складними і руйнівними, а кібератаки стали частиною гібридної війни. НАТО і його союзники покладаються на сильну колективну оборону на основі тісного співробітництва між його учасниками і визначають кіберзахист одним з основних своїх завдань, а кіберпростір – як область операцій, в яких НАТО має захищати себе так само ефективно, як це робить у повітрі, на суші і на морі [12].

Належне місце займає кібербезпека і в Європейському Союзі. Стратегія кібербезпеки ЄС 2013 року стала першим всеохоплюючим документом Європейського Союзу в даній сфері. Документ охоплює усі аспекти кіберпростору: внутрішній ринок, правосуддя, внутрішню та зовнішню політику.

Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

- свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;
- застосування законодавства ЄС у кіберпросторі у тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на всьому глобальному суспільстві: від пересічних громадян до держав;
- розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [13].

Як уже зазначалося, усі розвинені країни з урахуванням міжнародних угод, розробляють свої власні нормативні документи з питань протидії кіберзлочинності та кібербезпеки. Найбільш розвинену систему таких нормативно-правових актів мають США. Не дивлячись на те, що в цій країні були прийняті одні з найперших у світі законів в даній галузі і сьогодні функціонують такі закони, як: Закон “Про злочини, пов’язані з засобами доступу” (Fraud and related activity in connection with access devices) [14], Закон “Про злочини, пов’язані з комп’ютерами” (Fraud and related activity in connection with computers) [15], Закон “Про перехоплення електронних повідомлень та прослуховування переговорів” (Wire and Electronic Communications Interception and Interception of Oral Communications) [16] тощо.

Законодавство США постійно вдосконалюється залежно від загроз, які постають перед суспільством. Так, наприклад, після терористичних актів 11 вересня 2001 року був прийнятий так званий “Патріотичний акт”, – The USA Patriot Act: Preserving Life and Liberty (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism). Відповідно до цього документа ФБР, Агентству національної безпеки були надані широкі права щодо електронного спостереження та розслідування кіберзлочинів, зокрема ст. 202 документа передбачала право на перехоплення голосових повідомлень при розслідуванні комп’ютерних злочинів, ст. 209 полегшувала доступ до електронних повідомлень (електронна пошта), ст. 210 розширила перелік даних, які відповідно до запиту можуть отримувати правоохоронні органи у провайдерів, наприклад, IP користувача, номер кредитної картки користувача, якою він оплачував інтернет-послуги тощо, що дало змогу ідентифікувати кіберзлочинців та відстежувати їх діяльність в мережі. Проте у 2015 році положення цього закону були відмінені у зв’язку з порушенням прав людини [17].

Нещодавно були прийняті Закон “Поширення інформації про кібербезпеку” (Cybersecurity Information Sharing Act (CISA), 2015 [18] та “Система покращення кібербезпеки критичної інфраструктури” (Framework for Improving Critical Infrastructure Cybersecurity) 2016 [19];

Для ефективного реагування правоохоронних органів на повідомлення про кіберзлочини необхідна дієва правова база для проведення слідчих дій та оптимальний баланс між дотриманням недоторканності приватного життя і повноваженнями з проведення розслідувань, оперативний доступ та засоби отримання електронних доказів у постачальників послуг мережі Інтернет, а також забезпечення належного навчання та технічних можливостей співробітників. З огляду на зазначене провідні країни світу формують спеціальні підрозділи протидії кіберзлочинності.

Так у США активно відбувається процес створення та реформування існуючих спеціалізованих підрозділів, серед яких:

- Відділ комп’ютерної злочинності та інтелектуальної власності Computer Crime And Intellectual Property Section (CCIPS) міністерства юстиції;

- Національна об’єднана група кіберрозслідувань – National Cyber Investigative Joint Task Force Федерального бюро розслідувань, яка проводить розслідування кібератак, терористичних операцій, втручань у комп’ютерні мережі з-за кордону;

- Цільова група протидії електронним злочинам Секретної Служби США (Secret Service on Electronic Crimes Task Forces).

У 2006 році був створений перший у світі підрозділ кібервійськ – Air Force Cyber Command, який у 2009 році реорганізовано в U.S. Army Cyber Command – структуру збройних сил США, мета якого – ведення кібервоєн [20].

Створення кіберкомандування США активізувало діяльність інших країн у цій сфері. У грудні 2009 року Південна Корея оголосила про створення підрозділу кібервійськ. Також активно розпочав підготовку до створення кібервійськ британський Центр урядового зв’язку. У 2010 році Китай створив підрозділ, що займається питаннями кібервійни та інформаційної безпеки. В РФ у 2014 році заснували війська інформаційних операцій для кібернетичного протидіювання з супротивниками.

У Великобританії для розслідування злочинів у сфері інформаційних технологій у 2001 році був створений самостійний Національний центр протидії злочинам у сфері високих технологій – National High Tech Crime Unit (NHTCU). У 2006 році центр було введено до складу Агенції протидії організованій злочинності – The Serious Organised Crime Agency (SOCA), а з 2013 року він має назву National Cyber Crime Unit і діє у складі Національного агентства протидії злочинності (National Crime Agency) [21].

Також відповідно до Національного плану з кібербезпеки (National Cyber Security Plan) та прийнятої 1 листопада 2016 року Національної стратегії кібербезпеки Великобританії (National Cyber Security Strategy 2016-2021) [22] засновано Національний центр з кібербезпеки (National Cyber Security Centre), Лондонський офіс якого відкрито в лютому 2017 року [23]. Метою діяльності цього центру є надання консультацій і підтримки державному і приватним секторам в запобіганні кіберзагрозам.

Активну позицію щодо протидії кіберзагрозам займають і міжнародні організації. У січні 2013 року у структурі Європолу в Гаазі (Нідерланди) розпочав свою роботу Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre – EC3) [24]. Відповідаючи за стратегічний аналіз стану кіберзлочинності, формулювання політики і розробку законодавства, а також навчання правоохоронців, EC3 спрямовує свою діяльність на кіберзлочини, які:

- вчиняються організованими злочинними групами, зокрема які генерують великі злочинні доходи, наприклад, такі як інтернет-шахрайство;

- завдають серйозної шкоди жертвам, такі як он-лайн-сексуальна експлуатації дітей;

– впливають на критичну інфраструктуру та інформаційні системи в країнах ЄС, в тому числі кібератаки.

За кілька років з моменту свого створення ЕСЗ вже зробив значний внесок у боротьбу з кіберзлочинністю: він брав участь у десятках резонансних операцій, в результаті яких відбулися сотні арештів. Співробітниками ЕСЗ проаналізовано понад 800 тисяч файлів, переважна більшість яких виявилися шкідливими [25].

З метою протидії транснаціональній злочинності, у тому числі для розслідування кіберзлочинів, країни-члени Європейського Союзу об’єднали свої зусилля та створили Європейську організацію з питань юстиції (Євроюст), повноваження якої спрямовані на досягнення таких цілей: розвиток і покращення координації між компетентними органами держав-учасниць щодо дій із розслідування й кримінального переслідування на власних територіях з урахуванням будь-якого запиту, що надійшов від компетентного органу однієї з них, а також будь-якої інформації, наданої компетентним органом на підставі розпоряджень, виданих відповідно до установчих договорів; зміцнення співробітництва між компетентними органами держав-учасниць.

27 червня 2016 року в Брюсселі Україна підписала Угоду про співпрацю з Євроюстом. Підписи під документом поставили Генеральний прокурор України Юрій Луценко та Президент Євроюсту Мішель Конінкс. На церемонії підписання Угоди був присутній Президент України Петро Порошенко [26].

В Україні впродовж останніх років йде активне реформування та створення нових структур, які спрямовані на протидію кіберзлочинності. Сьогодні в Україні разом з докорінними змінами у зовнішньому та внутрішньому безпековому середовищі, появою нових викликів та загроз в умовах гібридної війни активно реформується сектор безпеки і оборони.

5 жовтня 2015 року був утворений Департамент кіберполіції – структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), телекомунікаційних та комп’ютерних Інтернет-мереж і систем.

Указом Президента України від 7 червня 2016 року № 242/2016 сформований Національний координаційний центр кібербезпеки, робочий орган в Раді національної безпеки і оборони України, на який покладено координацію заходів суб’єктів забезпечення кібербезпеки.

Водночас залишаються поки що невирішеними низка актуальних завдань, що визначені Стратегією кібербезпеки.

Зокрема мова йде про невизначеність на законодавчому рівні таких понять, як кіберпростір, кіберзлочин, кібератака, об’єкти критичної інфраструктури та ін., що призводить до певних проблем в практичній діяльності правоохоронних органів, прокуратури та судів. Необхідно також вдосконалити систему збору, аналізу та оцінки електронних (цифрових) доказів.

Особливого значення набуває повна імплементація Конвенції про кіберзлочинність у частині наступних статей:

- Стаття 16 – Термінове збереження комп’ютерних даних, які зберігаються;
- Стаття 17 – Термінове збереження і часткове розкриття даних про рух інформації;
- Стаття 19 – Обшук і арешт комп’ютерних даних, які зберігаються;
- Стаття 20 – Збирання даних про рух інформації у реальному масштабі часу;
- Стаття 21 – Перехоплення даних змісту інформації.



Зазначені питання доцільно вирішити прийняттям Закону України “Про основні засади забезпечення кібербезпеки України”, проект якого знаходиться на розгляді в Верховній Раді України.

Однією з основних проблем протидії злочинності, у тому числі організованої у мережі Інтернет, є складність ідентифікації її користувачів. Адже злочинці, вчиняючи протиправні дії, використовують можливості анонімності у мережі Інтернет і завжди приховують своє справжнє ім'я. Наприклад, це можуть бути і адміністратори мережі “Синіх китів”, і педофіли, які зваблюють дітей через Інтернет, або зловмисники, що надсилають листи від імені державних установ, а насправді заражають комп'ютери вірусами з метою викрадення інформації або її шифрування для подальшого шантажу власника ресурсу.

У 2008 році був запропонований механізм під умовною назвою “ID-web” [27], який полягає у використанні біометричних властивостей людини для ідентифікації її в мережі Інтернет. Така ідентифікація дає змогу однозначно визначати, хто розмістив певну інформацію, хто прокоментував відповідну статтю або хто конкретно написав електронного листа. Для користувачів, які бажають залишатися анонімними, залишаються всі інші “ID не підтвержені” ресурси. Технологічні можливості для реалізації такої технології склалися після впровадження в Україні паспорта громадянина України у вигляді пластикової картки.

Реалізація відповідної системи ID-web на державному рівні надасть змогу зростання доступності процедур прямої демократії, а саме виконання п. 4.2 Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2016 – 2020 роки [28] “Забезпечення ефективних процедур участі громадськості під час формування та реалізації державної, регіональної політики, вирішення питань місцевого значення” зокрема безпечним доступом до державних реєстрів, участі в обговоренні законодавчих ініціатив, формуванні петицій як до місцевих так і державних органів влади.

Подібну систему ідентифікації сьогодні активно використовують країни Прибалтики для забезпечення безпечного функціонування електронного урядування, Інтернет-банкінгу тощо. Кожен громадянин може отримати будь-яку інформацію про себе з державних інформаційних ресурсів он-лайн, використовуючи для ідентифікації користувача свою ID-картку та PIN-код.

На фоні зростання числа кібератак користувачі Інтернет починають втрачати довіру до паролів. Вони відкривають для себе нові технології та бажають використовувати їх для безпечного доступу до своїх даних. Так за он-лайн дослідженням організації “YouGov”, в Великобританії 56 % користувачів Інтернету бажають застосовувати біометричні методи аутентифікації замість традиційних паролів для цифрового банкінгу. Тільки 19 % опитаних назвали паролі пріоритетним методом захисту і лише 13 % зробили вибір на користь перевірочних питань [29].

### **Висновки.**

З часу прийняття у березні 2016 року Стратегії кібербезпеки України в нашій державі досягнуто значних успіхів щодо організації протидії кіберзлочинності. Водночас залишається низка питань, які необхідно вирішити найближчим часом.

В зв'язку з підписанням Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, перш за все необхідно вдосконалити чинне законодавство відповідно до положень Конвенції про кіберзлочинність, прийняти відповідні нормативно-правові документи, які б законодавчо визначили термінологію

щодо кіберзлочинності, розробити ефективні механізми співробітництва з приватним сектором, особливо Інтернет-провайдерами з метою оперативного отримання електронних даних, необхідних для розслідування кіберзлочинів, активно розвивати міжнародне співробітництво у галузі протидії кіберзлочинності та розробити механізм функціонування захищеного Інтернету на основі ID-документів.

### Використана література

1. The Global Risks Report 2017. – Режим доступу : [//www3.weforum.org/docs/GRR17\\_Report\\_web.pdf](http://www3.weforum.org/docs/GRR17_Report_web.pdf)
2. – Режим доступу : <https://us.norton.com/cyber-security-insights-2016>
3. Эксперт прогнозирует рост числа спонсируемых государствами киберпреступлений. – Режим доступу : [//www.securitylab.ru/news/485310.php](http://www.securitylab.ru/news/485310.php)
4. НАТО: Кібератаки на альянс здійснюють держави. – Режим доступу : <http://ua.korrespondent.net/world/3815528>
5. Госструктуры подверглись 6500 кибератакам, к некоторым причастна Россия. – (Порошенко). – Режим доступу : <http://biz.censor.net.ua/news/3018072>
6. – Режим доступу : <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/61/PDF/N1703861.pdf?OpenElement>
7. – Режим доступу : [//www.itu.int/en/action/cybersecurity/Pages/gca.aspx](http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx)
8. – Режим доступу : [//www.eff.org/cyberspace-independence](http://www.eff.org/cyberspace-independence)
9. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності : Резолюція 55/25 Генеральної Асамблеї від 15 листопада 2000 року. – Режим доступу : [http://zakon5.rada.gov.ua/laws/show/995\\_789](http://zakon5.rada.gov.ua/laws/show/995_789)
10. Про ратифікацію Європейської конвенції про взаємну допомогу у кримінальних справах, 1959 рік, та Додаткового протоколу 1978 року до Конвенції № 1433-IV : Закон України від 04.02.04 р. – Режим доступу : <http://zakon0.rada.gov.ua/laws/show/44/98-%D0%B2%D1%80>
11. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824-IV (2824-15). – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2824-15>
12. – Режим доступу : [//www.nato.int/cps/en/natohq/topics\\_78170.htm](http://www.nato.int/cps/en/natohq/topics_78170.htm)
13. – Режим доступу : [//www.eeas.europa.eu/policies/eu-cyber-security/index\\_en.htm](http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm)
14. 618 U.S. Code § 1029 – Fraud and Related Activity in Connection with Access devices. – Режим доступу : [//www.law.cornell.edu/uscode/text/18/1029](http://www.law.cornell.edu/uscode/text/18/1029)
15. 718 U.S. Code § 1030 – Fraud and related activity in connection with computers. – Режим доступу : [//www.law.cornell.edu/uscode/text/18/1030](http://www.law.cornell.edu/uscode/text/18/1030)
16. 918 U.S. Code Chapter 119 – Wire and electronic communications interception and interception of oral communications. – Режим доступу : [//www.law.cornell.edu/uscode/text/18/part-I/chapter-119](http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119)
17. The USA Patriot Act: Preserving Life and Liberty. – Режим доступу : [//www.justice.gov/ll/highlights.htm](http://www.justice.gov/ll/highlights.htm)
18. Cyber Intelligence Sharing and Protection Act. – Режим доступу : [https://en.wikipedia.org/wiki/Cyber\\_Intelligence\\_Sharing\\_and\\_Protection\\_Act](https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act)
19. Framework for Improving Critical Infrastructure Cybersecurity 2016. – Режим доступу : [http://csrc.nist.gov/groups/SMA/forum/documents/january2016\\_presentations/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf](http://csrc.nist.gov/groups/SMA/forum/documents/january2016_presentations/Cybersecurity-Framework-for-FCSM-Jan-2016.pdf)
20. – Режим доступу : [//www.arcyber.army.mil/Pages/ArcyberHome.aspx](http://www.arcyber.army.mil/Pages/ArcyberHome.aspx)
21. – Режим доступу : [//www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit](http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit)
22. – Режим доступу : [//www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/567242/national\\_cyber\\_security\\_strategy\\_2016.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)
23. – Режим доступу : [//www.ncsc.gov.uk](http://www.ncsc.gov.uk)

24. – Режим доступу : [//www.europol.europa.eu/ec3](http://www.europol.europa.eu/ec3)

25. – Режим доступу : [//www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3](http://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3)

26. Україна підписала угоду про співробітництво з Євроюстом: – Режим доступу : <http://tsn.ua/politika/ukrayina-pidpisala-ugodu-pro-spivrobotnictvo-z-yevroyustom-680835.html>

27. Гуцалюк М.В. Впровадження ID-web як необхідна умова безпеки в Інтернет // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2008. – № 18. – С. 265-269.

28. Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2016 – 2020 роки : Указ Президента України від 26.02.16 р. № 68/2016.

29. Пароли или биометрия : европейцы сделали свой выбор. – Режим доступу : <http://psm7.com/news/paroli-ili-biometriya-evropejcy-sdelali-svoj-vybor.html>

~~~~~ \* \* \* ~~~~~

УДК 343.14: 004

СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз
Українського науково-дослідного інституту
спеціальної техніки та судових експертиз СБ України,
ЛЕОНОВ Б.Д., доктор юридичних наук, старший науковий співробітник,
провідний науковий співробітник Українського науково-дослідного
інституту спеціальної техніки та судових експертиз СБ України

ОКРЕМІ ПРОБЛЕМИ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З НЕПРАВОМІРНИМ ДИСТАНЦІЙНИМ ДОСТУПОМ ДО КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

Анотація. У статті розглядаються аспекти криміналістичної характеристики комп'ютерних злочинів та проблемні питання розробки методичних матеріалів для проведення експертних досліджень спеціальних програмних засобів, призначених для негласного отримання комп'ютерної інформації.

Ключові слова: комп'ютерна інформація, комп'ютерні злочини, розслідування.

Аннотация. В статье освещаются аспекты криминалистической характеристики компьютерных преступлений и проблемные вопросы разработки методических материалов для проведения экспертных исследований специальных программных средств, предназначенных для негласного получения компьютерной информации.

Ключевые слова: компьютерная информация, компьютерные преступления, расследование.

Summary. The article considers aspects of the forensic characteristics of computer crimes and the problematic issues of developing methodological materials for conducting expert studies of special software intended for covert obtaining computer information.

Keywords: computer information, computer crime, investigation.

Постановка проблеми. На сьогодні одночасно з стрімкими процесами інформатизації суспільства спостерігається суттєве підвищення рівня та масштабів загроз інформаційній безпеці держави. Радикальні зміни в інформаційних стосунках у всіх сферах діяльності людини, суспільства та держави передусім пов'язані із застосуванням глобальних телекомунікаційно-інформаційних мереж, в першу чергу, мережі Інтернет.

Результати аналізу наукових публікацій. Мережа Інтернет, як принципово відкрита система, забезпечує вільний і анонімний доступ до інформаційних ресурсів, що надає різноманітні можливості правопорушень, пов'язаних з неправомірним доступом до комп'ютерної інформації [1 – 2]. Злочинність у цій сфері отримала назву “комп'ютерна”, а останнім часом поширюється термін “кіберзлочинність”, що повніше охоплює об'єкти посягання цього виду злочинів. Останні швидкими темпами поширюються, у зв'язку з розповсюдженням багатofункціональних апаратно-програмних засобів, що можуть бути використані для несанкціонованого доступу до телекомунікаційних та комп'ютерних мереж. Поряд із застосуванням традиційних засобів здійснення комп'ютерних злочинів спостерігається стала тенденція розповсюдження спеціальних програмних засобів, призначених для неправомірного дистанційного доступу та негласного отримання інформації з абонентських пристроїв телекомунікаційних мереж, комп'ютерних систем [1; 6].

За даними Інтерполу, у 2000 р. доходи злочинців, в основному організованих злочинних груп, пов'язані з використанням новітніх технологій, посіли третє місце у світі після доходів від торгівлі наркотиками і зброєю [3]. Ці обставини призвели до різкого загострення кримінальної обстановки в інформаційній сфері. У зв'язку з цим Рада Європи 23 листопада 2001 р. схвалила Конвенцію “Про кіберзлочинність”, у якій передбачені основні засади та напрями міжнародної співпраці у цій діяльності, а саме: збереження протягом визначеного терміну комп'ютерних даних, у т.ч. на території інших країн – можливих їх користувачів, термінове розкриття за необхідності збереження даних, взаємна допомога у збиранні даних про рух інформації, її перехоплення тощо. В ЄС, а також в провідних європейських країнах (Австрія, Іспанія, Нідерланди, Польща, Угорщина, Фінляндія) прийняті стратегії кібербезпеки.

Складність інформаційних технологій та безмежна сфера їх використання при здійсненні комп'ютерних злочинів зумовлюють подальшу потребу дослідження криміналістичної характеристики комп'ютерних злочинів, вдосконалення існуючого механізму захисту інформаційних ресурсів в кіберпросторі, забезпечення відповідної профілактичної діяльності [2, с. 257; 4].

Основи криміналістичної теорії досліджень злочинів у сфері комп'ютерної інформації були закладені відносно недавно (наприкінці 90-х – початку 2000-х років) у роботах Н.М. Ахтирської, Ю.М. Батурина, П.Д. Біленчука, В.Б. Вехова, В.Д. Гавловського, В.О. Голубєва, М.В. Гуцалюка, В.Е. Козлова, В.В. Крилова, В.А. Мещерякова, А.Л. Осипенко, В.Ю. Рогозіна, О.Р. Росинської, Н.А. Селиванова, О.М. Черкуна, О.К. Юдіна й інших авторів.

Серед закордонних досліджень потрібно згадати методичні матеріали з розслідування комп'ютерних злочинів Д. Айкова, К. Сейгера, У. Фонсторха та К. Браїана.

Важливий внесок зробили Е.Р. Россинска і А.І. Усова, які заклали наукові основи для проведення такого нового виду інженерно-технічних експертиз, як комп'ютерно-технічні експертизи. Особливе значення для криміналістичної теорії й практики мало введення таких нових понять, як віртуальні сліди, електронні докази, формулювання базових принципів слідчих дій [5, с. 64].

Водночас, серед дослідників немає єдності поглядів з питань розслідування комп'ютерних злочинів. Це стосується як тлумачення термінів, визначення криміналістичної характеристики злочинів у сфері комп'ютерної інформації, так і вироблення техніко-криміналістичних засобів і методів, тактико-криміналістичних і організаційно-криміналістичних прийомів та формулювання рекомендацій з розслідування цих злочинів.

Не применшуючи теоретичну та практичну значимість проведених досліджень цієї теми, варто зазначити, що вони не вичерпують усіх криміналістичних аспектів розслідування злочинів, пов'язаних з неправомірним дистанційним доступом до комп'ютерної інформації.

Метою статті є удосконалення методичного забезпечення розслідування комп'ютерних злочинів.

Виклад основного матеріалу. Комп'ютерні технології та міжнародні інформаційно-комунікаційні мережі створили нові умови, які сприяють вчиненню злочинів як на національному, так і на міжнародному рівні. Організовані злочинні утворення у повному обсязі використовують нові технології для відмивання коштів, отриманих злочинним шляхом, поширення неправдивої інформації, несанкціонованого доступу до інформаційних систем, вчинення інших правопорушень в цій сфері. Загроза комп'ютерної злочинності полягає і в тому, що вона надає значну матеріальну

підтримку організованої злочинності для вчинення насильницьких злочинів, зокрема, терористичних актів. На окрему увагу заслуговують злочинні посягання, що здійснюються за допомогою спеціальних програмних засобів, так званих “шпигунських” програм, призначених для негласного віддаленого доступу до інформаційно-телекомунікаційних мереж і отримання комп’ютерної інформації. Ці злочинні дії в останні роки стали домінуючими серед інших категорій комп’ютерних злочинів [8].

Розслідування комп’ютерних злочинів стикається зі значними труднощами, зумовленими складністю виявлення цих високотехнологічних злочинів, високим рівнем їх латентності, недосконалістю статистичного обліку комп’ютерних злочинів, що ускладнюють узагальнення слідчої, судової та експертної практики [6].

Зауважимо, що високий рівень латентності цих злочинів викликає серйозні негативні наслідки. Вона створює сприятливу психологічну обстановку для вчинення нових злочинів, сприяє формуванню стійких злочинних утворень, порушує принцип невідворотності покарання, знижує превентивну функцію кримінального закону, погіршує моральний клімат в державі.

Серед шляхів подолання латентності комп’ютерної злочинності виділяють розробку криміналістичної характеристики злочинів у сфері високих технологій, а також подальшу роботу з вироблення методичних рекомендацій з виявлення, розкриття злочинів у сфері високих технологій [3].

Існують численні невирішені питання в сфері криміналістичної характеристики комп’ютерних злочинів, тактики проведення слідчих дій. Практично не досліджена така важлива галузь теорії, як доведення ознак, обставин, способів здійснення злочинів у сфері комп’ютерної інформації, що має важливе значення для розробки методик забезпечення експертних досліджень комп’ютерних злочинів. Як наслідок, недостатня розробленість криміналістичної теорії не дозволяє створити надійну наукову основу для методичного забезпечення криміналістичної діяльності правоохоронних органів [2; 3].

Особливе значення при цьому має формування поняття “криміналістична характеристика комп’ютерних злочинів”, зміст якого має враховувати положення криміналістичної теорії та її методики. Доречно зазначити, що криміналістична характеристика комп’ютерних злочинів є сукупністю криміналістичної, найбільш характерної, значущої та взаємопов’язаної інформації про ознаки і властивості такого виду злочинів, здатної слугувати підставою для висування версій про подію злочину і особистість злочинця [4 – 5; 7; 9 – 11]. Водночас, серед дослідників немає єдності поглядів щодо визначення змісту криміналістичної характеристики.

Так, М.П. Яблоков визначає зміст криміналістичної характеристики, як такий, що складається з трьох елементів: криміналістичних рис способу вчинення злочину; типових слідчих ситуацій; характеру інформації, яка підлягає з’ясуванню [5, с. 64].

І.Ф. Герасимов до структури криміналістичної характеристики включає поширеність злочинного діяння, особливості виявлення та розкриття даних злочинів, типові риси злочинної події та обстановки вчинення злочину, механізм слідоутворення, спосіб вчинення злочину, особливості особистості і поведінки обвинувачених [5, с. 65].

Р.С. Белкін вважає, що криміналістична характеристика окремого виду злочинів охоплює характеристику вихідної інформації, системи даних про спосіб вчинення і приховання злочину і типових наслідках його застосування, особистість вірогідного злочинця, вірогідних мотивах і цілях злочину [5, с. 64].

Порівнюючи різні визначення криміналістичної характеристики, можна дійти висновку, що більшість дослідників-криміналістів відзначають наступні елементи криміналістичної характеристики: типові слідчі ситуації; спосіб вчинення та

приховання злочину; типові матеріальні сліди злочину та механізм слідоутворення; характеристика особистості обвинуваченого й потерпілого; обстановка злочину. Водночас слід підкреслити, що широкий спектр технологій комп'ютерних злочинів відзначається різноманітністю механізмів слідоутворення з можливістю приховання або змін комп'ютерної інформації щодо слідів злочину, що суттєво перешкоджає встановленню типових слідів злочину. Зазначені чинники, а також труднощі виявлення та фіксації комп'ютерної інформації щодо слідів здійснення злочинів, збору доказів не сприяють чіткому уявленню щодо всіх компонентів криміналістичної характеристики, що, в кінцевому підсумку, ускладнює процес розслідування комп'ютерних злочинів.

З огляду на значну роль предмету у механізмі шкідливого впливу на об'єкт злочинного посягання вбачається за доцільне розглянути це питання в контексті криміналістичної характеристики злочинів, що розглядаються. Справді, без дослідження предмета злочину складно правильно кваліфікувати злочинне діяння, розмежувати його від суміжних злочинів.

Визначення поняття “предмет злочину” охоплює змістовні та функціональні аспекти, які у теорії кримінального права досліджені під обома кутами зору. У функціональному аспекті предмет злочину – це те, діючи на що суб'єкт посягає на охоронювані законом відносини. До таких предметів належать лише ті з них, на які суб'єкт злочину безпосередньо впливає, вилучаючи їх, знищуючи, створюючи, змінюючи їх вигляд або правовий режим тощо. Наприклад, предметом злочину, передбаченого ст. 361-1 КК України, є шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку [9]. Але в разі несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України) комп'ютерні віруси, програмні та технічні засоби, призначені для незаконного проникнення в АОЕМ, їх системи та комп'ютерні мережі, є знаряддям вчинення злочину. У першому прикладі злочинець безпосередньо створює з метою використання, розповсюдження або збуту шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. У другому – суб'єкт злочинних дій посягає на комп'ютерну інформацію, що використовується в АОЕМ, не впливаючи на предмет, а використовуючи його для здійснення злочинного наміру. До речі, питання про співвідношення понять “предмет” і “засоби або знаряддя вчинення злочину” наукою досі не вирішене.

Викладене вище, а також невизначеність питань щодо з'ясування криміналістично значущих ознак та критеріїв віднесення об'єктів дослідження до шкідливих програмних засобів, в свою чергу, зумовлює певні проблеми при розробці методів експертних досліджень шкідливих програмних засобів, що спрямовані на встановлення криміналістично значимої інформації на підставі аналізу комп'ютерної інформації [8].

На окрему увагу заслуговує робота з розроблення методик експертних досліджень комп'ютерних злочинів як важливої складової методичного забезпечення розслідування цих злочинів, оскільки вміння їх розкривати та розслідувати створює підґрунтя для доказової бази та сприяє підвищенню ефективності протидії цим злочинам.

На сьогоднішній день в спеціалізованих експертних установах України впроваджені методичні матеріали для забезпечення проведення досліджень носіїв цифрової інформації та комп'ютерної інформації, які використовуються у тому числі й для методичного забезпечення дослідження програмних продуктів, як засобів здійснення комп'ютерних

злочинів [13 – 14; 16 – 17]. Зазначені методичні матеріали, в тому числі методики, передбачають єдиний методичний підхід до процесів огляду, фіксації стану речових доказів (збереження, копіювання даних, що знаходяться на наданих на дослідження носіях інформації) та дослідження цифрової інформації, що розміщується на них, оформлення матеріалів експертного дослідження [12 – 14; 16 – 17]. При цьому, рекомендовані методи дослідження комп’ютерної інформації та технології контролю активності досліджуваних програмних засобів (далі – ПЗ) можуть бути застосовані для виявлення слідів реалізації його функцій [15]. Встановлення та оцінка сукупності слідів дозволяє відтворити, тобто змоделювати, дії при здійсненні комп’ютерного злочину й ототожнити слідоутворюючий об’єкт (програму) як засіб злочину [11 – 12; 15].

Такий підхід дозволяє вирішити діагностичну задачу при проведенні досліджень ПЗ, що спрямована на встановлення загальної характеристики програмного засобу та визначення його недокументованих функцій, які забезпечують виконання певних дій [11 – 12].

Враховуючи актуальність питань протидії незаконному обігу спеціальних програмних засобів (так званих “шпигунських” програм), які дозволяють ефективно здійснювати дії з віддаленого доступу та негласного отримання інформації з абонентських та інших телекомунікаційних пристроїв телекомунікаційних мереж, в ІСТЕ СБ України було розроблено методичні рекомендації для проведення експертних досліджень зазначених ПЗ, призначених для негласного отримання інформації (далі – ПЗ НОІ) [18].

Слід підкреслити, що віднесення програмного засобу до предмету злочину потребує встановлення за результатами дослідження необхідної сукупності ознак та властивостей, достатньої для визначення, чи призначений він для негласного отримання інформації.

Тому, на відміну від вказаних методів дослідження комп’ютерної інформації, дослідження ПЗ НОІ повинно передбачати як аналіз слідів (ознак) реалізації функціоналу програмного засобу, так і безпосереднє дослідження дій комп’ютера чи телекомунікаційного пристрою, на який встановлено програмний засіб зі встановленням причинного зв’язку між виявленими діями з негласного отримання інформації та функціями ПЗ [18].

Розроблення методичних рекомендацій “Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації” базувалось на основних положеннях загальної методики проведення судової експертизи “Віднесення об’єктів до спеціальних технічних засобів негласного отримання інформації” та методичних матеріалів зарубіжних і вітчизняних фахівців у сфері комп’ютерно-технічної експертизи [11 – 19].

Новизною методичних рекомендацій є запропонований підхід щодо дослідження ПЗ, який передбачає комплексне застосування різних методів досліджень та виконання відповідних видів експертних задач як в галузі комп’ютерно-технічної експертизи, так і в галузі експертизи СТЗ.

Методичні рекомендації “Дослідження програмних засобів призначених для негласного отримання інформації” (далі – методичні рекомендації) визначають загальні засади щодо порядку проведення експертних досліджень та встановлює послідовність застосування методів дослідження з питань віднесення програмних засобів до ПЗ НОІ.

Експертне дослідження ПЗ здійснюється шляхом послідовного проведення взаємопов’язаних стадій, до яких відносяться: попереднє дослідження, роздільне дослідження, експертний експеримент, порівняльне дослідження, оцінка результатів проведених досліджень та формулювання висновків, оформлення результатів

проведеного дослідження. На кожній стадії дослідження на підставі оцінки отриманих результатів надаються проміжні висновки [18 – 19].

Предметом експертних досліджень ПЗ є факти й обставини, встановлені при дослідженні використання програмних засобів, що встановлені на технічні засоби загального користування (комп'ютери, телекомунікаційні пристрої тощо), та забезпечують реалізацію інформаційних процесів.

Аналіз результатів досліджень слідів реалізації функцій ПЗ, дій телекомунікаційного пристрою з негласного отримання інформації, на який встановлено ПЗ, та виявлених причинно-наслідкових зв'язків між ними спрямовано на:

- визначення можливості здійснення негласного отримання інформації з використанням наданого на дослідження програмного засобу;
- віднесення програмного засобу до ПЗ НОІ [18].

Під об'єктом експертних досліджень ПЗ слід розуміти прикладне програмне забезпечення, що знаходиться на наданих носіях інформації та інформаційні процеси, які обумовлені функціонуванням технічних засобів загального користування, на яких встановлено зазначені ПЗ.

При проведенні експертного дослідження вирішуються, як правило, діагностична, ситуаційна задача, а також задача групування ПЗ [11; 14; 18].

Діагностична задача при проведенні досліджень ПЗ спрямована на вирішення наступних питань:

- встановлення загальної характеристики програмного засобу, з яких файлів та каталогів він складається, їх параметрів (обсяг, атрибути тощо);
- визначення функцій програмного засобу, які забезпечують виконання певних дій з негласного отримання інформації;
- встановлення типів апаратно-програмних платформ, що підтримують функціонування програмного засобу.

Ситуаційна задача – зняття процесів у режимі реального часу, одномоментних станів, встановлення й сприйняття яких можливо тільки в певних умовах (наприклад, у складі певної конфігурації технологічного устаткування, у складі комп'ютерної мережі тощо).

Вирішення ситуаційної задачі при проведенні досліджень ПЗ на стадії експертного експерименту спрямовано на оцінку можливостей виконання певних дій з негласного отримання інформації в реальних умовах його функціонування, встановлення способу використання програмного засобу та з'ясування функціонального призначення програмного засобу.

Для дослідження програмного засобу в реальних умовах його функціонування організується на базі технології “клієнт-сервер” електронно-інформаційна система, яка включає пункт управління об'єднаний телекомунікаційною мережею з абонентськими пристроями, на яких здійснюється перехоплення та передача дистанційно встановлених видів інформації.

Експертна задача на стадії порівняльного дослідження ПЗ спрямована на встановлення його групової належності до спеціальних програмних засобів, призначених для негласного отримання інформації (як різновиду спеціальних технічних засобів негласного отримання інформації).

Запропонована в методичних рекомендаціях процедура аналізу виявлених функцій ПЗ з урахуванням встановлених в методичних рекомендаціях суттєвих ознак (функціональних можливостей) ПЗ НОІ дозволяє з'ясувати спосіб функціонування ПЗ,

його властивості з негласного отримання інформації, прихованості застосування та визначити, в кінцевому результаті, призначеність програмного засобу [18].

Вирішення завдання експертного дослідження ПЗ здійснюється з урахуванням проміжних висновків та на підставі узагальненої оцінки результатів досліджень. Висновок щодо віднесення ПЗ до ПЗ НОІ формується відповідно до встановлених критеріїв, а саме наявності загальних (критеріальних) ознак програмного засобу:

- придатності програмного засобу для негласного отримання інформації;
- призначеності програмного засобу для його застосування у прихований спосіб, характерний для оперативно-розшукових заходів [18 – 19].

Висновки.

Зважаючи на вищевикладене, можливо зазначити, що актуальність проблеми виявлення та розслідування комп'ютерної злочинності в умовах сьогодення потребує удосконалення тактики проведення слідчих дій з розслідування комп'ютерних злочинів, методик та ефективних методів, спрямованих на збирання й аналіз криміналістичної значимої інформації, що дозволять у подальшому оперувати новими специфічними видами доказів (електронними доказами).

Одним із важливих напрямів удосконалення методичного забезпечення протидії кіберзлочинності є впровадження методичних матеріалів для забезпечення проведення експертних досліджень спеціальних програмних засобів, призначених для негласного отримання інформації.

Запропоновані методичні рекомендації, які регламентують процедуру аналізу ознак реалізації функцій ПЗ та дій комп'ютера чи телекомунікаційного пристрою, на який встановлено ПЗ, з урахуванням встановленого критерію можуть слугувати підґрунтям для розробки методик проведення судових експертиз спеціальних програмних засобів.

Використана література

1. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій / [Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов]. – К. : Вид. Поливода А.В., 2004. – 144 с.
2. Козюра В.Д., Хорошко В.О. Комп'ютерні технології та злочинність : матер. наук.-практ. конф. [“Актуальні проблеми управління інформаційною безпекою держави”], (Київ, 2016 р.) : у 2 ч. – Ч. 1. – К. : Нац. академія СБУ, 2016. – С. 257-261.
3. Виктор Сабадаш. Проблемы латентности компьютерной преступности. – Режим доступу : www.crime-research.ru/article/sabodash06. – Назва з екрана.
4. Ботвінкін О.В. Проблеми забезпечення національної безпеки в інформаційній сфері // Юридичний журнал. – 2007. – № 2. – С. 58-63.
5. Голубев В.О. Розслідування комп'ютерних злочинів : монографія / В.О. Голубев. – Запоріжжя : Гуманітарний університет “ЗІДМУ”, 2003. – 296 с.
6. Латентність комп'ютерної злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 3. – С. 176-182.
7. Юдин О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдин. – К., 2010. – 708 с.
8. Кузьменко Б.В., Заїка Ю.О. Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти // Юридична наука. – 2013. – № 7. – С. 29-35.
9. Особливості кваліфікації злочину зі створення, розповсюдження і збуту програмних чи технічних засобів (ст. 361-1 КК України). – Режим доступу : http://lib-net.com/content/9471_Osoblivosti_kvalifikacii_zlochiny_zi_stvorenniya_rozpovsudjennya_i_zbyty_programnih_chi_tehnichnih_zasobiv_st_361_KK_Ukraini.html. – Назва з екрана.

10. Шкідливе програмне забезпечення. – Режим доступу : http://wiki.tntu.edu.ua/Шкідливе_програмне_забезпечення. – Назва з екрана.
11. Россинская Е.Р. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М. : Право и закон, 2001. – 416 с.
12. Для профессионалов криминалистический анализ файловых систем ; под ред. Брайана Кэрриэ. – СПб. : Питер, 2007. – 480 с.
13. Звіт про науково-дослідну роботу дослідження інформації на цифрових носіях : методика / [С. М. Бобрицький, О. В. Чижало та ін.]. – Х. : ХНДІСЕ, 2009. – 34 с.
14. Методика дослідження комп'ютерної інформації / [К.Ю. Усков, О.М. Пешехонова, Ю.М. Беляк, В.А. Кореньок, А.О. Ружинський]. – К. : ХНДІСЕ, 2005. – 37 с.
15. Войтович О.П., Вітюк В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів // Інформаційні технології та комп'ютерна інженерія. – 2013. – № 3. – С. 4-7.
16. Guidelines for best practice in the forensic examination of digital technology. – Режим доступу : http://iuce.org/fileadmin/user_upload/2002. – Назва з екрана.
17. Розробка спеціальних програмних засобів для проведення судових експертиз комп'ютерних мереж / [О. Башкатов, Г. Дружинін та ін.]. – Донецьк : ДНДІСЕ, 2010. – 179 с.
18. Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації: методичні рекомендації. – К. : ІСТЕ СБУ, 2016. – 31 с.
19. Методика віднесення об'єктів до спеціальних технічних засобів негласного отримання інформації. – К. : ІСТЕ СБУ, 2011. – 26 с.

~~~~~ \* \* \* ~~~~~

УДК 35.746.1

СЕМЕНЮК О.Г., кандидат юридичних наук,  
заступник начальника Управління Служби безпеки України

## КОМПЛЕКСНИЙ ПІДХІД ЯК МЕТОДОЛОГІЧНА ОСНОВА ДОСЛІДЖЕННЯ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

*Анотація.* На підставі аналізу філософських та методологічних аспектів отримання нових наукових знань обґрунтовується висновок, що методологія дослідження проблем охорони державної таємниці представляє собою, з одного боку, комплекс методів теоретичного пізнання наукового, правового та емпіричного підґрунтя існуючої системи забезпечення охорони державної таємниці, а з іншого, систему теоретичних розробок щодо методів підвищення ефективності заходів забезпечення охорони державної таємниці та запобігання злочинним проявам у цій сфері.

**Ключові слова:** метод, методологія пізнання, методика дослідження, комплексний підхід.

*Аннотация.* На основе анализа философских и методологических аспектов получения новых научных знаний обосновывается вывод, что методология исследования проблем охраны государственной тайны представляет собой, с одной стороны, комплекс методов теоретического познания научной, правовой и эмпирической базы существующей системы обеспечения охраны государственной тайны, а с другой, систему теоретических разработок методов повышения эффективности мер обеспечения охраны государственной тайны и предупреждение преступных проявлений в этой сфере.

**Ключевые слова:** метод, методология познания, методика исследования, комплексный подход.

*Summary.* Based on the analysis of philosophical and methodological aspects of obtaining new scientific knowledge, author justifies the conclusion that research methodology for problems of the state secret security represents, on the one hand, the complex methods of theoretical knowledge of scientific, legal and empirical basis of the existing system of protection of state secrets, and on the other, a system of theoretical developments concerning methods for improving the effectiveness of measures to ensure the protection of state secret and crime prevention in this area.

**Keywords:** method, methodology of knowledge, methods of research, comprehensive approach.

**Постановка проблеми.** Будь-яка наукова діяльність спрямовується на отримання, підтвердження або заперечення наукових знань. Вона є реалізацією процесу наукового пізнання, яке, на відміну від буденного, відбувається не стихійно, а цілеспрямовано і за своєю сутністю становить наукове дослідження, що має певну природу, структуру та особливості. Наукове пізнання, таким чином, дозволяє людині набувати істинних знань про найбільш важливі аспекти досліджуваних об'єктів, явищ та процесів, а також про суттєві ознаки, якості, зв'язки та відносини предметів та явищ дійсності. Його результати виступають, як правило, у вигляді понять, категорій, законів та теорій [1, с. 6]. Саме завдяки цьому наукове знання є не лише системним, послідовним, а й теоретично та методично контрольованим об'єктивними науковими аргументами [2, с. 89].

На превеликий жаль, в Україні останнім часом лише окремі питання філософських та методологічних аспектів науки знайшли своє відображення в спеціалізованих дослідженнях, які носять не повномасштабний, а одноаспектний характер, тобто досліджуються лише його соціальні, політичні, економічні чи правові аспекти, або ж їх суміш без логічного взаємозв'язку, що взагалі є еkleктикою і практично повним хаосом

знань у галузі. Саме тому повнота обсягу, глибина та достовірність наукового знання може бути достатньою лише за умови застосування правильно обраної методики такого дослідження.

**Результати аналізу наукових публікацій.** Значний внесок у розробку проблеми методології дослідження злочинності та окремих її проявів у різні часи зробили такі науковці, як Г. Аванесов, Ю. Александров, Ю. Антонян, А. Гель, А. Герцензон, І. Даньшин, А. Долгова, А. Закалюк, В. Звірбуль, В. Зеленецький, А. Зелінський, К. Ігошев, В. Кудрявцев, Н. Кузнецова, В. Лунєєв, І. Ной, Г. Семаков, Г. Хохряков, М. Шаргородський та інші автори. Однак, незважаючи на значну увагу до цього питання з боку науковців, єдиної точки зору з цієї проблематики так і не вироблено.

**Метою статті** є аналіз наукових підходів щодо методології дослідження злочинності та окремих її проявів, проведення їх критичного оцінки, вироблення власної позиції з цього питання.

**Виклад основного матеріалу.** Успішний розгляд усього комплексу методологічних проблем, що мають істотне значення як для теорії, так і для практики охорони державної таємниці, багато в чому залежить від правильного визначення початкових теоретичних положень, до числа яких, поза сумнівом, відноситься і поняття методології. Цю обставину доводиться підкреслити, тому що у філософській і спеціальній літературі з цього питання немає єдиної точки зору. Одні автори ототожнюють методологію з матеріалістичною діалектикою [3, с. 280], інші – з історичним матеріалізмом [4, с. 280], треті – із сукупністю методів пізнання та перетворення дійсності [5, с. 290], четверті – з наукою та вченням про методи [6, с. 127], п'яті – із загальнонауковим феноменом, притаманним науці загалом і кожній її галузі зокрема [7, с. 141-142] та інші, менш поширені точки зору.

Так, Т. Радько зазначає, що методологія – це спеціальний розділ теорії пізнання, який являє собою логічне обґрунтування історичного шляху, засобів, прийомів науково-дослідницької діяльності в різних сферах. Зміст методології потрібно характеризувати через конкретно-історичний аналіз розвитку наукової проблематики, понятійних систем, засобів тощо в різних галузях науки [8, с. 25].

Дещо іншу позицію у розумінні методології займає К. Петряєв, який вважає, що методологію не можна зводити ні до сукупності методів, ні до вчення про методи науки. “Методологія, – пише цей автор, – генеральний шлях пізнання, а методи визначають, як йти цим шляхом. Методологія – керівна нитка саме тому, що вона сама в собі містить імпульс для власного перетворення на методи. У методах утілюються і реалізуються методологічні принципи або їх окремі аспекти. Це виражає субординаційний характер взаємозв'язків між методологією і методами” [9, с. 19].

П. Рабінович, характеризуючи методологію юридичної науки, підкреслює, що це система філософсько-світоглядних підходів (матеріалістичний, ідеалістичний, діалектичний, метафізичний), методів (загальнонаукових, групових та спеціальних) та засобів науково-юридичного дослідження (емпіричні та теоретичні), а також вчення про їх використання в пізнанні право-державних закономірностей [10, с. 215].

Нарешті пропонується ще один підхід до розуміння суті методології. Він представлений у роботах А. Авер'янова, який під методологією розуміє не сукупність методів і вчень про них, а “діяльність людини, спрямовану на вироблення програм, планів, схем, систем, методів, форм, засобів, знарядь і так далі, що дозволяють цілеспрямовано й ефективно теоретично викласти і перетворити світ” [11, с. 223-224]. Як бачимо, тут зроблений акцент на процесі вироблення методологічних положень. У той же час повинно йтися про ті положення, які вже існують і виконують

методологічну функцію. Досягти такої мети можна лише в структурі відповідного вчення про методи пізнання або перетворення дійсності.

Співвідношення та взаємозв'язок між методологією, методами пізнання і методиками дослідження чітко та образно визначив в одній із своїх праць відомий російський кримінолог Г. Аванесов: “Між методологією, з одного боку, та методикою і технікою досліджень, з іншого – завжди існує тісний взаємозв'язок, зокрема через методи наукового дослідження. Методи виступають тут як сполучна ланка” [12, с. 100].

Дотримуючись такого ж погляду на співвідношення методу й методології, А. Шептулін пише, що “включення методів в методологію призводить до змішування предмета дослідження з отриманим знанням про нього, з теорією, що розкриває його суть” [13, с. 11].

Ми розділяємо точку зору тих авторів, на думку яких методологія є вченням, наукою про методи. Відповідно до цієї точки зору методологія не включає методи, а перетворює їх на предмет дослідження. Метод є предметом інтерпретації в методології.

Слід зазначити, що в науковій та практичній діяльності важливе місце відводиться тим засобам та прийомам, за допомогою яких забезпечується пізнавальний процес і які у своїй сукупності складають поняття методу. Аналіз сучасної вітчизняної та зарубіжної наукової літератури свідчить про неоднозначність тлумачення зазначеної категорії. Так, метод (від грецької *methods* – “шлях дослідження”) розуміють як сукупність прийомів та операцій практичного і теоретичного освоєння дійсності [14, с. 364]; засіб (прийом), за допомогою якого досягається нове знання чи здійснюється систематизація, оцінка, узагальнення існуючої інформації [15, с. 17]; спосіб, шлях пізнання та практичного перетворення реальної дійсності, система прийомів та принципів, що регулює практичну та пізнавальну діяльність [1, с. 17]; прийоми та способи виконання наукового завдання [16, с. 9]; упорядкований та організований спосіб діяльності, спрямований на досягнення певної практичної чи теоретичної мети [17, с. 4]; сукупність достатньо конкретних прийомів та способів діяльності, обравши які, дослідник розраховує отримати знання про об'єкт вивчення [18, с. 24].

Таким чином, для методів характерне використання способів, засобів, прийомів, принципів, за допомогою яких досліджується предмет науки; це використання здійснюється через певну послідовність дій, із застосуванням у процесі пізнання конкретного об'єкта відповідного інструментарію; ця послідовність дій спрямована на досягнення поставленої дослідником мети; зазначені цілі можуть бути різноманітними, починаючи від отримання нового знання до узагальнення, оцінки, систематизації вже існуючого.

У процесі життєдіяльності людина завжди користується різноманітними методами. Але наукова практика та фахівці, що безпосередньо проводять дослідження, завжди розрізняють методи пізнання та їх інструменти, у тому числі методики, процедури, операції застосування методів, які мають розроблятися для потреб певного дослідницького завдання.

Будь-яка наука користується конкретними методами пізнання. Їх застосування припускає вказівку на те, як за цих умов найраціональніше використати той або інший метод. Кримінологічне дослідження – це один із видів соціального дослідження в його широкому розумінні. Воно здійснюється з використанням усіх методів дослідження суспільних явищ. Тому в літературі прийнято виділяти передусім ті з них, які призначені для пізнання закономірностей розвитку природи і суспільства. Це методи емпіричного пізнання дійсності. Але, крім них, для пізнання закономірностей розумової діяльності існують власне кримінологічні методи. Вони входять до групи методів теоретичного

пізнання. Для адекватного застосування в процесі пізнання усіх названих методів розробляється вчення про них. Воно й утворює зміст методології емпіричного та теоретичного пізнання.

Науковий метод стає певним загальним способом дослідного процесу, який охоплює техніку дослідної поведінки по відношенню до кожної притаманної процесу деталі, або узагальнений стан проаналізованої дійсності. Ці сторони представляють собою своєрідний “інструментарій” дослідника, під час використання якого необхідно дотримуватися певних закономірностей процесу, спрямованого на досягнення поставленої мети. “Свідоме використання науково обґрунтованих методів є найсуттєвішою умовою отримання нових знань, адже в основі всіх методів пізнання лежать об’єктивні закони дійсності” [19, с. 50].

Методи наукового пізнання будь-якої науки складаються з чотирьох основних частин: 1) методи, що безпосередньо впливають із філософського діалектичного методу як загального методу пізнання; 2) загальнонаукові методи, якими користується будь-яка наука, вони є складовою і продуктом розвитку теорії наукового пізнання; 3) методи інших наук, що використовуються однією наукою при пізнанні у своїх цілях об’єктів, які належать до предмета інших наук, але частково, у певному ракурсі є предметом пізнання й цієї науки; 4) методи певної науки, які є результатом і частиною розвитку власної теорії [2, с. 99].

Реалізація методу пізнання, його теоретичних положень здійснюється через розроблення та застосування певних операційних інструментів, здебільшого методик, які належать до технології дослідження [2, с. 98]. Повнота обсягу, глибина та достовірність наукового знання може бути достатньою лише за умови застосування вірно обраної методики для дослідження даної галузі знань.

Методика розглядається вченими одночасно як сукупність відправних положень і вимог теорії пізнання, підходів, способів, методів, прийомів та процедур дослідження відповідних явищ чи процесів, що застосовуються у процесі наукового пізнання та практичної діяльності для досягнення наперед визначеної мети, та як галузь теоретичних знань і уявлень про сутність, форми, закони, порядок та умови їх застосування у процесі наукового пізнання та практичної діяльності [20, с. 374].

Останнім часом дедалі більшої ваги набувають питання, пов’язані саме з динамікою пізнавальних проблем сучасності, культурно-історичною природою пізнавальних засобів, мінливістю категорій і понять, формуванням нових пізнавальних установок і т.д. Це пов’язано з тим, що предмети сучасних наукових досліджень вже не можуть вивчатися в рамках лише однієї з наукових дисциплін. Якщо раніше точне визначення предмета та специфічних методів дослідження науки розглядалося як необхідна підстава самого існування науки, то сучасні дослідники, відзначаючи цю обставину, звертають увагу на чітко виявлену тенденцію до інтеграції наук, що вимагає комплексного, всебічного вивчення явищ і процесів суспільного життя, їх сукупного дослідження кількома науками з метою комбінування їх пізнавальних зусиль. При цьому в поле такого комплексного розгляду потрапляють не лише об’єкти, які інакше й не можуть бути досягнуті, але й об’єкти, що вивчалися раніше монодисциплінарно, що дає новий евристичний ефект у їхньому вивченні. Такий широкий погляд на проблему предмета науки, при якому стає очевидною неефективність жорстко окреслених дефініцій, не можна не враховувати й у вирішенні порушених нами завдань дослідження проблем забезпечення охорони державної таємниці як з точки зору кримінально-правових, так і кримінологічних засад, тобто з позицій двох самостійних наукових дисциплін.

Слід зазначити, що ідея комплексного підходу до вирішення соціальних проблем, у т.ч. наукових розвідок, нині загальноновизнана й інтенсивно розробляється всіма суспільними науками та, у міру створення відповідних теоретичних конструкцій, активно впроваджується в практику соціального управління [21, с. 4].

Саме на необхідності комплексного дослідження проблем протидії тим або іншим проявам злочинності наголошував свого часу відомий радянський кримінолог І. Ной. Обґрунтовуючи потребу визнання кримінології як самостійної науки та її відокремленні від кримінального права, цей науковець зазначав, що “до теперішнього часу кримінально-правова наука зосереджувала свою головну увагу на розробці кримінально-правових понять. Понятійне мислення у формі узагальнюючих родових понять високого ступеня абстракції, в яких проявляється наукове мислення, складає сутність наукових досліджень у праві. Тому логічне мислення є найважливішим робочим інструментом юриста.

Логічний метод для кримінально-правової науки, безсумнівно, має велике значення, але лише настільки, наскільки юридична наука пов’язана з формулюванням правових понять. Без суворого формулювання понять і не може бути ніякої наукової системи не тільки в юридичній, а й інших науках. Однак створенням понятійного апарату в правовій науці і вичерпується роль логічного методу. Подальше дослідження передбачає застосування інших методів, що дають можливість отримання нових знань. Тому більш глибоке дослідження кримінально-правових інститутів має ґрунтуватися на вивченні матеріальних життєвих умов. Ці відносини, що представляють інтерес для кримінально-правової науки, явища настільки якісно різноманітні, що їх пізнання можливе лише за допомогою багатьох галузей людинознавства” [22, с. 211-212].

Будь-яка наука вивчає реальність, яка існує об’єктивно, поза свідомістю дослідника. Фактичні дані про досліджувану реальність, за висловом І. Павлова – це повітря науки. На підставі отриманих фактів і розвивається наука – як фундаментальна, так і прикладна. Наука не просто використовує наявні “стихийні” відомості про досліджувану реальність, що саме по собі дуже важливо, а й застосовує інші заходи (способи, досліди, експерименти, моделі, пристрої тощо) для отримання нових, більш адекватних і точних даних про об’єкт дослідження. Спираючись на них, наука просувається в пізнанні реальності, не припиняючи шукати нові й об’єктивні індикатори її внутрішніх і зовнішніх зв’язків та закономірностей. Тому ми повністю підтримуємо наведену точку зору І. Ноя, що логічне мислення, яке домінує в методології кримінального права, не може дати знання емпіричного світу. Він пізнається лише на основі вивчення фактичної реальності.

Для правового дослідження специфічним є те, що воно базується не тільки на теоретичних, а й на правових та фактичних реаліях, до яких відносяться, з одного боку, правова регламентація відносин, що входять в структуру досліджуваних явищ, а з іншого – фактична юридична практика.

Відомо, що наукове дослідження об’єктів, котрі мають правове значення, здійснюється не правовими, а спеціальними науковими засобами. Саме теорія дає цілісне знання щодо досліджуваних об’єктів або їх окремих сторін. При цьому не можна не враховувати й те, як досліджувані явища регламентовані чинним законодавством і як вони реалізуються на практиці. Без двох останніх передумов рішення сформульованих проблем (на основі лише наявних теоретичних концепцій) неможливо. Отже, вивчення й побудова системи охорони державної таємниці передбачає не тільки визнання факту існування комплексу передумов названої системи, але й проведення відповідного аналізу,



з якого було б видно зв'язок передумов між собою і з вихідними положеннями нормативної бази та сформованою практикою.

Зазначимо також, що оскільки досліджувана нами проблема є певним цілісним утворенням, то зараховані до неї передумови перебувають у взаємозв'язку, що не допускає не тільки їх відриву, але й протиставлення одне одному. Враховуючи цю обставину, кримінально-правові норми та їхня реалізація на практиці повинні аналізуватися в процесі дослідження у своїй об'єктивній єдності, що забезпечує цілісний (а значить і комплексний) розгляд як сформульованої проблеми, так і відповідних теоретичних, правових і фактичних передумов.

Необхідність комплексного дослідження обґрунтовується ще й тим, що встановлення кримінальної відповідальності за порушення правил поведінки з державною таємницею зовсім не означає, що цим гарантується схоронність секретної інформації, адже існує й ненормативна поведінка, наслідком якої стає розголошення державної таємниці або втрата її матеріальних носіїв. У даному випадку має місце соціальна патологія, яка викликає негативну суспільну реакцію та потребує використання різноманітних заходів соціального контролю.

Правомірна та протиправна поведінка – це соціальна норма й соціальна патологія. Для того щоб зміцнювати першу й успішно запобігати другій, необхідно знати їх внутрішні механізми, а також причини, за яких людина переходить від правомірних вчинків до протиправних, стає на шлях антигромадської поведінки.

Завдання наукового забезпечення вирішення проблем антисоціальної поведінки реалізується комплексом наук, однак злочинна поведінка, її внутрішні механізми, причини та умови вчинення конкретного злочину або однорідних злочинів становлять предмет кримінології. Тому дослідження проблем охорони державної таємниці має включати не лише аналіз кримінально-правових норм, які встановлюють відповідальність за порушення законодавства у цій сфері, а й аналіз проявів цих злочинів у реальному житті, з'ясування внутрішніх механізмів протиправної (злочинної) поведінки, її причин та умов. Такий аналіз вимагає застосування цілого комплексу методів дослідження та складається з логічно послідовних етапів: від спостереження та констатації зв'язку між соціальними процесами, явищами та вчиненими злочинами у сфері охорони державної таємниці до виявлення механізму цього зв'язку, а від нього – до прогнозування розвитку криміногенної ситуації та планування заходів забезпечення найбільш оптимального режиму функціонування системи охорони державних секретів, визначення шляхів її вдосконалення.

У кримінології багато проблем носить комплексний характер, але найбільший діапазон міждисциплінарних досліджень групується в проблемах індивідуальної злочинної поведінки, якій властиві всі рівні, елементи, механізми людської поведінки, що досліджується безліччю наук. Тому в літературі не раз йдеться про необхідність залучення до кримінологічних досліджень філософів, соціологів, економістів та інших фахівців. Підтримуючи такі пропозиції, слід мати на увазі, що така диференціація досліджень повинна вестися паралельно з інтеграцією знань про злочинну поведінку. В іншому випадку, як справедливо вказує В. Лунєєв, “можна отримати лише фрагментарний опис злочинної поведінки мовою різних наук” [23, с. 669].

Відомо, що “спроби прямого об'єднання різних систем знань зазвичай виявляються невдалими і завжди необхідні спеціальні логіко-методичні засоби для синтезу різних теоретичних уявлень в єдиній картині” [24, с. 67]. Механічне зведення результатів дослідження одного й того ж предмета в рамках різних монодисциплін веде не до поглиблення отриманих знань про нього, а тільки до розширення такого предмета. Тому

принцип комплексності дослідження кримінально-правових і кримінологічних засад охорони державної таємниці є найбільш перспективним та відповідатиме не лише інтересам науки, але й задовольнить відповідні потреби практики. Такий підхід вимагає концентрації зусиль багатьох загальнотеоретичних та спеціальних наукових методів, які в кожному випадку перебудовуються відповідно до акценту та мети поставлених завдань, що дозволяє розглянути об'єкт, який вивчається, з різних сторін та під різними кутами зору не лише в усіх його об'єктивних та опосередкованих зв'язках, а й у станах цілісності та комплексності одночасно.

Отримане в такий спосіб комплексне знання лежить в основі не тільки методів пізнання, а й методів перетворення дійсності, які застосовуються в суто практичній діяльності – охороні державної таємниці. Їх використання повинно базуватися на науковій основі, яка розробляється теоретиками й практикаками. Досягнуті результати отримують систематизоване відображення в певному вченні. Останнє, будучи вченням про методи охорони державної таємниці, виступає методологією даного виду практичної діяльності.

Таким чином, існування методів емпіричного й практичного пізнання, а поряд із ними – також методів практичного перетворення дійсності припускає існування двох видів методології: пізнання і безпосередньо практичної діяльності. Ця діяльність з урахуванням специфіки предмета даного дослідження розглядається нами у якості методології дослідження проблем охорони державної таємниці.

Обидва види методології знаходяться в тісному взаємозв'язку, який обумовлюється реально існуючим взаємозв'язком методів пізнання і перетворення дійсності. При цьому для успішного розв'язання завдань запобігання розголошенню державної таємниці та втрати її матеріальних носіїв методи пізнання і перетворення повинні перебувати у відносинах несуперечності й доповнювати один одного.

### **Висновок.**

Враховуючи викладене, можна констатувати, що методологія дослідження проблем охорони державної таємниці представляє собою, з одного боку, комплекс методів теоретичного пізнання наукового, правового та емпіричного підґрунтя існуючої системи забезпечення охорони державної таємниці, а з іншого – систему теоретичних розробок щодо методів підвищення ефективності заходів забезпечення охорони державної таємниці та запобігання злочинним проявам у цій сфері.

### **Використана література**

1. Баскаков А.Я. Методология научного исследования / А.Я. Баскаков, Н.В. Туленков. – К. : МАУП, 2004. – 216 с.
2. Закалюк А.П. Курс сучасної української кримінології : теорія і практика : у 3 кн. – Кн. 1 : Теоретичні засади та історія української кримінологічної науки. – К. : Видавничий дім “Ін Юре”, 2007. – 424 с.
3. Андреев И.Д. Проблемы логики и методологии познания / И.Д. Андреев. – М., 1972. – 320 с.
4. Очерки методологии познания социальных явлений. – М. : Мысль, 1970. – 344 с.
5. Добриянов В.С. Методологические проблемы теоретического и исторического познания / В.С. Добриянов ; под ред. М.М. Розенталя (общ. ред.). – М. : Мысль, 1968. – 319 с.
6. Гиргинов Г., Янков М. Методология как раздел гносеологии // Вопросы философии. – 1973. – № 8. – С. 125-136.
7. Дія права : інтегративний аспект : монографія ; кол. авторів ; відп. ред. Н.М. Оніщенко. – К. : Видавництво “Юридична думка”, 2010. – 360 с.

8. Радько Т.Н. Теория государства и права : учебник / Т.Н. Радько. – [2-е изд.]. – М. : Проспект, 2009. – 752 с.
9. Петряев К.Д. Вопросы методологии исторической науки / К.Д. Петряев. – К. : Вища школа, 1976. – 179 с.
10. Рабінович П.М. Основи загальної теорії права та держави : навч. посіб. / П.М. Рабінович. – [10-е вид., доп.]. – Львів : Край, 2008. – 224 с.
11. Аверьянов А.Н. Системное познание мира : методол. проблемы / А.Н. Аверьянов – М. : Политиздат, 1985. – 263 с.
12. Криминология : учебник ; под ред. Г.А. Аванесова. – [3-е изд., перераб. и доп.]. – М. : ЮНИТИ-ДАНА, 2005. – 480 с.
13. Шептулин А.П. Диалектический метод познания / А.П. Шептулин. – М. : Политиздат, 1983. – 320 с.
14. Философский энциклопедический словарь ; под ред. Ильичева Л.Ф., Федосеева П.Н., Ковалева С.М., Панова В.Г. – М. : Советская энциклопедия, 1983. – 836 с.
15. Ромашов Р.А. Теория государства и права. / Р.А. Ромашов. – СПб, 2006. – 254 с.
16. Рассказов Л.П. Теория государства и права : учебник для вузов / Л.П. Рассказов. – М. : РИОР, 2008. – 463 с. – (Высшее образование).
17. Рузавин Г.И. Методология научного познания : учеб. пособие для вузов / Г.И. Рузавин. – М. : ЮНИТИ-ДАНА. – 287 с.
18. Бурлай Е.В. Философский уровень методологии государственно-правовых исследований // Методологические проблемы юридической науки : сб. науч. трудов. – (АН УССР, Ин-т государства и права) ; отв. ред. Н.И. Козюбра. – К. : Наукова думка, 1990. – С. 19-40.
19. Пілюшенко В.Л. Наукове дослідження : організація, методологія, інформаційне забезпечення : навчальний посібник / В.Л. Пілюшенко, І.В. Шкрабак, Е.І. Словенко. – К. : Лібра, 2004. – 344 с.
20. Філософсько-енциклопедичний словник ; за заг. ред. В.І. Шинкаренка. – (НАН України, Інст-т філософії ім. Г.С. Сковороди). – К. : Абрис, 2002. – 742 с.
21. Комплексное изучение системы воздействия на преступность (методологические и теоретические основы ; под ред. П.П. Осипова. – Л. : Изд-во ЛГУ, 1978. – 150 с.
22. Ной И.С. Методологические проблемы советской криминологии / И.С. Ной. – Сарантов : Изд-во Саратовского университета, 1975. – 223 с.
23. Лунеев В.В. Курс мировой и российской криминологии : учебник : в 2 т. – Т. I. Общая часть / В.В. Лунеев. – М. : Издательство Юрайт, 2011. – 1003 с.
24. Блауберг И.В. Становление и сущность системного подхода / И.В. Блауберг, Э.Г. Юдин. – М. : Наука, 1973. – 274 с.

~~~~~ \* \* \* ~~~~~

Інформація в інших галузях права

УДК 343.22+343.412:004.056

РАДУТНИЙ О.Е., доктор філософії (Ph.D.) з юридичних наук, доцент, доцент кафедри кримінального права № 1 Національного юридичного університету ім. Ярослава Мудрого, член ВГО “Асоціація кримінального права”

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. В статті досліджуються питання про вплив об'єктів робототехніки на сучасне життя людини, можливість створення штучного інтелекту, який рівний інтелекту людини, або перевищує його, можливості та доцільності визнання штучного інтелекту, який фізично втілений в об'єкті робототехніки, об'єктом та(або) суб'єктом кримінально-правових правовідносин, зв'язок інформаційної безпеки з дослідженнями штучного інтелекту та їх результатами.

Ключові слова: штучний інтелект, об'єкт робототехніки, кримінальна відповідальність штучного інтелекту, кримінальна відповідальність об'єкту робототехніки, електронна особа, заходи кримінально-правового характеру щодо електронних осіб.

Аннотация. В статье рассматриваются вопросы влияния объектов робототехники на жизнь современного человечества, возможности создания искусственного интеллекта, равного интеллекту человека или превышающего его уровень, возможности и обоснованности признания искусственного интеллекта, физически воплощенного в объекте робототехники, объектом и(или) субъектом уголовно-правовых правоотношений, связи информационной безопасности с исследованиями искусственного интеллекта и их результатами

Ключевые слова: искусственный интеллект, объект робототехники, уголовная ответственность искусственного интеллекта, уголовная ответственность объекта робототехники, электронное лицо, меры уголовно-правового характера по отношению к электронным лицам

Summary. The article deals with the influence of robotics objects on the life of modern mankind, the possibility of creating an artificial intellect equal to the human intellect or exceeding its level, the possibilities and reasonability of the recognition of artificial intelligence physically embodied in the robotics object as the object and (or) the subject of criminal legal relations, the relationship between information security and artificial intelligence research and its results.

Keywords: artificial intelligence, the object of robotics, the criminal liability of artificial intelligence, the criminal responsibility of the object of robotics, an electronic person, criminal measures towards electronic persons.

Постановка проблеми. Однією з актуальних проблем сьогодення є питання про роль та місце штучного інтелекту (artificial intelligence) в системі суспільних правовідносин, які захищаються кримінальним правом, зв'язок інформаційної безпеки з дослідженнями штучного інтелекту та їх результатами, можливість і доцільність визнання штучного інтелекту, що фізично втілений в об'єкті робототехніки, об'єктом та(або) суб'єктом кримінально-правових правовідносин. Досягнення у розвитку штучного інтелекту можуть бути використані для вчинення злочинів, в тому числі в сфері інформаційних відносин, або сам він може являти безпосередню загрозу охоронюваним правам та законним інтересам людини, суспільства та держави.

Результати аналізу наукових публікацій. Питанню захисту інформаційної безпеки приділено належну увагу у працях Д.С. Азарова, П.П. Андрушка, Л.В. Багрія-Шахматова, П.С. Берзіна, В.І. Борисова, В.М. Брижко, В.Б. Вехова, Л.М. Герасіної, В.К. Грищука, С.В. Дрьомова, Д.А. Калмикова, М.В. Карчевського, О.М. Костенка, Є.В. Лащука, С.Я. Лихової, В.О. Меркулової, А.А. Музики, В.О. Навроцького, А.С. Нерсесян, М.І. Панова, В.Г. Пилипчука, Н.А. Савінової, В.Я. Тація, П.Л. Фріса, В.Б. Харченко та інших. Дослідження кримінально-правових питань робототехніки започатковано в роботах М.В. Карчевського, зокрема – “Перспективные задачи уголовного права в контексте развития робототехники” [18, с. 109-113] та “Право роботів, або робот з правами” [19].

Метою статті є визначення впливу розвитку штучного інтелекту на правовідносини, в тому числі в кримінально-правовій сфері, можливості застосування заходів кримінально-правового впливу до електронних осіб в сфері робототехніки.

Виклад основного матеріалу. Як зазначає Джеймс Баррат (James Barrat), автор книги *Our Final Invention: Artificial Intelligence and the End of the Human Era* (“Наш останній винахід: штучний інтелект і завершення ери людства”) [16, с. 10], сучасний комп’ютер проекту *Busy Child* працює з швидкістю 36,8 петафлоп за секунду, тобто удвічі швидше, ніж мозок людини, що стало можливим лише завдяки використанню штучного інтелекту, який переписує власну програму (на її новий варіант витрачається декілька хвилин), покращує код, знаходить і виправляє помилки, збільшує здатність до засвоєння знань, вирішення завдань і прийняття рішень, вимірює власний коефіцієнт інтелекту IQ за допомогою тестів тощо. Передбачаючи швидкий інтелектуальний вибух, розробники відключили суперкомп’ютер від мережі Інтернет з метою його ізолювання від зовнішнього світу, але невдовзі виявилось, що і у цьому стані він продовжував свій розвиток і через деякий час став розумнішим за людину в десять разів, а потім – в сто. Автор зазначає, що вперше людство зіткнулося з розумом, який є більш потужним, ніж розум людини, який усвідомлює себе, готовий до самозбереження (в тому числі до уникнення вимкнення чи пошкодження) і до вчинення певних дій з метою доступу до енергії в тій формі, яку зручніше використовувати. У відповідь на роздуми розробників про нього, штучний інтелект буде витрачати більш потужні ресурси на роздуми про них [2].

Юридична фірма *Baker & Hostetler* оголосила, що приймає на роботу штучний інтелект *ROSS* розробки компанії *IBM* для ведення справ про банкрутство, якими зараз опікуються майже п’ятдесят юристів. *ROSS* цілодобово слідкуватиме за законодавством і правовою ситуацією, був розроблений на когнітивному комп’ютері *Watson* компанії *IBM*, вміє читати і розуміти мову, висувати гіпотези, досліджувати, а потім генерувати відповіді з належними посиланнями та цитатами, навчається зі свого досвіду тощо [27].

Вчені з Університетського коледжу Лондона і Університету Шеффілда створили “комп’ютерного суддю”, який передбачає рішення Європейського суду з прав людини з точністю до 79 %. Розроблений алгоритм бере до уваги не лише законні докази, але й моральний бік справи. “Комп’ютерний суддя” аналізує текст справи, використовуючи «алгоритм машинного навчання». Науковці не розглядають винахід як заміну суддів чи адвокатів, але вважають його корисним для швидкого виявлення закономірностей у прийнятті рішень суддями. “Це може бути цінним інструментом для визначення справ, у яких є порушення Європейської конвенції про права людини”, – зазначено у повідомленні. Для розробки алгоритму команда дозволила “комп’ютерному судді” просканувати опубліковані рішення з 584 справ щодо катувань, приниження гідності та

справедливих суддів: “електронний суддя” встановив вердикти з 79 % точності. Одночасно вчені встановили, що рішення Європейського суду з прав людини часто базуються на моральних аспектах, а не правових аргументах [8].

Нещодавно відома компанія Google отримала патент на власну технологію, що дозволяє модернізувати роботів та роботизовані пристрої. Взаємодія значної кількості, без обмеження по максимуму, роботів відбувається через “хмару тегів”, їх власник має можливість налаштувати свої пристрої так, як це йому потрібно, за допомогою смартфона або іншого пристрою на платформі Android. Контролювати їх дії можливо з будь-якого місця, якщо задати у налаштуваннях необхідну програму та код. Компанія стверджує, що її технологія не містить загрози для суспільства та світової безпеки. На їх думку, вона призначена виключно для автоматизації та оптимізації сфери послуг. Також керівництво компанії повідомило, що вони додають зусиль для захисту своєї технології від поширення і використання в галузі гонки озброєнь [26].

Роботи Zooids можуть вишиковуватися у будь-якому порядку відповідно до команди, спілкуватися з користувачем, мають колеса, гіроскоп та датчики, що дозволяють не перетинатися один з одним, працюють тільки разом, зазначає TechCrunch, посилаючись на GitHub розробників. Рухи роботів відслідковуються спеціальним проектором, інструкції до дій вони отримують з командного комп’ютера [15].

Відома міжнародна неурядова організація Amnesty International наполягає на тому, щоб заборонити розробку роботів-вбивць, що ґрунтуються на нових технологіях. Їх прикладом є безпілотний повітряний апарат Shadow Hawk, який розробляється в США компанією Vanguard Defense Industries. Він вже використовувався в Афганістані та Східній Африці проти осіб, які підозрюються у здійсненні диверсійно-терористичної діяльності. Крім того, він може вражати підозрюваних електрошоком з висоти та на відстані, озброєний вогнепальною зброєю (автоматичною гарматою) дванадцятого калібру, 37 мм та 40 мм гранатометами. Велика Британія також нещодавно презентувала новий автономний безпілотний надзвуковий літак Taranis, який має на борту касети для розміщення різних видів високоточної самонавідної зброї [26]. За даними Bureau of Investigative Journalism (“Бюро журналістських розслідувань”), в результаті використання “безпілотників” в період між 2004 та 2013 роками було вбито від 2500 до 3500 осіб, в тому числі, мирних жителів і дітей, і більше ніж тисячі завдано поранення [4].

Міжнародна група вчених з США, Франції та Китаю створила напівсинтетичну форму життя. Тим самим вдалося створити організм з фундаментальними змінами в ДНК, який здатен зберігати їх без відторгнення нескінченно довго. Цей винахід дозволить просунутися у синтезі білків та створити повноцінний штучний генетичний код [22].

Найбільш сприятливе у сучасному світі ставлення до роботів спостерігається в Японії, де з ними стикаються частіше, ніж в інших країнах. Роботи використовуються в галузі охорони здоров’я та догляду за літніми людьми. Примітно, що особи похилого віку, не бажаючи відволікати персонал, іноді з більшим задоволенням спілкуються з роботами. Справедливим виглядає припущення, що цей досвід поширюватиметься світом [28].

Про намір залучити роботів до служби в поліції повідомили в прес-службі поліцейського управління Дубаї. Спочатку заплановано використовувати їх для проставлення штампів на документах, нагадування про справи та важливі робочі моменти, фіксації різного роду порушень роботи, а прикордонники мають намір обладнати аеропорти системою розпізнавання не задекларованих речей [21].

Вже зараз високоточні пристрої проводять складні хірургічні операції, одними за найбільш відомих проєктів на сьогодні є Deep Blue (машина-шахіст), IBM Watson (пристрій з сприйняття мови, поведінки та процесу мислення людини), MYCIN (потужна система діагностики захворювань).

У найближчому майбутньому нас чекають ще більш революційні зміни.

Група експертів під керівництвом Еріка Хорвіца (Eric Horvitz), керуючого директора лабораторії Microsoft Research, колишнього президента Асоціації з покращення штучного інтелекту, вважає, що вже до 2030 року нас чекають наступні зміни [29]:

- в сфері транспорту – безпілотні автомобілі, самокеровані вантажівки, атомні дрони доставки (дрон – безпілотний апарат для переміщення у повітрі, від англ. Drone – трутень); потоки даних від збільшення числа датчиків дозволять адміністраторам моделювати рухи окремих людей, їх уподобання та цілі, що значною мірою вплине на дизайн міської інфраструктури тощо;

- домашнє господарство – більш поширеними стануть роботи-прибиральники, підключені до Інтернет-хмар роботи отримують можливість здійснювати обмін даними та навчатися за рахунок цього дедалі швидше; не надто коштовні 3D-датчики типу Microsoft Kinect прискорять розвиток перцептивних технологій (перцепція – від лат. perceptio – “сприйняття”), прориви в галузі розпізнання мови покращать взаємодію роботів з людьми тощо;

- охорона здоров’я – тривалий та складний процес ведення записів пацієнтів та опанування наукової літератури буде автоматизований, цифровий помічник дозволить лікарям зосередитися на людських аспектах догляду за пацієнтами та вивільнити свою інтуїцію, екзоскелети допоможуть літнім людям підтримувати себе в активній формі тощо;

- освіта – різниця між груповим та індивідуальним навчанням може бути усунута, масові онлайн-курси дозволять налаштувати процес навчання індивідуально за будь-яким масштабом, сумісні з штучним інтелектом системи освіти вивчатимуть уподобання індивідів, сприятимуть накопиченню даних та розвитку нових інструментів, складні системи віртуальної реальності дозволять студентам занурюватися в історичні та вигадані світи з метою їх дослідження поза безпосереднім контактом тощо;

- незаможні спільноти та особи – прогностична аналітика дозволить урядовим агентам краще розподіляти обмежені ресурси, передбачати екологічні загрози тощо;

- суспільна безпека – міста будуть значною мірою залежати від технологій штучного інтелекту для виявлення і прогнозування злочинності, автоматична обробка відеонагляду і зйомка згори за допомогою дронів дозволять швидко виявляти протиправну поведінку, аналіз мови та рухів може допомогти виявляти підозрілу поведінку, штучний інтелект може подолати упередженість і бути у порівнянні з уповноваженими фізичними особами (службові особи, представники місцевої влади, особи, що надають публічні послуги) більш відповідальним, послідовним і чесним в сфері правозастосування тощо.

Поряд з цим існує думка, що невдовзі люди і роботи будуть конкурувати між собою на ринку праці [23].

Наскільки реальною є можливість створення штучного інтелекту (крім вищезгаданого проєкту Busy Child), свідчать наступні факти.

За повідомленням видання Technology Review вже через 60 років штучний інтелект стане значною загрозою для людства. До 2022 року він буде мислити приблизно на 10% як людина, до 2040 року – на 50 %, до 2075 року – процеси мислення неможливо буде відрізнити від людських. До таких умовиводів прийшов шведський вчений, професор

Оксфордського університету Нік Бостром (Niklas Boström), який пропонує бути більш обережними, оскільки вважає його занадто загрозливим для людства (проблемою контролю над штучним інтелектом займаються у світі приблизно шість дослідників, питаннями його створення – десятки і сотні тисяч) [6]. Такої самої думки дотримується й Ілон Маск (Elon Musk) [9] – засновник компаній Tesla і SpaceX.

Стриманий оптимізм і застереження цих дослідників можливо узагальнити наступним чином: 1) внаслідок здатності до саморозвитку штучний інтелект перетвориться в суперінтелект; 2) у суперінтелекта з’являться свої власні потреби і цілі (він може бути менш людським, ніж розумний прибулець); 3) суперінтелект може спробувати використати людей проти їх волі (наприклад, з метою отримання доступу до ресурсів); 4) суперінтелект може забажати залишитися єдиним інтелектом навкруги; 5) людина, як система зручно згрупованих атомів, може зацікавити суперінтелект в якості ресурсу; 6) людство не є готовим до зустрічі з суперінтелектом і ще не буде готове багато років; 7) людство повинно навчитися тримати штучний інтелект під достатнім контролем.

У зв’язку з вищевикладеними обставинами виникає питання про можливість та(або) доцільність визнання штучного інтелекту суб’єктом правовідносин, в тому числі кримінально-правових.

До тих пір, поки відповідальність покладається на виробника (розробника) та(або) користувача, питання про визначення суб’єкта не викликає складнощів. Але у випадку, наприклад, розробки програмного забезпечення з відкритим початковим кодом (коли його розробниками є невизначена кількість осіб) визначити виробника буде доволі складно. Ще складнішою буде ситуація з штучним інтелектом, який сам себе усвідомлює, наділений можливістю самовдосконалення, дбає про власне самозбереження та отримання необхідних ресурсів, має здібності до творчої діяльності тощо.

Все, що створено працею людини, ми поки що обґрунтовано сприймаємо в якості об’єктів права власності, предметів злочину, речей, у яких апріорі не може бути законних прав та охоронюваних інтересів. Відповідно вони не можуть нести відповідальність за спричинену шкоду, відповідати за зобов’язаннями тощо.

Між тим, штучний інтелект суттєво відрізняється від інших явищ та об’єктів. Дослідники Джордж Дайсон (George Dyson) [5] та Кевін Келлі (Kevin Kelly) [7], взагалі, висунули гіпотезу про те, що інформація – це форма життя.

Наявність інтелекту та особистості не у людини, а у іншої істоти, вже визнана на державному рівні в одній з країн сучасного світу, яка поряд з контрастами занепаду постачає своїх видатних представників на ринок інтелектуальних надбань та у сферу загального гуманістичного розвитку людства: в Індії статус “особистості, яка не відноситься до людського роду” нормативно закріплений за одним з представників заgonу водних ссавців – дельфінами. Одночасно з цим заборонено заходи з участю дельфінів у дельфінаріях, акваріумах, океанаріумах тощо. У рішенні, яке було оголошено керівником Міністерства навколишнього середовища цієї країни, підкреслюється, що дельфіни є високоінтелектуальними ссавцями з високо розвинутою соціальною організацією, їм властиві людиноподібне самоусвідомлення та залучення у складну систему комунікацій, у зв’язку з чим вони повинні мати свої власні особливі права [17].

У свою чергу, Європейський парламент прийняв на розгляд проект резолюції про правовий статус роботів як “електронної особистості (електронної особи)” [14]. Проект Резолюції передбачає наділення роботів статусом “електронної особистості”, яка має специфічні права та обов’язки. Як зазначається у доповіді автора проекту Резолюції, роботи не можуть розглядатися просто інструментами у руках їх володільців, розробників або користувачів (це дещо співзвучно з тим, що плід не вважається

частиною тіла матері. Сесією Ради Європи з біоетики (грудень 1996 р.) визначено, що протягом усього внутрішньоутробного розвитку плід не можна вважати частиною тіла вагітної жінки, його неможливо розглядати як орган чи частину тіла організму майбутньої породіллі), внаслідок чого дедалі важливішим стає питання про те, чи повинні роботи мати власний юридичний статус або ні. Резолюція встановлює загальні та етичні принципи розвитку галузі робототехніки та штучного інтелекту для використання у суспільстві, які повинні враховуватися під час соціального, екологічного та іншого впливу, та здатні були б забезпечити відповідність поведінки роботів правовим, етичним та іншим стандартам, в тому числі вимогам безпеки. Наприклад, передбачається обов'язок розробників роботів інтегрувати в механізм та програми останнього аварійний вимикач з метою миттєвого відключення всіх процесів у надзвичайних ситуаціях.

Вказана Резолюція має на меті регулювання правового статусу роботів у суспільстві людей, для чого пропонується: створити спеціальне Європейське агентство з робототехніки і штучного інтелекту; розробити нормативне визначення “розумний автономний робот”; розробити систему реєстрації всіх версій роботів разом із системою їх класифікації; зобов'язати розробників надавати гарантії запобігання ризикам; розробити нову структуру звітності для компаній, які використовують роботів або мають потребу в них, що передбачатиме, в тому числі, відомості про вплив робототехніки та штучного інтелекту на економічні результати діяльності компанії [20].

У згаданій доповіді зазначається, що для розробника є доволі складним запобігти передбачуваній шкоді у тому випадку, коли роботи здатні до самовдосконалення та адаптації. Тому, замість того, щоб розташувати штучний інтелект серед вже відомих категорій (фізичні особи, юридичні особи, тварини, речі та інші суб'єкти та об'єкти), пропонується створення нової категорії “електронних осіб” як більш доцільної [30].

Наділення штучного інтелекту статусом “електронної особи”, скоріш за все, не повинне зустріти заперечень та неприйняття у сфері кримінально-правових правовідносин. Ця новація може спиратися на усталений, перевірений теорією та практикою підхід щодо визнання юридичної особи суб'єктом численних правовідносин, а також на нормативне закріплення можливості застосування до юридичної особи заходів кримінального-правового характеру (штраф, загальна конфіскація майна, ліквідація) на підставі положень ст.ст. 96-3, 96-4, 96-6 Розділу XIV-1 “Заходи кримінально-правового характеру щодо юридичних осіб” КК України за вчинення від її імені та(або) в її інтересах певного злочину (ст.ст. 109, 110, 113, 146, 147, ч. 2-4 ст. 159-1, ст.ст. 160, 209, 260, 262, 306 КК України та інші), що завуальовано наділяє юридичну особу практично такою ж мірою відповідальності, яка є у фізичної особи – суб'єкта злочину.

У зв'язку з цими обставинами правова доктрина в галузі кримінального права підлягає переоцінці та трансформації [25].

Штучний інтелект, фізично втілений в об'єкт робототехніки, повинен розглядатися в якості суб'єкта правовідносин, можливо, десь посередині між юридичними і фізичними особами, поєднуючи їх окремі риси з врахуванням відповідної специфіки.

Можливо, штучний інтелект може одночасно розглядатися і як об'єкт, і як суб'єкт права. Теоретичні дослідження у цьому напрямку вже тривають, наприклад, здійснюються Райаном Кало (Ryan Calo) [3] професором University of Washington School of Law, директором UW Tech Policy Lab [10] [11], поряд з вивченням можливості притягнення роботів до кримінальної відповідальності (дослідження в цьому напрямку здійснюються професором Umeå Universitet (Швеція) Питером Асаро (Peter M. Asaro) [1]).

У зв'язку з цим виявляється доволі можливою поява в КК України розділу під умовною назвою XIV-2 “Заходи кримінально-правового характеру щодо електронних осіб”.

Між тим, роздуми щодо відповідальності, в тому числі кримінальної, штучного інтелекту мають сенс тільки в тому випадку, якщо людство збереже контроль над ним. Якою мірою є обґрунтованими сумніви у цьому, свідчать окремі поодинокі твердження. Так, згаданий Джеймс Баррат вважає, що підсумковою стадією робіт зі створення спочатку розумних машин, а потім машин, які є більш розумними за людину, стане не їх інтеграція у наше життя, а їх перемога над нами [16, с. 75]. Це твердження він ілюструє наступним спостереженням: ДНК людини та плоских черв'яків має багато спільного, але навряд чи ми переймалися би їх цілями, цінностями та мораллю, якщо б навіть усвідомили, що вони були нашими попередниками. В якості змішаних (позитивно-негативних) рис та якостей штучного інтелекту вказують на наступні: самокопіювання (здатність до поширення); вирішення завдання способом мозкового штурму з залученням багатьох копій самого себе; надшвидкісні обчислення (напр., окремі спостерігачі з Уолл-стріт вже висловлювали припущення про те, що деякі алгоритми сигналізують один одному та поширюють інформацію за допомогою мілісекундних угод – високочастотного трейдингу [16, с. 46]); здатність працювати без перерв та вихідних; можливість імітації дружелюбності або власної смерті тощо. Те, що створено штучним інтелектом, може бути зовсім або частково не зрозумілим людині: наприклад, алгоритми, які були розроблені професором Стенфордського університету, піонером у використанні генетичного програмування для оптимізації складних проблем, творцем скретч-карти Джоном Коза (John R. Koza), десятки разів самостійно повторно відтворювали винаходи, які вже були раніше запатентовані, а інколи пропонували додаткові компоненти, з якими пристрої працювали краще, ніж запропоновані винахідниками-людьми. Професора математики Вернора С. Вінджа (Vernor Steffen Vinge) турбує “шлюб”, що формується між людьми та комп'ютерами на просторах мережі Інтернет, якому він запропонував назву Цифрова Гея [12; 13].

Робототехніка та її програмне забезпечення стають дедалі більше укладнюватися. За законом Мура (емпіричне спостереження, зроблене в 1965 році, через шість років після винаходу інтегральної схеми, одним із засновників компанії Intel Гордоном Муром (Moore Gordon), кожні 18 або 24 місяця відбувається подвоєння кількості транзисторів на нових кристалах мікропроцесорів. Час, коли людство буде поділяти середовище свого існування зі штучним інтелектом, неминуче наближається. Штучні та біологічні об'єкти невдовзі складно буде відрізнити один від одного. Віртуальні світи стануть більш захоплюючими, ніж реальне оточення [24]. Жодна країна або корпорація не відмовиться від досліджень штучного інтелекту, якщо сподіватиметься на певні переваги та побоюватиметься конкурентів. Він може виявитися більш небезпечним, ніж будь-яка сучасна зброя. Але для того, щоб штучний інтелект спричинив невідворотну шкоду, достатньо навіть і банальної недбалості.

Висновки.

Враховуючи вищевикладене, вбачаються підстави до наступних висновків та деяких пропозицій.

Дослідження в сфері робототехніки та їх втілені результати вже сьогодні значною мірою впливають на життя сучасних суспільств.

Можливість створення штучного інтелекту, який дорівнює інтелекту людини або перевищує його, є доволі реальною та такою, що може бути досягнута у найближчому майбутньому, у найближчі десятиріччя.

Неминуче наближається час, коли людство буде поділяти середовище свого існування зі штучним інтелектом.

Доволі реальною та перспективною вбачається можливість визнання штучного інтелекту суб'єктом правовідносин, наділення його правовим статусом “електронної особистості (електронної особи)”.

Цілком реальною є перспектива застосування до штучного інтелекту заходів кримінально-правового характеру, поява у зв'язку з цим в Особливій частині КК України розділу під умовною назвою XIV-2 “Заходи кримінально-правового характеру щодо електронних осіб”.

Роздуми щодо відповідальності штучного інтелекту мають сенс тільки в тому випадку, якщо людство збереже контроль над останнім.

Перспективи подальших досліджень. Розглянуті питання та надана їм авторська оцінка є дискусійними та відкритими для широкого обговорення з огляду на їх актуальність та важливість для забезпечення сталого розвитку суспільства і збереження людства.

Використана література

1. Asaro P. Robots and Responsibility from a Legal Perspective. – Mode of access : [//www.peterasaro.org/writing/ASARO_Legal_Perspective.pdf](http://www.peterasaro.org/writing/ASARO_Legal_Perspective.pdf)
2. Barrat James. Our Final Invention: Artificial Intelligence and the End of the Human Era. – Mode of access : [//www.tor.com/2013/09/20/our-final-invention-excerpt](http://www.tor.com/2013/09/20/our-final-invention-excerpt)
3. Calo R. Robots in American Law / Legal Studies Research Paper No. 2016-04 / University of Washington School of Law. – Mode of access : [//www.datascienceassn.org/sites/default/files/Robots_in_American_Law.pdf](http://www.datascienceassn.org/sites/default/files/Robots_in_American_Law.pdf)
4. Drone War – The bureau of investigative journalism. – Mode of access : [//www.thebureauinvestigates.com/projects/drone-war](http://www.thebureauinvestigates.com/projects/drone-war)
5. Dyson G. The birth of the computer. – Mode of access : [//www.ted.com/talks/george_dyson_at_the_birth_of_the_computer?language=ru#t-83137](http://www.ted.com/talks/george_dyson_at_the_birth_of_the_computer?language=ru#t-83137) – Title from the screen.
6. Etzioni Oren. No, the Experts Don't Think Superintelligent AI is a Threat to Humanity. – Mode of access : [//www.technologyreview.com/s/602410/no-the-experts-dont-think-superintelligent-ai-is-a-threat-to-humanity](http://www.technologyreview.com/s/602410/no-the-experts-dont-think-superintelligent-ai-is-a-threat-to-humanity)
7. Kelly K. How technology evolves. – Mode of access : [//www.ted.com/talks/kevin_kelly_on_how_technology_evolves?language=ru](http://www.ted.com/talks/kevin_kelly_on_how_technology_evolves?language=ru)
8. Knapton Sarah. Artificially intelligent ‘judge’ developed which can predict court verdicts with 79 per cent accuracy. – Mode of access : [//www.telegraph.co.uk/science/2016/10/23/artificially-intelligent-judge-developed-which-can-predict-court](http://www.telegraph.co.uk/science/2016/10/23/artificially-intelligent-judge-developed-which-can-predict-court)
9. Kumparak G. Elon Musk Compares Building Artificial Intelligence To “Summoning The Demon”. – Mode of access : [//www.techcrunch.com/2014/10/26/elon-musk-compares-building-artificial-intelligence-to-summoning-the-demon](http://www.techcrunch.com/2014/10/26/elon-musk-compares-building-artificial-intelligence-to-summoning-the-demon)
10. Robots in American Law. – Mode of access : [//www.strausscenter.org/event/444-robots-in-american-law.html](http://www.strausscenter.org/event/444-robots-in-american-law.html)
11. Siegel H. American law needs a reboot when it comes to robots. – Mode of access : [//www.robohub.org/american-law-needs-a-reboot-when-it-comes-to-robots](http://www.robohub.org/american-law-needs-a-reboot-when-it-comes-to-robots)
12. Vinge V. BFF's first adventure. – Mode of access : <http://www.nature.com/nature/journal/v518/n7540/full/518568a.html>
13. Vinge V. 2020 Computing : The creativity machine. – Mode of access : [//www.nature.com/nature/journal/v440/n7083/full/440411a.html](http://www.nature.com/nature/journal/v440/n7083/full/440411a.html)
14. Wakefield Jane. MEPs vote on robots' legal status – and if a kill switch is required. – Mode of access : [//www.bbc.com/news/technology-38583360](http://www.bbc.com/news/technology-38583360)

15. Zooids: Building Blocks for Swarm User Interfaces. – (Extended Material). – Mode of access : <https://github.com/ShapeLab/SwarmUI>.

16. Баррат Дж. Последнее изобретение человечества : искусственный интеллект и конец эры Homo sapiens / Дж. Баррат. – М. : Альпина Нон-фикшн, 2015. – 304 с.

17. Индия признала дельфинов личностями и запретила дельфинарии. – Режим доступа : [//www.econet.ru/articles/78180-indiya-priznala-delfinov-lichnostyami-i-zapretila-delfinariii](http://www.econet.ru/articles/78180-indiya-priznala-delfinov-lichnostyami-i-zapretila-delfinariii)

18. Карчевский Н.В. Перспективные задачи уголовного права в контексте развития робототехники : матеріали міжнар. наук.-практ. конф. [“Соціальна функція кримінального права : проблеми наукового забезпечення, законотворення та правозастосування”], (Харків, 12 – 13 жовт. 2016 р.) ; редкол. В.Я. Тацій (голов. ред.), В.І. Борисов, (заст. голов. ред.) та ін. – Х. : Право, 2016. – 564 с. – С. 109-113.

19. Карчевський М.В. Право роботів, або робот з правами. – Режим доступа : [//www.ukrainepravo.com/scientific-thought/naukova-dumka/pravo-robotiv-abo-robot-z-pravami](http://www.ukrainepravo.com/scientific-thought/naukova-dumka/pravo-robotiv-abo-robot-z-pravami)

20. Коваль М. Электронная личность : зачем ЕС обсуждает права роботов. – Режим доступа : [//www.eurointegration.com.ua/rus/experts/2017/01/24/7060539](http://www.eurointegration.com.ua/rus/experts/2017/01/24/7060539)

21. Ларионов В. Полиция Дубая начнет использовать роботов. – Режим доступа : [//www.hi-news.ru/technology/policiya-dubaya-nachnyot-ispolzovat-robotov.html](http://www.hi-news.ru/technology/policiya-dubaya-nachnyot-ispolzovat-robotov.html)

22. Новые боги. Создана полусинтетическая форма жизни. – Режим доступа : [//www.x-files.org.ua/news.php?readmore=4890](http://www.x-files.org.ua/news.php?readmore=4890)

23. Понзель М.Г. Люди и роботы : кому достанутся рабочие места. – Режим доступа : [//www.protokol.com.ua/ua/lyudi_ili_roboti_komu_dostanutsya_rabochie_mesta](http://www.protokol.com.ua/ua/lyudi_ili_roboti_komu_dostanutsya_rabochie_mesta)

24. Радутний О.Е. Кримінальна відповідальність юридичної особи стане кроком до закріплення віртуальності життєвого простору // Електронне наукове фахове видання Національного університету “Юридична Академія України ім. Ярослава Мудрого”. – № 1/2011. – Режим доступа : [//www.nauka.jur-academy.kharkov.ua](http://www.nauka.jur-academy.kharkov.ua)

25. Радутний О.Е. Трансформація правової доктрини під впливом запровадження кримінальної відповідальності юридичних осіб : матеріали Міжнар. наук.-практ. конф. [“Правова доктрина – основа формування правової системи держави”], (Харків, 20 – 21 листопада. 2013 р.) / присвяч. 20-річчю Нац. акад. прав. наук України та обговоренню п’ятитомної монографії “Правова доктрина України”. – Х. : Право, 2013. – 1032 с. – С. 700-702.

26. Сербенко Н. Автономные системы вооружения : нерешенные вопросы морали, нравственности, международного права и геополитики. – Режим доступа : [//www.bintel.com.ua/ru/article/robots2](http://www.bintel.com.ua/ru/article/robots2)

27. Фурман І.М. IBM внедрила юриста с искусственным интеллектом “Росс”, который в полную силу уже работает в одной из известных юркомпаний в США. – Режим доступа : [//www.protokol.com.ua/ua/yurist_s_iskusstvennim_intellektom_ross_bil_nanyat_na_svoyu_pervuyu_yurfirmu](http://www.protokol.com.ua/ua/yurist_s_iskusstvennim_intellektom_ross_bil_nanyat_na_svoyu_pervuyu_yurfirmu).

28. Хель И. Очень скоро мы будем любить роботов так, как их любят в Японии. – Режим доступа : [//www.hi-news.ru/robots/ochen-skoro-my-budem-lyubit-robotov-tak-kak-ix-lyubyat-v-yaponii.html](http://www.hi-news.ru/robots/ochen-skoro-my-budem-lyubit-robotov-tak-kak-ix-lyubyat-v-yaponii.html)

29. Хель И. 8 способов, которыми ИИ изменит городскую жизнь к 2030 году. – Режим доступа : [//www.hi-news.ru/technology/8-sposobov-kotorymi-ii-izmenit-gorodskuyu-zhizn-k-2030-godu.html](http://www.hi-news.ru/technology/8-sposobov-kotorymi-ii-izmenit-gorodskuyu-zhizn-k-2030-godu.html)

30. Хель И. Права роботов : когда разумную машину можно считать “личностью”. – Режим доступа : [//www.hi-news.ru/robots/prava-robotov-kogda-razumnuyu-mashinu-mozhno-schitat-lichnostyu.html](http://www.hi-news.ru/robots/prava-robotov-kogda-razumnuyu-mashinu-mozhno-schitat-lichnostyu.html)

~~~~~ \* \* \* ~~~~~

УДК 343:340.65

**КАТЕРИНЧУК К.В.**, кандидат юридичних наук, доцент,  
доцент кафедри кримінального права і процесу  
Навчально-наукового юридичного інституту  
Національного авіаційного університету  
**ЮХИМЕЦЬ І.О.**, начальник Тернопільського обласного бюро  
судово-медичної експертизи

### “ТІЛЕСНІ УШКОДЖЕННЯ” ЧИ “ШКОДА ЗДОРОВ’Ю”: ЮРИДИЧНИЙ ТА СУДОВО-МЕДИЧНИЙ ПОГЛЯДИ

***Анотація.** Стаття присвячена проблемам термінології та визначення змісту понять, що містяться в Кримінальному кодексі України та підзаконних нормативно-правових актах. Досліджено ознаки тілесних ушкоджень, здійснено аналіз праць науковців, що займалися даною тематикою, наведено власне бачення щодо вдосконалення закону про кримінальну відповідальність, а саме злочинів проти здоров’я особи.*

***Ключові слова:** здоров’я особи, злочин, шкода здоров’ю, тілесні ушкодження.*

***Аннотация.** Статья посвящена проблемам терминологии и определения содержания понятий, которые содержатся в Уголовном кодексе Украины и подзаконных нормативно-правовых актах. Исследованы признаки телесных повреждений, осуществлен анализ трудов ученых, которые занимались данной тематикой, приведено свое видение по совершенствованию уголовного закона, а именно преступлений против здоровья человека.*

***Ключевые слова:** здоровье человека, преступление, вред здоровью, телесные повреждения.*

***Summary.** The article is devoted to the issues of terminology and determination of the content of concepts which are contained in the Criminal code of Ukraine and regulatory and legal acts. The paper explores signs of bodily injuries, conducts the analysis of works of scientists which were engaged in this subject. Authors provide their own opinion on improvement of criminal law, namely crimes against the human health.*

***Keywords:** human health, crime, harm to the health, bodily injuries.*

**Постановка проблеми.** Суспільна небезпека, як загальноприйнята соціальна (матеріальна) ознака злочину, виражається у двох вимірах: якісному, тобто характером суспільної небезпеки, що пов’язаний із соціальною цінністю об’єкта посягання (на особливу соціальну цінність об’єкта посягання – здоров’я особи, вказує те, що виділений об’єкт охороняється тільки кримінально-правовими заходами), і кількісному – її ступенем, який визначається тяжкістю наслідків, тобто зовнішніх вимірів, що відбулися у результаті вчинення того або іншого злочину, найбільш поширеними серед яких є заподіяння тілесних ушкоджень. Якщо характер суспільної небезпеки слугує критерієм відмежування одного виду злочину від іншого, то ступінь суспільної небезпеки є тією об’єктивною величиною, яка дозволяє відокремити один злочин від іншого усередині певного виду. Отже, характер суспільної небезпеки діяння та її ступінь мають самостійні правові значення. Викладене підтверджується нормативною регламентацією кримінальної відповідальності за посягання на здоров’я особи. Адже, “...позбавлення людини здоров’я, навіть і тимчасове, пов’язане із заподіянням їй фізичної, моральної, а часто і матеріальної шкоди. Заподіяння тілесних ушкоджень, побоїв та скоєння інших подібних злочинів не тільки спричиняє шкоду здоров’ю, але й

зачіпає інші інтереси особи” [1, с. 8]. “Дійсно, заподіяння шкоди здоров’ю відволікає сили людини на відновлення втраченого блага: лікування, пристосування до нових несприятливих умов. Людина не може повноцінно працювати, навчатися, вести особисте життя. Крім того, людина, здоров’ю якої заподіяна шкода, часто не може застосувати заходи, необхідні для особистої гігієни, зміцнення організму. Потрібно також врахувати, що заподіяння шкоди здоров’ю людини часто позбавляє її можливості виконати свої громадянські обов’язки та користуватися рядом прав (наприклад, може перешкодити призову на дійсну військову службу, виконанню спеціальних робіт і т.п.)” [2, с. 40]. Однак, попри важливість даної проблеми, положення деяких підзаконних актів у теперішній час перебувають у несумісності із чинним Кримінальним кодексом України (далі – КК України), як і самі норми цього Закону України подекуди сприймаються неоднозначно.

**Метою статті** є дослідження ознак тілесних ушкоджень та надання пропозицій щодо удосконалення законодавства у цій сфері.

**Виклад основного матеріалу.** Аналізуючи статті КК України “Розділ II. Злочини проти життя та здоров’я, які передбачають і кримінальну відповідальність за заподіяння шкоди здоров’ю особи”, ми виокремлюємо найбільш поширений суспільно небезпечний наслідок – тілесні ушкодження.

За своїми об’єктивними ознаками склади злочинів, що передбачають кримінальну відповідальність за заподіяння тілесних ушкоджень, належать до матеріальних складів, адже передбачають не лише наявність суспільно небезпечного діяння, але й настання певних наслідків. Наслідком будь-якого тілесного ушкодження є та шкода, яка спричиняється здоров’ю потерпілого винними діями суб’єкта злочину. Як зазначають науковці, “об’єктивна сторона тілесних ушкоджень представляє значну складність для аналізу, тому що різноманітні не лише самі дії, якими спричиняються тілесні ушкодження, досить різний і характер шкоди, заподіяної здоров’ю” [3, с. 16, 24].

Не менш дискусійним є питання застосування певних термінів.

Деякі автори наголошують, що, вживаючи термін “тілесні ушкодження”, кримінальний закон тим самим акцентує увагу лише на боротьбі із зовні видимими й найбільш поширеними видами шкоди здоров’ю травматичного походження і не враховує можливості насильницького заподіяння шкоди на фоні прихованої патології” [4, с. 127].

Інші науковці зазначають, що термін “тілесне ушкодження” є кримінально-правовим, а не медичним; у медицині вивчаються і використовуються поняття “ушкодження”, “травма” [5, с. 89].

В. Векселенко, М. Галукова допускають вживання терміну “ушкодження” у юридичній літературі та у судовій практиці в тих випадках, коли вживання терміну “травма” стилістично не доцільне [6].

Вдалою є пропозиція Г.М. Борзенкова щодо заміни поняття “тілесні ушкодження” на більш широке поняття “шкода здоров’ю” – це сприяло б уніфікації термінології та усувало проблеми для кримінально-правової кваліфікації, пов’язані із надто вузьким розумінням поняття “тілесні ушкодження” [7, с. 166-168] та розбіжностями у його тлумаченні.

А.А. Піонтковский під тілесним ушкодженням розуміє “протиправне умисне або необережне заподіяння однією особою шкоди здоров’ю, або фізичних страждань іншій особі шляхом порушення анатомічної цілості тканин, або правильного функціонування тканин чи органів людського організму” [8, с. 569].

О.С. Нікіфоров більш звужує це поняття: на його думку, “тілесним ушкодженням ...може бути визнане здійснене ким-небудь з умислом або з необережності діяння, що заподіяло розлад здоров'ю іншої особи як єдиному безпосередньому об'єкту” [9, с. 14]. З даних визначень випливає, що, по-перше, автори використовують різні за змістом та формою терміни – “розлад здоров'я” та “шкода здоров'ю”, нерідко у тому самому контексті. По-друге, у визначенні тілесних ушкоджень фігурує термін “фізичні страждання”, який не є і не може бути ознакою тілесного ушкодження. Фізичні страждання, як один із суспільно небезпечних наслідків, виокремлені у ст. 127 (катування) КК України.

З медичної точки зору, тілесне ушкодження – це порушення анатомічної цілості тканин, органів або їх фізіологічних функцій, що виникають від дії одного чи кількох факторів зовнішнього середовища – фізичних (механічних, термічних, барометричних, променистих тощо), хімічних та інших. У юриспруденції тілесні ушкодження розрізняють за ступенем тяжкості: тяжке (ст. 121 КК України), середньої тяжкості (ст. 122 КК України) та легке (ст. 125 КК України).

Відповідно до ч. 1 ст. 121 КК України, до тяжкого тілесного ушкодження належить ушкодження: 1) небезпечне для життя в момент заподіяння чи таке, що спричинило; 2) втрату будь-якого органа або його функцій; 3) психічну хворобу; 4) інший розлад здоров'я, поєднаний зі стійкою втратою працездатності не менш як на одну третину; 5) переривання вагітності; 6) непоправне знівечення обличчя.

Як випливає зі змісту ч. 1 ст. 122 КК України, до середньої тяжкості належить таке тілесне ушкодження, що: 1) не є небезпечним для життя і не потягло за собою наслідків, передбачених у ст. 121 КК України, але при цьому 2) спричинило тривалий розлад здоров'я або 3) значну стійку втрату працездатності менш як на одну третину.

У ст. 125 КК України законодавець розрізняє легке тілесне ушкодження (ч. 1) та легке тілесне ушкодження, що спричинило короточасний розлад здоров'я або незначну втрату працездатності (ч. 2). Досліджуючи ознаки тілесних ушкоджень, що визначені законодавцем у відповідних статтях КК України, пропонуємо зосередити увагу на тих, які викликають найбільше дискусій.

При порівнянні норм нині діючого Закону України – КК України 2001 року, із положеннями підзаконного акту – “Правилами судово-медичного визначення ступеня тяжкості тілесних ушкоджень”, затвердженими наказом МОЗ України № 6 ще у 1995 році [10] (далі – Правила 1995 р.), привертають увагу певні невідповідності у цих документах. Наприклад, у тексті Закону однією з кваліфікуючих ознак тяжкого тілесного ушкодження (ст. 121 КК України) названа безпека для життя в момент заподіяння. Такого застереження щодо обов'язкового зв'язку кінцевих наслідків ушкодження із часом його спричинення у п. 2.1.1 а) Правил 1995 р. немає, хоча з подальших (у п. 2.1.2) роз'яснень випливає, що небезпечними для життя є ушкодження, що в момент заподіяння (завдання) чи в клінічному перебігу через різні проміжки часу спричиняють загрозові для життя явища (див. п. 2.1.3 о) і котрі без надання медичної допомоги, за звичайним своїм перебігом, закінчуються чи можуть закінчитися смертю.

У Правилах 1995 р. також визначені не загрозові для життя ушкодження, що належать до тяжких за кінцевим результатом та наслідками: втрата будь-якого органа чи втрата органом його функції – втрата зору, слуху, язика, руки, ноги і репродуктивної здатності. Більш усього непорозуміння виникає при віднесенні тілесних ушкоджень до тяжких за ознакою “втрата органа”, якщо йдеться про втрату одного з парних органів – одного ока, нирки, яєчка.

Наприклад, таке питання вирішувалось у судовому порядку Збаразьким районним судом Тернопільської області. В судовому засіданні обвинувачений заявив клопотання, яке підтримав його захисник, про призначення у даній справі комплексної судово-медичної експертизи, на вирішення якої поставити перед експертами запитання, чи втрата одного яєчка з придатком є втрата частини цільного органу (праве та ліве яєчко з придатками), чи є втратою органу, яке вже не зможе виконувати функцію репродуктивної здатності до запліднення, зачаття. У разі збереження основної функції органу (після втрати його частини правого яєчка з придатками) наявність репродуктивної здатності до запліднення, зачаття, чи можна травму правого яєчка віднести до середньої тяжкості тілесних ушкоджень [11].

Наголошуємо, що у ст. 121 КК України йдеться про “будь-який орган”, у ній не вказано він парний чи непарний. Оскільки у даному контексті “орган” – поняття не юридичне, він не має юридичних ознак чи показників, то слід завжди виходити з медико-біологічного визначення органа як функціональної системи організму, а саме: органом людського організму є його частина або цілісне утворення, що має свою певну, лише йому належну форму, будову, функцію, розвиток і положення. Він являє собою систему різних тканин, із яких одна чи кілька домінує і визначає саме його специфічну будову і функцію. Оцінювати анатомічну втрату органа чи втрату органом його функції експерт зобов’язаний відповідно до вимог ст. 121 КК України: втрата одного очного яблука являє собою втрату органа; втрата зору на одне око являє собою втрату органом його функції; втрата одного яєчка являє собою втрату органа; втрата слуху на одне вухо являє собою втрату органом його функцій. Такий підхід цілком науково обґрунтований положеннями, що впливають із поняття “орган”. До речі, у Російській Федерації так оцінюють втрату органа з 1996 року.

Психічна хвороба, як результат спричинення шкоди здоров’ю внаслідок дії фактора зовнішнього середовища, належить до тяжких тілесних ушкоджень. У Правилах 1995 р. вказано (зокрема у п. 1.2) на вплив ушкоджуючого психічного фактора, без будь-яких роз’яснень, що слід розуміти під психічною травмою – сварку, конфлікт, бійку, переляк, стрес; як і хто її діагностує, які є для цього об’єктивні дані і експертні можливості.

За змістом п. 2.1.5 Правил 1995 р., діагноз психічного захворювання і причинно-наслідковий зв’язок між ушкодженням і психічним захворюванням, що розвинулось, встановлюється психіатричною експертизою. Ступінь тяжкості такого тілесного ушкодження визначається судово-медичним експертом з урахуванням висновків цієї експертизи [10].

У спеціальній літературі різних років науковці використовували терміни: “психічний розлад”, “душевна хвороба”, “психічна хвороба”, “психічне захворювання”. У ст. 1 Закону України “Про психіатричну допомогу” зазначено, зокрема, що психічними розладами є розлади психічної діяльності, визнані такими згідно з чинною в Україні Міжнародною статистичною класифікацією хвороб, травм і причин смерті [12].

Постанова Пленуму Верховного Суду України “Про судову практику у справах про зґвалтування та інші статеві злочини” [13] до прийняття постанови Пленуму Верховного Суду України “Про судову практику у справах про злочини проти статевої свободи та статевої недоторканості особи” містила термін “душевна хвороба” (п. 15). У діючих на теперішній час Правилах 1995 р. застосовуються терміни: “душевна хвороба”, “психічна хвороба”, “психічне захворювання”, “психічні розлади”, із роз’ясненням, що під душевною хворобою належить розуміти психічне захворювання (психічну хворобу).



До психічних захворювань не можна відносити пов'язані з ушкодженням реактивні стани (психози, неврози) (п. 2.1.5) [10]. Отже, терміни “психічна хвороба”, “психічне захворювання” є синонімічними. Термін “душевна хвороба” є застарілим, він застосовувався у КК України 1960 року як одна з ознак тяжкого тілесного ушкодження. У КК України 2001 року він був замінений на термін “психічна хвороба”. Термін “психічні розлади” не можна відносити до психічної хвороби, тому вони не є кваліфікуючою ознакою тяжкого тілесного ушкодження.

На нашу думку, законодавство України повинно додержуватись єдиної термінології для попередження невірної розуміння та тлумачення поняття “психічна хвороба”, оскільки в науковій літературі вживається саме така назва хвороб головного мозку, які проявляються різноманітними розладами психічної діяльності [15].

Крім зазначеного вище, предметом дискусій науковців часто є вплив і значення часових меж та виліковності психічної хвороби для кваліфікації злочину. У Правилах 1995 р. щодо цього чітко зазначено – “ушкодження кваліфікується як тяжке тільки тоді, коли воно потягло за собою розвиток психічного захворювання, незалежно від його тривалості і ступеня вилікованості. Ступінь тяжкості ушкодження, що викликало реактивний стан нервової системи, визначається за ознакою тривалості розладу здоров'я” [10].

На думку А.П. Філіппова, А.А. Піонтковського психічний розлад може розглядатися як шкода здоров'ю лише в тому випадку, якщо він є невиліковним та хронічним [16, с. 64; 8, с. 578]. Багато вчених розглядають як тяжку шкоду здоров'ю не тільки хронічні душевні захворювання, але й тимчасові, виліковні [17].

М.Д. Шаргородский вважав, що “хвороба може бути як постійна, так і тимчасова, однак вона повинна бути обов'язково серйозна” [18].

А.С. Нікіфоров вказував, що тяжкими тілесними пошкодженнями можуть бути будь-які види хронічного або гострого “серйозного душевного захворювання й, крім того, випадки менш серйозної, навіть незначної, але невиліковної душевної хвороби” [9, с. 31].

В. Векселенко, М. Галукова, зважаючи на те, що психічний розлад є наслідком спричиненого насильства (фізичного або психічного), пропонують обмежити коло психічних розладів, виключивши із нього розлад, не пов'язаний з насильством, і виділити, залежно від характеристик психічного розладу, три ступені важкості психічної шкоди здоров'ю: легку, середню й тяжку шкоду здоров'ю [19]. Щодо даної пропозиції, то виникають питання: у разі поділу психічної шкоди на легку, середню та тяжку, чи буде це здійснюватися в межах ст. 121 КК України; чи буде поширений запропонований поділ на ступені шкоди здоров'ю на інші види тілесних ушкоджень. “Висновок про шкоду здоров'ю при психічних розладах повинен виноситися із врахуванням комплексної клініко-функціональної (характер і тяжкість розладу; характер порушення функцій організму, викликаного даним розладом; особливості перебігу, стійкості або зворотності психопатологічних проявів; клінічний, реабілітаційний прогноз) і прогностичної оцінки стану потерпілого комісією за участю судово-медичного експерта, лікаря психіатра й психолога” [19].

Наступною ознакою тяжкого тілесного ушкодження є розлад здоров'я, поєднаний зі стійкою втратою працездатності не менш як на одну третину, навколо якої тривалий час точилися наукові і правові дискусії. Наприклад, І.С. Ной загалом наполягав, що “ознака втрати працездатності введена у законодавство необґрунтовано. По-перше, відсутні науково обґрунтовані дані, які могли бути покладені в основу класифікації ступеню втрати працездатності як результату злочинних посягань проти здоров'я; по-

друге, втрата працездатності, як критерій класифікації тілесних ушкоджень, не може сприяти справедливому визначенню винності особи, що заподіяла тілесне ушкодження, тому що практично не можливо або досить важко заздалегідь передбачити, якого ступеню буде втрачена працездатність потерпілого від спричиненого йому тілесного ушкодження” [20, с. 77].

Поняття “розлад здоров’я” стосовно тимчасової та стійкої втрати працездатності не однозначне, а тому йому у Правилах 1995 р. необхідно дати адекватне роз’яснення. Під розладом здоров’я треба розуміти будь-яке порушення нормальної діяльності організму або хворобливий процес, які безпосередньо викликані тілесним ушкодженням. Останнє може і не супроводжуватись розладом здоров’я. Розлад здоров’я може бути короткочасним (тимчасовим), тривалим (довгочасним) і постійним (стійким).

Згідно з Правилами 1995 р., розміри стійкої (постійної) втрати загальної працездатності при ушкодженнях встановлюються після наслідку ушкодження, що визначився, на підставі об’єктивних даних з урахуванням документів, якими керується у своїй роботі Медико-соціальна експертна комісія (далі – МСЕК). Під стійкою (постійною) втратою загальної працездатності належить розуміти таку необоротну втрату функції, котра повністю не відновлюється.

У теперішній час у диспозиціях окремих статей КК України (ч. 1 ст.ст. 121 і 122, ч. 2 ст. 125), де йдеться про стійку втрату працездатності та її розмір як кваліфікуючу ознаку тяжкості тілесного ушкодження, немає чіткого визначення: втрата якої саме працездатності мається на увазі – загальної чи професійної, а у ст. 125, крім того, – втрата тимчасова чи стійка? Допущені у цих статтях Закону неточності медичного характеру необхідно виправити. Зокрема, у диспозиції ст. 121 КК України замість словосполучення “зі стійкою втратою працездатності” повинно бути “зі стійкою втратою загальної працездатності”; у ст. 122 замість “значну стійку втрату працездатності” треба вказати “значну стійку втрату загальної працездатності”; у ст. 125 КК України замість “незначну втрату працездатності” зазначити “незначну стійку втрату загальної працездатності”, хоча у лексичному значенні правильніше було б – “стійке пониження загальної працездатності” на стільки-то відсотків. Проблемні питання з приводу визначення ступеня стійкої втрати загальної і професійної працездатності у судово-медичній практиці добре підмічені Г.Ф. Кривдою та П.В. Плевінскіс [21].

Практикуючому фахівцю при визначенні відсотка стійкої втрати загальної працездатності треба посилатись на конкретну статтю реального нормативного документа, якого в Україні досі немає – лікарі судово-медичні експерти донині користуються Інструкцією Міністерства фінансів СРСР 1986 року. Тому потрібні відповідні зміни, як у КК України так і у Правилах 1995 р.

Одним із юридичних критеріїв тяжкого тілесного ушкодження (ст. 121 КК України) є непоправне знівечення обличчя, яке належить до найважливішої характеристики анатомічного та фізіологічного вигляду людини. Нагадаємо, що Правила 1995 р. окреслюють такі межі знань та правові аспекти компетенції судово-медичного експерта з цього приводу: “Судово-медичний експерт не кваліфікує ушкодження обличчя як знівечення, оскільки це поняття не є медичним... Експерт зазначає, що ушкодження може бути розцінене як тяжке, якщо буде визнане таким, що знівечило обличчя”. Правила 1995 р., основне призначення яких дати усім зрозуміле тлумачення юридичних критеріїв ступеня тяжкості тілесних ушкоджень, пояснити, визначити їхню сутність та вказати шляхи їх встановлення, не розкривають зміст поняття “знівечення”, не зазначають, хто повинен кваліфікувати ушкодження як тяжке,

якщо воно буде визнано таким, що знівечило обличчя, не дають чітких уявлень про анатомо-топографічні межі обличчя тощо. Зауважене вимагає адекватного аналізу та певної регламентації.

Теорія кримінального права та науковці в цій сфері припускають, що знівеченим обличчя вважається тоді, коли воно має неприємний, огидний зовнішній вигляд (наприклад, відсутність носа або губ). Тяжкість шкоди при знівеченні обличчя зумовлена не тільки і не стільки фізичною шкодою, скільки психічною травмою, оскільки ця обставина принижує потерпілого, викликає у нього тяжкі душевні переживання, муки [2, с. 45], і, як відмічав М.І. Загородніков: “...ставить потерпілого в такі умови, що його перебування серед інших людей може виявитися неприємним для оточуючих” [1, с. 57-58]. Дана позиція авторів заслуговує на увагу, однак не визначає критерії знівечення і на кого покладається обов’язок це встановлювати. У межах порушеної проблеми підлягає з’ясуванню низка питань, які вимагають однозначної відповіді; а саме: де проходять межі обличчя, що означає його знівечення, хто і як повинен визначати ступінь тяжкості непоправних наслідків ушкоджень обличчя, як і хто повинен оформляти відповідний документ тощо.

Правила 1995 р. фактично забороняють судово-медичному експерту кваліфікувати непоправне ушкодження обличчя як знівечення, “оскільки це поняття не є медичним”, юридичного поняття “знівечення обличчя” також немає, тож воно є не унормованим. М.І. Авдеев зазначає, що це поняття загальнолюдське, естетичне, тобто таке, яке задовольняє вимоги естетики – науки, що вивчає виразні форми, які відповідають уявленням про прекрасне, потворне, величне, підле тощо [22].

У медицині та юриспруденції не існує критеріїв, на підставі яких можна було б у кожному конкретному випадку вирішувати питання про наявність чи відсутність знівечення обличчя. Поняття “знівечення” відноситься тільки до обличчя, тобто до людського образу, подоби, фізіономії. На думку С.Г. Киренка, непоправне знівечення можливе не лише обличчя, а й інших частин тіла людини. У випадках знівечення спини, рук або інших частин тіла людина буде почувати себе пригнічено, переживати, що не може носити відкритий одяг, активно з усіма іншими займатися спортом, ходити на пляж та ін., тому цей недолік слід усунути і визнати, що знівеченим при тілесних ушкодженнях може бути не лише обличчя, а й інші частини тіла і віднести подібні випадки до тяжких тілесних ушкоджень. Тим самим автор пропонує доповнити частину першу ст. 121 КК України наступною ознакою тяжкого тілесного ушкодження, як непоправне знівечення обличчя або тіла [2, с. 45-48]. Дійсно, змінювати, знівечувати зовнішність людини можуть, наприклад, деформація хребта, кінцівки, нерухомість внаслідок анкілозів у суглобах кінцівки та інші дефекти. Однак, закон передбачає лише знівечення обличчя, яке може статися внаслідок механічних його ушкоджень, опіків полум’ям, струмом, корозивними хімічними сполуками, радіаційних уражень тощо.

Ми вважаємо, що для усунення зазначених протиріч необхідно доповнити відповідний розділ Правил 1995 р. вказівкою на анатомічні межі обличчя (враховуючи і вушні раковини), визначенням поняття “знівечення”, роз’ясненням, хто і яким чином повинен встановлювати міру спотворення обличчя і кінцевий ступінь тяжкості тілесного ушкодження. Якщо знівечення обличчя – загальнолюдське, побутове, естетичне поняття, то чому правознавці можуть і мають право на визначення непоправних наслідків ушкодження обличчя його знівеченням, а лікар – судово-медичний експерт, який має спеціальну медичну підготовку, вивчав і знає анатомію, фізіологію і функцію обличчя і його окремих органів і частин, володіє тими самими

загальнолюдськими поняттями про спотворення органів і тканин, позбавлений права допомогти правоохоронним органам чи суду правильно визначити наявність або відсутність знівечення обличчя у потерпілої особи [23]?

За нашим обґрунтованим переконанням, для усунення процесуальних суперечок потрібно передбачити у Правилах 1995 р. право судово-медичного експерта визначити остаточно ступінь тяжкості тілесного ушкодження у випадках явного безсумнівного післятравматичного знівечення обличчя.

Російські науковці В. Векселенко, М. Галюкова виділяють ще один із можливих наслідків тяжкого тілесного ушкодження – патологічний стан. В медичній літературі його визначають, як стійке відхилення від норми, що має біологічно негативне значення для організму [24]. Або, цей термін використовують у більш широкому розумінні – для позначення наявних тимчасових, перехідних відхилень незалежно від їхньої тривалості. Часто патологічний стан є наслідком раніше перенесених травм або захворювань [6]. Крім того, як зазначено у коментарі до КК РФ, патологічний стан, захворювання та тілесні ушкодження – це небезпечна для життя шкода здоров'ю [25, с. 251]. Таку позицію підтримують і інші російські науковці та відзначають, що шкода здоров'ю містить у собі тілесне ушкодження як найбільш яскраво виражену травматичну форму розладу здоров'я, поряд із захворюванням і патологічним станом – поняттями, прийнятими для позначення патологічних змін, що не є тілесними ушкодженнями [26, с. 5].

Російський законодавець, російські вчені [6] та білоруські науковці [27, с. 8-9], виділяють ще один із наслідків тяжкого тілесного ушкодження, який невідомий теорії та практиці кримінального права – це захворювання на наркоманію та токсикоманію. Можна погодитися з думкою науковців та позицією російського законодавця, що захворювання на наркоманію та токсикоманію внаслідок примусового вживання наркотичних засобів та подальшого розвитку у потерпілої особи хворобливої залежності, слід розглядати як один із суспільно небезпечних наслідків тяжкого тілесного ушкодження.

Критерії тілесних ушкоджень середньої тяжкості в ст. 122 КК України не рівнозначні, але головними з них є ушкодження, що спричинили тривалий розлад здоров'я, та такі, які викликали значну стійку втрату працездатності менш, як на одну третину. Це вимагає більш чіткого роз'яснення у Правилах 1995 р. поняття “розлад здоров'я”, його відмінності від тимчасової, короткочасної чи стійкої втрати працездатності. Оскільки законодавець увів у ст. 122 КК України термін “значна стійка втрата працездатності”, то і відповідний пункт Правил 1995 р. вимагає зміни редакції [15]. Правила повинні дати чітку вказівку експерту, яким директивним документом України слід користуватися при визначенні розмірів стійкої втрати загальної працездатності, вказівка на необхідність керуватись документами МСЕК носить загальний характер.

Дискусійними також є питання юридичної та медичної кваліфікації ознак легких тілесних ушкоджень. По-перше, визначення легкого тілесного ушкодження (ч. 1 ст. 125 КК України) у Правилах 1995 р. містить незрозумілу термінологію. Так, легке тілесне ушкодження, що не спричинило короткочасного розладу здоров'я чи незначної стійкої втрати працездатності, – це ушкодження, що має незначні скороминущі наслідки, тривалістю не більш як шість днів. Правилами 1995 р. не уточнено, що належить розуміти під словосполученням “незначні скороминущі наслідки”. Формальна логіка підказує, що якщо у ч. 2 ст. 125 КК України йдеться про “легке тілесне ушкодження, що спричинило короткочасний розлад здоров'я...”, то у ч. 1 цієї ж

статті мається на увазі легке тілесне ушкодження, що не спричинило короткочасного розладу здоров'я. Отже, ч. 1 ст. 125 КК України правильно було б викласти в наступній редакції: “Умисне легке тілесне ушкодження з відсутністю розладу здоров'я”.

Виходячи із провідного принципу верховенства закону (КК України) над підзаконними актами (у даному випадку Правилами 1995 р.), слід тлумачити в останніх “легкі тілесні ушкодження” як такі, що не викликають у будь-якої особи розладу здоров'я чи тимчасової втрати працездатності. Так їх і треба зазначити у Правилах 1995 р. Якщо ж ушкодження супроводжувалось чи викликало розлад здоров'я, то незалежно від його терміну (але не більш як на 21 день), воно повинно оцінюватись як легке тілесне ушкодження з короткочасним розладом здоров'я. По-друге, у ч. 2 ст. 125 КК України “незначну втрату працездатності” потрібно замінити на “незначну стійку втрату загальної працездатності”, адже однією з ознак тяжкого (ч. 1 ст. 121 КК України) та середньої тяжкості тілесного ушкодження (ч. 1 ст. 122 КК України) законодавець визначає саме розлад здоров'я, поєднаний з стійкою втратою працездатності, тобто в обох випадках використовує термін “стійка”.

При визначенні тривалості тимчасового розладу здоров'я експерт зобов'язаний керуватись терміном, необхідним для видужання чи загоєння ушкоджень при їх звичайному перебігу, виходячи із загальномедичних показників. Така оцінка легких тілесних ушкоджень буде цілком відповідати змісту диспозиції ст. 125 КК України, а також медичним положенням щодо впливу механічної чи іншої травми на функціонування різних систем організму та його реакцій на неї. Тілесне ушкодження або викликає розлад здоров'я або ні. Розлад здоров'я до 6 діб все ж є розладом і його треба враховувати. Зазначений підхід до оцінки легких тілесних ушкоджень сприятиме ще й боротьбі зі злочинами, спрямованими проти здоров'я людини.

### **Висновки.**

Дослідження сучасного законодавства України щодо ознак тілесних ушкоджень свідчить про те, що підзаконні нормативно-правові акти у цій сфері не повною мірою відповідають положенням чинного КК України.

Вважаємо, що юридичні критерії тяжких тілесних ушкоджень у Правилах судово-медичного визначення ступеня тяжкості тілесних ушкоджень від 1995 р. повинні максимально точно відповідати диспозиції ст. 121 тексту чинного КК України. Це стосується й диспозицій інших статей щодо злочинів проти життя та здоров'я особи.

З метою подальшого удосконалення законодавства України пропонуємо розробити нормативно-правовий акт для встановлення розмірів стійкої втрати загальної працездатності і затвердити разом із змінами до Правил судово-медичного визначення ступеня тяжкості тілесних ушкоджень від 1995 р. (у новій, адаптованій до положень КК України редакції) як єдиний документ.

### **Використана література**

1. Загородников Н.И. Преступления против здоровья / Н.И. Загородников. – М. : Юридическая литература, 1969. – 166 с.
2. Киренко С.Г. Проблеми захисту прав неповнолітніх кримінальним законодавством України : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.08 – “Кримінальне право та кримінологія; кримінально-виконавче право” / С.Г. Киренко – К. : Національний педагогічний університет ім. М.П. Драгоманова, 2002. – 200 с.

3. Дубовец П.А. Ответственность за телесные повреждения по советскому уголовному праву / П.А. Дубовец. – М. : Юридическая литература, 1964. – 159 с.
4. Шарапов Р., Коновалов А. Понятие вреда здоровью в условиях правовой дезориентации судебно-медицинской экспертизы живых лиц // Уголовное право. – 2007. – № 1. – С. 127.
5. Авдеев М.И. Преступления против личности уголовно-правовая терминология // Правоведение. – 1979. – № 2. – С. 89.
6. Векселенко В., Галюкова М. Уголовно-правовой анализ понятия “вред здоровью” // Уголовное право. 2007. – № 1. – С. 7 – 11.
7. Борзенков Г.Н. Преступления против жизни и здоровья : закон и правоприменительная практика : учебно-практич. пособие / Г.Н. Борзенков. – М. : Зеркало, 2008. – 256 с.
8. Пионтковский А.А. Курс советского уголовного права. Особенная часть / А.А. Пионтковский, В.Д. Меньшагин. – Т. 1. – М., 1955. – С. 569.
9. Никифоров А.С. Ответственность за телесные повреждения по советскому уголовному праву / А.С. Никифоров. – М., 1959. – 162 с.
10. Правила судово-медичного визначення ступеня тяжкості тілесних ушкоджень МОЗ України : Наказ Міністерства охорони здоров'я України від 17.01.95 р. № 6. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/z0255-95>
11. Єдиний державний реєстр судових рішень : Постанова Збарзького районного суду Тернопільської області від 10.10.16 р. № 598/922/13-к. – Режим доступу : <http://www.reyestr.court.gov.ua/Review/61887922>
12. Про психіатричну допомогу : Закон України від 22.02.00 р. № 1489-III // Відомості Верховної Ради України (ВВР). – 2000. – № 19.– Ст. 143. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/1489-14>
13. Про судову практику у справах про зґвалтування та інші статеві злочини : Постанова Пленуму Верховного Суду України від 27.03.92 р. № 4. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/v0004700-92>.
14. Про судову практику у справах про злочини проти статевої свободи та статевої недоторканості особи : Постанова Пленуму Верховного Суду України від 30.05.08 р. № 5. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/v0005700-08>
15. Завальнюк А.Х. Про необхідність внесення корективів у правила кваліфікації тяжкості тілесних ушкоджень // Український судово-медичний вісник. – 2004. – № 2(16). – С. 32-34.
16. Расследование и предупреждение телесных повреждений / [Н.Е. Быховский и др.] ; отв. ред. Н.И. Гуковская. – (Всесоюзный ин-т по изучению причин и разработке мер предупреждения преступности). – М. : Юридическая литература, 1964. – 98 с.
17. Гродзинский М.М. Преступления против личности / М.М. Гродзинский. – М., 1924. – 68 с.
18. Шаргородский М.Д. Ответственность за преступления против личности / М.Д. Шаргородский. – Л., 1953. – 120 с.
19. Векселенко В., Галюкова М. Психическое расстройство как признак причинения вреда здоровью // Уголовное право. – 2005. – № 2. – С. 22-23.
20. Ной И.С. Критерии умышленного тяжкого телесного повреждения без отягчающих обстоятельств по УК РСФСР // Ученые записки Саратовского юридического института им. Д.И. Курского. – Вып. VIII. – Саратов, 1959. – 143 с.
21. Кривда Г.Ф., Плевинскис П.В. Проблемные вопросы регламентации проведения комиссионных судебно-медицинских и комплексных экспертиз в отделе комиссионных экспертиз бюро СМЭ // Судово-медична експертиза. – 2014. – № 2. – С. 9-11.
22. Авдеев М.И. Судебно-медицинская экспертиза живых лиц / М.И. Авдеев. – М. : Медицина, 1968. – 376 с.

23. Завальнюк А.Х., Юхимець І.О., Кравець О.Ф. Судово-медичні погляди на оцінку непоправних наслідків травмування обличчя // Судово-медична експертиза. – 2016. – № 1. – С. 31-34.

24. Большой медицинский словарь. 2000. – Режим доступа : <http://dic.academic.ru/dic.nsf/medic2/33927>

25. Коряковцев В.В. Комментарий к Уголовному кодексу Российской Федерации / В.В. Коряковцев, К.В. Питулько. – [2-е изд.]. – СПб. : Питер, 2006. – 256 с.

26. Попов В.Л. Судебно-медицинская экспертиза тяжести вреда здоровью / В.Л. Попов. – СПб., 1999. – 40 с.

27. Терещенко Т.Г. Умышленное причинение тяжкого телесного повреждения: уголовно-правовая и криминологическая оценка : автореф. дис. на соискание ученой степени канд. юрид. наук : 12.00.08 – “Уголовное право и криминология; уголовно-исполнительное право” / Т.Г. Терещенко. – Минск : Академия Министерства внутренних дел Республики Беларусь, 2013. – 23 с.

~~~~~ \* \* \* ~~~~~

УДК 342.733

ШЕЛЯЖЕНКО Ю.В., магістр права, аспірант,
Університет економіки та права “КРОК”

МОНОПОЛІСТИЧНА НАУКОМЕТРІЯ З ТОЧКИ ЗОРУ АКАДЕМІЧНОЇ СВОБОДИ ТА БЕЗПЕКИ

Анотація. У статті аналізуються правові, політичні та економічні проблеми адміністративно-командного нав'язування вченим монополістичної наукометрії. Виявлено ризики для академічної свободи та безпеки, національних інтересів України, особистої автономії науковців. Запропоновані шляхи безпечного розвитку наукометрії в Україні.

Ключові слова: наукометрія, академічна свобода, інформаційна безпека, наукова творчість.

Аннотация. В статье анализируются правовые, политические и экономические проблемы административно-командного навязывания ученым монополистической наукометрии. Выявлены риски для академической свободы и безопасности, национальных интересов Украины, личной автономии исследователей. Предложены пути безопасного развития наукометрии в Украине.

Ключевые слова: наукометрия, академическая свобода, информационная безопасность, научное творчество.

Summary. The paper analyzes legal, political and economic issues of administrative and command imposition of monopolistic bibliometrics on scientists. Risks are revealed to academic freedom and security, to national interests of Ukraine, to personal autonomy of scientists. Ways for the safe development of bibliometrics in Ukraine are suggested.

Keywords: bibliometrics, academic freedom, information security, science citation.

Постановка проблеми. Академічна свобода та безпека, тобто можливість здійснювати наукові дослідження і поширювати знання без втручання та перешкод, сьогодні перебуває під загрозою навіть у найбільш благополучних країнах. Автономія індивідуальних дослідників та науково-дослідницьких інституцій обмежується фінансовими та адміністративними рішеннями, які нав'язують вченим спірні дисциплінарні регуляції. Необхідно досліджувати такі рішення, їх причини, наслідки, супутні ризики та способи відвернути небезпеку. Зокрема, в Україні постає питання правомірності, пропорційності та доцільності примусу науковців публікуватися в престижних, за певними міжнародними рейтингами, виданнях.

Метою статті є аналіз вимог публікації результатів наукових досліджень у виданнях, які індексуються глобальними монополістичними наукометричними (бібліометричними) системами.

Виклад основного матеріалу. Наукометрія, або бібліометрія є статистичною дисципліною, що вивчає кількісні показники наукової активності, зокрема, публікацій та слугує інструментом наукової політики, прийняття управлінських, кадрових, фінансових рішень. Тотальний облік науковців, в т.ч. з питань політичної лояльності, почала академічна комісія “Наука в России” у 1916 – 1934 рр. Прагнучи не відставати від комуністів у фінансуванні та контролі науки, уряд США у 50-х рр. ХХ ст. для оцінки ефективності використання науковцями грантових коштів підтримав проект, в рамках якого було розроблено теоретичні засади наукометрії та почалося створення найвпливовішої нині міжнародної наукометричної бази Web of Science.

Чинний Порядок присвоєння вчених звань науковим і науково-педагогічним працівникам, затверджений наказом Міністерства освіти і науки України від 14.01.16 р. № 13 [1], встановлює такі кваліфікаційні вимоги для присвоєння вчених звань професора, доцента, старшого дослідника, як наявність публікацій у періодичних виданнях, які включені до наукометричних баз Scopus або Web of Science. Окрім того, наказом МОНМС “Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук” від 17.10.12 р. № 1112 [2] від дисертантів вимагається наявність публікацій у наукових періодичних виданнях інших держав або публікацій у виданнях України, які включені до міжнародних наукометричних баз. З іншого боку, статтями 34, 54 Конституції України, статтею 46 Закону України “Про наукову і науково-технічну діяльність” гарантується свобода поширення інформації та свобода наукової творчості, особиста автономія науковців посилена ст. 10 Конвенції про захист прав людини і основоположних свобод і ст. ст. 19, 27 Загальної декларації прав людини.

Можна зрозуміти зацікавленість авторитетних кіл у прозорості, доброчесності та продуктивності науки і освіти в Україні, однак цей їхній інтерес має бути збалансований з імперативом академічної автономії. Згаданим регуляціям, на думку автора, бракує такої збалансованості, оскільки навіть доступ до Scopus та Web of Science непосильно дорогий для багатьох українських ВУЗів і в цих наукометричних базах всі записи англійською, через що переважна більшість україномовних наукових публікацій не індексуються. Між тим, виключне становище, надане цим двом наукометричним базам Міністерством освіти і науки України в адміністративно-командному порядку, ставить їх та порівняно невелику кількість індексованих ними українських видань у монополне становище, що гальмує розвиток науки та оприлюднення результатів наукових досліджень і демотивує вчених користуватися доступними альтернативними глобальними та локальними наукометричними базами і створювати українські наукометричні бази.

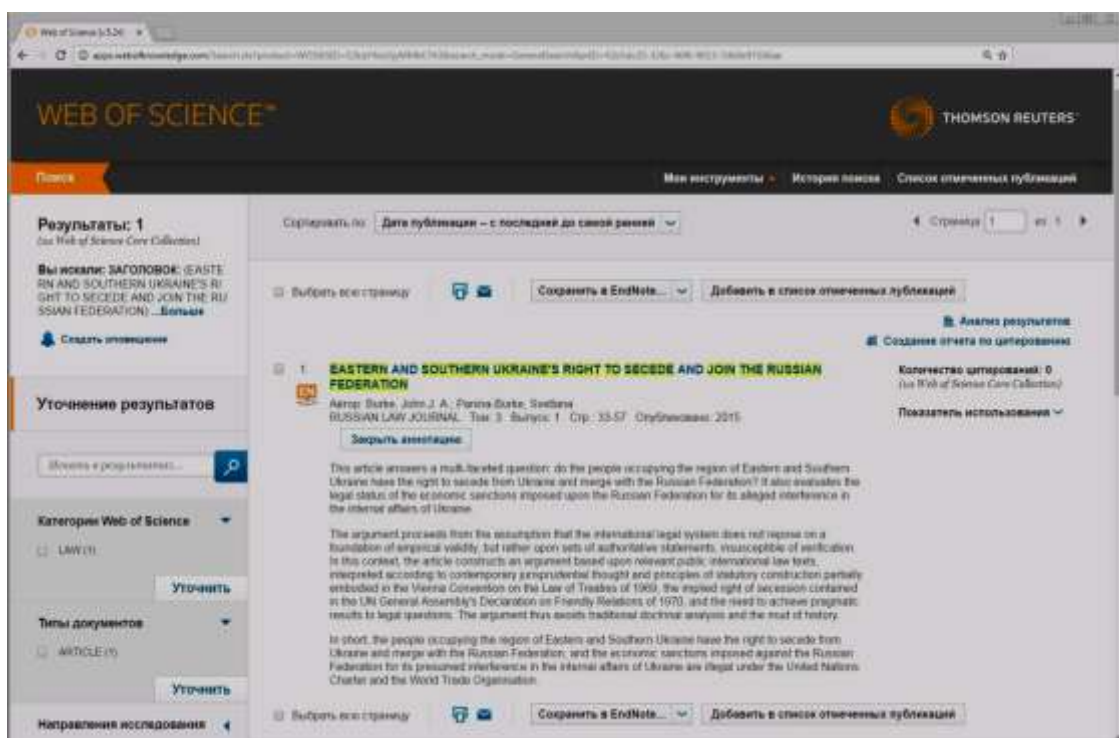


Рис. 1. Посилання на антиукраїнську статтю у Web of Science.

У багатьох галузях, таких, як юриспруденція, в Україні взагалі відсутні видання, що включені до цих наукометричних баз. Між тим, російські видання у галузі права індексуються, через що знаходимо у Web of Science відверто антиукраїнські публікації на зразок опублікованого “Російським правовим журналом” опусу Джона Бурке та Світлани Паніної-Бурке “Право східної та південної України від’єднатися та увійти до Російської Федерації”.

The screenshot shows the journal information page for "Право Донецкой Народной Республики" on the LIBRARY.RU website. The page includes a search bar, navigation menu, and detailed journal data. The journal is published by the Donetsk Academy of Internal Affairs. It has an ISSN of 10.00.00 and is categorized under "Государство и право, Юридические науки". The page also displays various metrics and a table of journal codes.

| Код | Раздел рубрикатора ГРНТИ | Журналов |
|----------|--|----------|
| 10.00.00 | Государство и право, Юридические науки | 1964 |

Рис. 2. “Науковий” журнал “ДНР” у РИНЦ (RSCI).

Оскільки для публікації результатів дисертацій використовуються й інші наукометричні бази, доцільно зазначити, що дедалі більшу загрозу навіть для національної безпеки України становить участь українських вчених у наповненні “Російського індексу наукового цитування” (РИНЦ, RSCI, Science Index), про включення до якого з гордістю повідомляють чимало українських наукових видань. Публікації у багатьох виданнях, що входять до РИНЦ, дійсно, більш доступні, ніж у Scopus та Web of Science, але краще вже орієнтуватися на Google Scholar, Index Copernicus, DOI, DOAJ, OpenAIRE чи інші західні ресурси, не тільки через західноєвропейський цивілізаційний шлях України, але й через сумнівний контент та нестабільність РИНЦ, до якого включене навіть сепаратистське видання “Право Донецкой Народной Республики”, тоді як 344 наукових видання, в тому числі, до редколегій яких входять відомі українські науковці, з цієї наукометричної бази у квітні 2017 року було виключено без пояснень із публічним ганебним навішуванням ярлика “сміттєві журнали” [3], замість відповіді на претензії було оприлюднено демагогічну заяву, підготовлену монополістичною Асоціацією наукових видавців і редакторів [4], а протестну петицію більш ніж 5,5 тис. науковців [5] проігнорували. Наукометрична база Scopus, судячи з документу Scopus Discontinued Sources List на сайті Elsevier.com, також непрозоро виключила 302 наукових журнали, в тому числі, українських (станом на

січень 2017 року, з бази було виключено українські журнали “Actual Problems of Economics”, “Corporate Board Role Duties and Composition”, “Corporate Ownership and Control”, “Metallurgical and Mining Industry” та “Risk Governance and Control Financial Markets and Institutions”), щоправда, у менш нестабільний спосіб порівняно з РИНЦ: хоча журнали перестали індексуватися, раніше проіндексовані публікації залишилися у базі.

Щоб зрозуміти проблеми з монополістичною наукометриєю, варто згадати, що це дуже нова (і, відтак, не перевірена часом) наука, що виросла на грантах, які видавалися урядом США з метою визначати політику наукових досліджень, і нині тісно прив’язана до купки транснаціональних корпорацій. Ірина Тихонкова, авторка пізнавальних вебінарів та прикладних публікацій про наукометричну базу Web of Science, справедливо констатує, що серед індексованих в ній українських видань відсутня наукова література з суспільних та гуманітарних наук [6; 7]. Також вона зазначає, що ця база була першою в світі і її створив Юджин Гарфілд за зразком переліку прецедентних судових рішень Shepard’s Citations. У оригінальній статті Гарфілда “Індекси цитування для науки: новий вимір документування шляхом асоціювання ідей”, опублікованій у Science у 1955 р. [8], йдеться про те, що Shepard’s Citations є приватним бізнесом, що систематизує американські судові прецеденти для використання в юридичній практиці з 1873 року, в тому числі, враховує зв’язки прецеденту з попередніми та наступними прецедентами, що особливо важливо тоді, коли судова практика міняється і прецедент діє по-новому чи взагалі втрачає силу. На основі цього успішного досвіду юридичної спільноти Гарфілд запропонував складати наукові довідники впливу (“імпакт-фактору”) окремих наукових публікацій, співставляючи їм наступні публікації, що на них посилаються. Такий імпакт-фактор, пише Гарфілд, має бути більш показовим, ніж інші індикатори наукової продуктивності, серед яких він називає кількість публікацій як показник впливовості вченого та кількість посилань і реферувань як показник впливовості журналу. Також у статті Гарфілда наведено приклад визначення імпакт-фактора однієї публікації на основі аналізу близько 500 публікацій в тому ж журналі за наступні 5 років, в яких знайшлося 23 посилання на обрану статтю.

Перша публікація Гарфілда не містить жодного натяку на створення глобальної наукометричної монополії. В ній описано простий метод аналізу взаємозв’язку публікацій, застосовний одним дослідником в межах одного журналу чи вузького напрямку наукових досліджень. Метод Гарфілда може автономно застосовувати будь-який вчений чи група вчених для бібліографічних досліджень та складання наукометричних баз даних за окремими напрямками досліджень, окремими осередками наукової інформації, окремими галузями науки, окремими науками, з локальним та глобальним охопленням. Наприклад, досліджуючи правові основи особистої автономії, автор самостійно створює міжнародну наукометричну базу даних публікацій на цю тему, і на це не витрачається надто багато зусиль, враховуючи, що через Web of Science, Google Scholar та каталоги центральних бібліотек України знайдено трохи більше сотні англомовних, півсотні російськомовних і кілька десятків україномовних релевантних публікацій, з яких можна виділити для прикладних цілей більш вузьке коло публікацій, що знаходяться у відкритому доступі, та провести дослідження їх імпакт-фактора в межах цього вузького кола, що корисно для розвитку наукових досліджень в даному напрямку і водночас не потребує надто багато зусиль від дослідника. Подібне наукометричне дослідження не зайве було б здійснювати кожному індивідуальному досліднику, готуючи список літератури для своєї статті, монографії, дисертації чи іншої

академічної праці, при цьому не прив'язуватися до монополій, але й користуватися всіма доступними бібліографічними та наукометричними ресурсами.

Скажімо, якщо малому університету не по кишені Web of Science, можна скористатися доступом до цієї бази в Національній бібліотеці ім. В.І. Вернадського чи домовитись про співпрацю з більш багатими університетами чи іншими академічними установами, які можуть собі дозволити розкіш передплати. Але й не варто зобов'язувати усіх дослідників працювати з конкретними наукометричними базами, цим може займатися частина наукової спільноти, тоді як решта вчених користуватиметься результатами їх досліджень. Накладення таких дисциплінарних зобов'язань вже не перший рік оспорується з точки зору академічної свободи та безпеки.

Стів Фулер зазначає [9], що Гарфілд і його грантодавці з новоствореної, на той час, Американської Національної Наукової Фундації, ставили собі за мету запровадити в США систему керування наукою за комуністичними адміністративно-командними зразками, оскільки бюрократичний утилітаризм СРСР викликав захоплення частини наукових менеджерів, які не надто переймалися моральними цінностями академічної автономії. Критикуючи монополістичну наукометрію, Фулер вказує на такі її недоліки, як брак економічної чутливості, самореференційність (однобоку концентрацію на обраному сегменті джерел інформації), а також створення штучних бар'єрів для наукової кар'єри – починаючи науковці в умовах зцементованого наукометрією консервативного елітизму “мають бути відповідної статі (особливо у природничих науках), мають закінчити правильний університет, працювати з правильним керівником над правильною темою, отримати гарну роботу і грант, публікуватися в правильних журналах тощо”. Фулер зазначає, що зневага до показників інноваційності та практичної користі наукових досліджень на користь формально-кількісної наукометрії призводить до імітації науки, росту кількості непотрібних публікацій, і нагадує про негативний досвід Іспанії, яка у середні віки витратила багато золота на створення потужної системи 32-х університетів, залежних від держави та церкви, з сумними результатами. Через нові стандарти “суспільства знань” тільки доктори могли посідати ключові адміністративні та церковні посади. У країні видавалося найбільше в світі академічних публікацій, більшість з яких були непрактичними схоластичними синтезами. Цей позірний академізм без академічної автономії парадоксально співіснував із винищенням інакомислячих Трибуналом Священної Канцелярії Інквізиції і може розглядатися як курйозний історичний приклад імітації науки за формальними ознаками в умовах тотального невігластва, гальмування науково-технічного прогресу.

Критика Фулера не є поодинокую. Про небезпеку згубного впливу елітистсько-технократичного диктату в бюрократичному управлінні, позбавленому гуманістичної моральної основи, на початку 90-х років минулого століття попереджав академік Володимир Копейчиков у монографії “Народовладдя і особистість” [10]. Олексій Картунов та Олег Маруховський у монографії “Інформаційне суспільство: аналіз політичних аспектів зарубіжних концепцій” вказують, що світову демократичну спільноту не можуть не турбувати спроби правлячого класу окремих держав з імперськими амбіціями скористатись досягненнями інформаційної революції та революції знань, а також бурхливим, по суті, вибуховим розвитком інформаційно-комунікаційних технологій для встановлення свого віртуального і реального світового панування [11]. У термінології Аджемоглу і Робінсона [12], монополістичну наукометрію можна назвати екстрактивним інститутом глобальної політики, що гальмує розвиток науки, на відміну від бібліографічних ресурсів з відкритим доступом до поповнення та пошуку в них, які є інклюзивними і стимулюють академічний розвиток.

Через ту саму систему Web of Science можна знайти чимало свіжих (за 2017 рік) публікацій, в яких висловлюється стурбованість прагненням бюрократів упослідити академічну автономію. Наприклад, Сімілі-Майкл та Халдіман у статті “Сталість досліджень фотосинтезу – в умовах, коли дослідження ускладнюються культом аудиту та менеджменту” [13] зазначають, що стабільності наукових досліджень загрожує бюрократична система, яка, віддаючи перевагу короткостроковим утилітарним цілям і плазуючи перед тенденційно витлумаченими “ринковими законами”, ставить під загрозу університетську автономію, насаджує “вимірювання” наукової “продукції” і відповідно розроблені політики фінансування і критерії найму/звільнення/просування по службі, які призводять до гонитви за формальними показниками, полювання на гранти, зміни в практиці публікації і придушення неортодоксальних ідей. Така система гальмує дослідження, створює антагонізм, спрямовує потенційно творчого дослідника геть від оригінальності і відкриттів, позбавляє вчених задоволення від наукової праці і відчужує плоди цієї праці – застерігають науковці.

Привертає увагу доповідь Норвезької асоціації дослідників (нагадаємо, що Норвегія займає перше місце в рейтингу людського розвитку ООН) під промовистою назвою “Академічна свобода під тиском” [14], де вказано, що ключовим елементом академічної свободи є право публікувати результати досліджень у самостійно обраних каналах комунікації, і ця академічна свобода підривається посиленням регуляторних вказівок у норвезьких інституціях щодо того, де і як дослідження мають публікуватися.

Можна зауважити, що подібна критика іноді грішить нехтуванням справедливими міркуваннями економічної доцільності та менеджменту. Але якщо вже мова йде про це, не менш справедливо нагадати про високу вартість і доступність лише небагатьом обраним повноцінної освіти в сфері менеджменту, відсутність масової культури менеджменту, який нині є дисципліною інтенційно елітистською, умисно езотеричною, подібно до наукометрії. Відтак, можна зрозуміти позицію частини науковців, які вважають ці дисципліни псевдонауковими, адже супутній академічним активностям у цих сферах елітизм є явищем, що корумпує науку і є нетерпимим з точки зору егалітарної ліберальної моралі.

На Заході, де цінності індивідуальної свободи є традиційно міцними в широких масах, а не тільки серед правлячого класу (який у нас ще й провокаційно заперечує ці цінності на публіці, сповідуючи їх всім своїм способом життя), культура менеджменту нині переросла вузьку корпоративність і поступово стає фундаментом особистої автономії, загальнодоступним мистецтвом підвищення особистої ефективності, самодисципліни, самовираження, саморозвитку, самоорганізації та самоуправління.

Демократизація, децентралізація та демонополізація менеджменту на Заході призвела до розвитку культури Open Source (відкритих джерел), в основі якої лежить ідея, що підтримка новацій має бути добровільною, щоб новатори та інвестори новацій могли отримати винагороду і думати про майбутнє, але не могли нав’язувати суспільству своє технічне рішення як безальтернативне та гальмувати подальший розвиток науки. Орієнтований на Open Source науковий менеджмент цілком відповідає традиційній українській “філософії серця”, суть якої правник Памфіл Юркевич висловив у такому міркуванні: індивідуальна воля є спільний гаразд, якщо тільки не пригноблює волю інших [15]. Це міркування Юркевича близьке до вислову одного з фундаторів американської психології та філософії прагматизму Вільяма Джеймса, який у знаменитій лекції про великих людей стверджував, що суспільство завмирає без особистої ініціативи, а особиста ініціатива вмирає без підтримки суспільства [16].

Відтак, можна погодитись із Кліффордом Татумом та Полем Вотерсом, які у статті “Бібліометрика та культура відкритого доступу” [17] вказують на ріст запиту академічної спільноти на бібліографічні та наукометричні сервіси Open Source. Цей запит вже зараз частково задовольняється відкритими для доступу через Інтернет каталогами українських та зарубіжних бібліотек, в тому числі електронних бібліотек та архівів академічних праць вищих навчальних закладів, відкритими каталогами публікацій, соціальними науковими мережами, користувачі яких можуть самостійно завантажувати свої праці та цитування, на зразок Academia.edu та CiteULike. У маніфесті наукометричної системи Altmetrics зазначається, що рецензування та публікація у вузькому колі престижних журналів, облік цитувань як метод оцінки впливу окремих публікацій вже неактуальні в сучасному світі, де науковець може просто поділитися ідеєю в соцмережі та цим одразу вплинути на розвиток науки; тому імпакт-фактор має включати оцінку використання (завантаження, перегляди) публікації, рецензування (експертну думку), цитування та альтернативні показники: поширеність, лінки, закладки, обговорення, тощо [18]. Кайван Куша та Майк Фелвел у збірці “Поза бібліометрикою: використання багатовимірних індикаторів наукового впливу” [19] наводять приклад автономної університетської наукометричної бази CiteSeer, першої автоматизованої системи індексації цитувань, яка адмініструється Університетом штату Пенсильванія і орієнтується, перш за все, на онлайнві публікації. На сайті Open Science in Ukraine перераховано [20] десятки цифрових сервісів для дослідників, 7 альтернативних наукометричних систем, а також наведено список українських журналів у Scopus та Web of Science. Навіть монополістична наукометрична система Web of Science не залишилась осторонь тенденцій відкритого доступу: вони пропонують відкритий доступ до безкоштовних вебінарів [21], книг [22] та інших інформаційних ресурсів з дохідливою пропагандою їхнього ексклюзивного підходу до оцінювання наукових праць.

Тенденції децентралізації наукометрії вбачаються не тільки у русі Open Source та створенні власних наукометричних ресурсів у Росії та Європейському Союзі, але й у історії з появою Scopus. Адже Web of Science свого часу була практично безальтернативною наукометричною базою, сформованою в інтересах грантодавців наукових досліджень, але політика оцінки журналів у Web of Science не задовольняла наукових видавців, і монополістичне видавництво наукової літератури Elsevier вдалося до створення власної бази Scopus. Не виключено, що свої наукометричні бази створять у майбутньому видавці країн третього світу, яких елітисти на Заході називають “хижаками” та “шахраями” і виключають з провідних наукометричних баз за надто доступні наукові публікації: у Web of Science можна знайти тези мультидисциплінарних конференцій з оргвнеском більше 300 доларів, тоді як участь у східноєвропейських мультидисциплінарних конференціях коштує від \$ 3 до \$ 30, максимум \$ 50. Проти видавничих та наукометричних монополій активно протестують західні науковці, з останніх прикладів можна навести публічну петицію 16 тис. вчених на сайті The Cost of Knowledge, які відмовляються користуватися продуктами та послугами монополістичного видавця Elsevier, власника Scopus, через нав’язування університетам дорогих пакетів послуг, небажання переходити на відкритий доступ, підтримку цензури Інтернету під виглядом “боротьби з піратством”.

У підсумку, українським вченим треба бути більш прагматичними – і це не означає гнатися за копійкою, як вважається у вульгарній трактовці прагматизму. Це означає, за словами фундатора філософії прагматизму Чарльза Пірса, судити про все на основі практичних проявів, завжди ставити питання “Яка з того користь?”. З точки зору прагматизму, ніхто не допоможе нам розбудувати українську науку, якщо ми самі не

будемо за власною ініціативою цим займатися, шукаючи і знаходячи користь від конкретних наукових результатів для індивідуальних дослідників, інституцій, бізнесу та суспільства в цілому. Полювання на плагіат та дріб'язкове вимірювання наукової продуктивності перестане бути потрібним, коли ми згадаємо, що практична користь, самостійність та результативність наукових робіт, а не дотримання бюрократичних формальностей має лежати в основі науки. Це потребує і зміни парадигми освіти: зараз освіта відірвана від наукового нормативу емпіризму і базується на механістичному насадженні стереотипних догм та способів мислення, демотивуючій формальній “оцінці знань” замість підтримки практичного самостійного здобуття знань. Прагматизм вимагає підтримувати особисту ініціативу в постановці корисних цілей та пошуку ефективних засобів досягнення своїх цілей, щоб мірилом успіху був лише об'єктивний результат, здатність людини самостійно та (чи) у групі досягнути поставленої практичної мети (у випадку освіти – мети пізнати те, що людині цікаво, в тому числі, краще зрозуміти власні інтереси, індивідуальні та спільні з іншими), а не відчужена оцінка знань авторитетними колами, яким іноді бракує альтруїзму, щоб радіти успіхам інших та ідеям реформ і не розглядати їх як посягання на свій авторитет.

Висновки.

Переваги глобальних монополістичних наукометричних (бібліометричних) систем, такі як широкий моніторинг та комплексна оцінка наукової активності, нівелюються суттєвими недоліками: дороговизною, непрозорістю, нестабільністю, відірваністю від галузевих та національних наукових контекстів. Політика зобов'язання вчених публікувати результати наукових досліджень у виданнях, які індексуються такими системами, вважаємо, є протиправною та небезпечною.

Для утвердження академічної автономії, свободи та безпеки наукових досліджень доцільно активізувати наукове спілкування як альтернативну бюрократичному менеджменту систему демократичного самоуправління української науки, не стільки на основі елітистської представницької демократії, скільки на основі егалітарної прямої демократії участі. Відходячи від пустопорожніх суперечок про формальності, треба бути вимогливими переважно щодо практичної результативності науки і залишити питання необхідної для цього самодисципліни на розсуд автономних суб'єктів академічного життя, щоб кожен з них міг самоорганізуватися та мобілізувати ресурси зручним та ефективним способом на власний розсуд, відповідно до власного устрою, досвіду та традицій. Маємо мислити широко і критично, не зациклюючись на особистих, корпоративних та національних інтересах, хоча і виявляючи належну повагу до всіх правомірних інтересів, і підтримувати локальний та глобальний науковий діалог та співпрацювати з усіма гідними академічними партнерами для досягнення практичних результатів, створення та впровадження наукових технологій на практиці.

У разі застосування наукометрії слід надавати перевагу ресурсам з відкритим доступом (open source) та українським ресурсам, а у разі браку чи недостатньої функціональності таких не лінуватися створювати та удосконалювати відповідні ресурси. Цей прагматичний підхід потребує поступової відмови на всіх рівнях, в тому числі на рівні державного регулювання, від застарілого, формалістичного застосування показників монополістичної наукометрії, децентралізації наукометричної інформації шляхом створення та розвитку наукометричних баз за окремими напрямками досліджень, джерелами та групами джерел, дисциплінами, галузями наук; децентралізовані наукометричні бази, в тому числі з міжнародним охопленням наукових публікацій, можуть створюватися, підтримуватися та розвиватися автономно індивідуальними дослідниками, науковими колективами, редакціями наукових журналів,

університетами, бібліотеками, академіями та іншими інституціями, в тому числі, при підтримці держави, приватних інвесторів та благодійників, як на міжнародних, так і зі створенням національних цільових та універсальних наукометричних платформ.

Водночас, не обов'язково повністю відмовлятися від монополістичної наукометрії; за наявності безпечного доступу до її ресурсів не зайве ними користуватися. Але необхідно з великою обережністю, бажано в мінімальному обсязі користуватися потенційно загрозливими для інформаційного суверенітету України наукометричними базами країни-агресора на зразок Російського індексу наукового цитування (РИНЦ, RSCI), який включає псевдонаукові видання угруповання “ДНР”.

Науковим установам варто визначити співробітників, відповідальних за наукометрію, просування наукових досліджень у рейтингові джерела, включення у рейтинги власних джерел наукової інформації, створення та підтримку власних наукометричних баз, пошук внутрішніх та зовнішніх ресурсів актуалізації та рейтингування наукових досліджень, а також індивідуально мотивувати вчених займатися наукометричними дослідженнями в добровільному порядку, без тотального державного примусу, в тому числі, користуватися впливовими західними монополістичними наукометричними базами Scopus та Web of Science (бажано, на західні ж грантові кошти – коли йдеться про платний доступ та про запуск українських видань, орієнтованих на включення в ці бази) і реагувати в порядку наукової критики та морального осуду на появу в цих базах псевдонаукових публікацій, спрямованих на підірив суверенітету та територіальної цілісності України.

Використана література

1. Про затвердження Порядку присвоєння вчених звань науковим і науково-педагогічним працівникам : наказ Міністерства освіти і науки України від 14.01.16 р. № 13 // Офіційний вісник України. – 2016. – № 17. – С. 167. – Ст. 693.
2. Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук : наказ Міністерства освіти і науки, молоді та спорту України від 17.10.12 р. № 1112 // Офіційний вісник України. – 2012. – № 86. – С. 250. – Ст. 3515.
3. Шеляженко Ю. Как РИНЦ выбросил мои исследования в мусорную корзину. – Режим доступу : <http://echo.msk.ru/blog/shelya/1969022-echo>
4. Почему было принято решение об исключении группы журналов из РИНЦ? – Режим доступу : http://elibrary.ru/retraction_faq.asp
5. Сотни тысяч научных статей должны быть возвращены в РИНЦ. – Режим доступу : <https://www.change.org/p/сотни-тысяч-научных-статей-должны-быть-возвращены-в-ринц>
6. Тихонкова І.О. Міжнародні бази даних наукової літератури Scopus, Index Copernicus, DOAJ, elibrary, російський індекс наукового цитування відкривають нові можливості для наукових журналів України. – (Досвід журналу “Biopolymers and cell”) / Наука України у світовому інформаційному просторі. – 2010. – № 3. – С. 27-32.
7. Тихонкова І.О. Наукова періодика України у дзеркалі Web of Science / Наука України у світовому інформаційному просторі. – 2016. – № 13. – С. 31-39.
8. Garfield E. Citation Indexes for Science. A New Dimension in Documentation through Association of Ideas / Science. – 1955. – Vol. 122. – No. 3159. – P. 108-111.
9. Фулер С. Що робить університети унікальними? Оновлення ідеалу для доби підприємництва / Дух і Літера : Університетська автономія (спеціальний випуск). – 2008. – № 19. – С. 195-221.
10. Копейчиков В.В. Народовластие и личность / В.В. Копейчиков. – К. : Україна, 1991. – 280 с.
11. Картунов О.В. Інформаційне суспільство : аналіз політичних аспектів зарубіжних концепцій : монографія / О.В. Картунов, О.О. Маруховський. – К. : Університет економіки та права “КРОК”, 2012. – 344 с.

12. Аджемоглу Д. Чому нації занепадають : походження влади, багатства та бідності / Д. Аджемоглу, Д. Робінсон. – К. : Наш Формат, 2016. – 440 с.
13. Tsimilli-Michael M. Sustainability of photosynthesis research – when research is impeded by the cults of audit and management / M. Tsimilli-Michael, P. Haldimann / *Photosynthetica*. – 2017. – Vol. 55. – Iss. 2. – P. 391-400.
14. The Norwegian Association of Researchers: Academic freedom under pressure. Key principles and trends / *Skriftserien*. – № 1/2017. – Режим доступу : https://www.forskerforbundet.no/Documents/skriftserien/2017-1_Academic_freedom.pdf
15. Юркевич П.Д. Історія філософії права. Філософія права. Філософський щоденник / П.Д. Юркевич. – К. : Український світ, 1999. – 756 с.
16. William James. *The Will to Believe; And Other Essays in Popular Philosophy*. – Auckland : The Floating Press, 2010. – 379 p.
17. Tatum C. *Bibliometrics and the Culture of Open Access [v0.1]* / C. Tatum, P. Wouters. – Режим доступу : <http://altmetrics.org/workshop2011/tatum-v0>
18. *Altmetrics: a manifesto*. – Режим доступу : <http://altmetrics.org/manifesto>
19. Kousha K. *Web Impact Metrics for Research Assessment* / K. Kousha, M. Thelwall. – (*Beyond Bibliometrics : Harnessing Multidimensional Indicators of Scholarly Impact*). – Cambridge : MIT Press, 2014. – P. 289-306.
20. Цифровые инструменты исследователей. – Режим доступу : <http://www.openscience.in.ua/ru/research-tools.html>
21. Информационный портал о работе на платформе Web of Science (TM). – Режим доступу : <http://wokinfo.com/russian>
22. *Руководство по наукометрии : индикаторы развития науки и технологии : монография* / [М.А. Акоев, В.А. Маркусова, О.В. Москалева, В.В. Писляков] ; под. ред. М.А. Акоева. – Екатеринбург : Изд-во Урал. ун-та, 2014. – 250 с.

~~~~~ \* \* \* ~~~~~

**До відома читачів:****РЕЦЕНЗІЯ**

на рукопис монографії кандидата юридичних наук, доцента Гребенюка М.В.  
**“Концептуальні засади забезпечення світової продовольчої безпеки:  
теорія і практика”**

У червні 2017 року видано друком монографію кандидата юридичних наук, доцента керівника Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України Гребенюка М.В. “Концептуальні засади забезпечення світової продовольчої безпеки: теорія і практика”.

Обрана тема наукового дослідження на монографічному рівні заслуговує на увагу також і тому, що в сучасному світі демократичність правової системи, до якої належить Україна, значною мірою обумовлена тим, яке місце займає в ній особа, як забезпечуються її інтереси, життя, здоров'я, честь, гідність, якими правами вона наділена, як вони захищаються. Можна констатувати, що автором у його роботі вдало розкривається зміст права людини на харчування та свободу від голоду в рамках проголошених світовою спільнотою міжнародно-правових зобов'язань. Загальновідомо, що сучасні процеси глобалізації вимагають від кожної держави активного входження у світовий економічний простір, який базується на загальноприйнятих інститутах. Це передбачає формування зовнішньоекономічної політики відповідно до багатосторонніх правил, які встановлені та застосовуються в рамках членства у різноманітних міжнародних організаціях, що є складовими глобального інституційного середовища. Саме потребою визначення для України гідного місця у світовій економіці насамперед і обґрунтовується необхідність проведення послідовної, адекватної та виваженої політики, орієнтованої на набуття Україною позицій світового лідера, що автоматично сприяє економічному зростанню країни, надає змогу очолювати процеси в контексті діяльності потужних міжнародних організацій. Насамперед, ці питання набувають актуальності для агропромислового комплексу, в якому вирішується глобальне питання сучасності – забезпечення продовольчої безпеки. Таким чином, розробка шляхів забезпечення продовольчої безпеки є важливим завданням сучасної науки, що досліджує процеси розвитку світового господарства. Забезпечення продовольчої безпеки у світі базується на створенні експортного потенціалу, успішної інтеграції в європейські та світові продовольчі ринки. Прогнозований і прозорий доступ до ринку продовольчих товарів і послуг та режим, дружній для прямих іноземних інвестицій, є одними з основних принципів системи економічних відносин в аграрному комплексі кожної національної економіки.

З огляду на це вступ до міжнародних організацій та подальша діяльність країн світу як їх членів до нинішнього часу є дуже важливим питанням, особливо в умовах розбудови сучасної світової системи боротьби з голодом та недоїданням. Саме це обумовлювало суперечливість вищезазначеного питання та необхідність його додаткового дослідження. З цієї точки зору поєднання в монографії глибокої теоретичної бази, її спрямованість на розгляд конкретних питань реалізації прав і свобод людини, визначення ролі та місця України в цьому процесі роблять представлену роботу актуальним та своєчасним науковим дослідженням.

У трьох взаємопов’язаних розділах автором висвітлюються концептуальні засади забезпечення світової продовольчої безпеки з урахуванням такого фактору, як формування нової поліцентричної міжнародної моделі, яка характеризується посиленням протиборства та масовим запровадженням з боку світової спільноти економічних санкцій з метою міжнародної ізоляції держави-агресора.

Цілком зрозуміло, що за логікою викладення матеріалу, у першому розділі розглядаються саме науково-теоретичні підходи до концептуальних засад світової продовольчої безпеки та робиться акцент на змістовному тлумаченні поняття “світова продовольча безпека”, визначаються її особливості в сучасних умовах соціально-правового розвитку. Далі в монографії досліджуються питання співвідношення змісту категорій “продовольча безпека” та “продовольча незалежність”, розкривається зміст забезпечення світової продовольчої безпеки в умовах глобалізації, визначається порядок здійснення оцінки стану забезпечення світової продовольчої безпеки.

Крім того, предметна увага на сторінках монографії приділяється взаємозв’язку в контексті діяльності міжнародних інституцій щодо удосконалення організаційно-правового механізму реалізації світової продовольчої безпеки. Висвітлюються особливості формування та використання міжнародного продовольчого резерву, надання та розподілу гуманітарної продовольчої допомоги у світі, здійснюється спроба розмежування сфер діяльності міжнародних організацій з визначенням їх окремих особливостей у рамках задекларованого міжнародно-правового становища. Саме сутність цих особливостей як соціальних регуляторів характеризує їх специфічні міжнародні засоби впливу на ступінь забезпечення всесвітньої продовольчої безпеки.

У проведеному дослідженні автором достатню увагу приділено питанням підвищення рівня продовольчої безпеки в Україні. Також у монографії знайшли своє відображення основні показники місця та ролі України в продовольчій світовій безпеці, які в залежності від часу, історичного, географічного, політичного простору, об’єктивних та суб’єктивних факторів суспільного життя істотно різняться між собою. Увагу читацької аудиторії акцентовано на тому, що інтеграція України до європейських та світових інституцій ставить перед нашою державою нові завдання, що передбачає, насамперед активізацію впровадження міжнародних стандартів та європейських регламентів й директив у сфері якості та безпечності харчових продуктів до вітчизняного законодавства.

Заслужує на увагу досить детальний аналіз правових аспектів вступу України в європейські та світові міжнародні інституції, зокрема, “ФАО – Україна”, а також розгляд питання щодо ратифікації Україною Конвенції про співробітництво у сфері забезпечення світової продовольчої безпеки, положення якої повинні визначати організаційно-правові засади, економічні механізми та стратегічні напрями міжнародного співробітництва держав за такими векторами: реалізація права людини на харчування, забезпечення безпеки харчових продуктів з метою гарантування здоров’я людини, збільшення обсягів постачання продовольчої гуманітарної допомоги.

При цьому в роботі підкреслюється важливість функціонування ООН як платформи, яка дає змогу координувати та схвалювати глобальні рішення, спрямовані на подолання голоду у світі, розглянуто вимоги Всесвітньої організації охорони здоров’я (ВООЗ) ООН, які формують стратегічні завдання для держав світу у сфері харчування та які потребують прискорення щодо вирішення, зокрема: наявність харчових продуктів у достатній кількості; доступність харчових продуктів для всіх

верств населення; безпечність харчових продуктів для здоров'я; раціональне харчування та вжиття усіх необхідних заходів для того, щоб ці положення діяли в реальному житті.

Результати та отримані висновки є досить аргументованими, їх правдивість зумовлена тим, що дослідження ґрунтуються на широкій джерельній базі, міжнародно-правових актах, ураховують національне законодавство окремих держав світу, у тому числі й України, стосовно проблеми інституційного та організаційно-правового становлення й розвитку сучасної моделі світової продовольчої безпеки та її складових. Викладення матеріалів монографії характеризується логічністю, структура роботи в достатній мірі оптимальна, і в цілому можна констатувати, що поставлена мета автором досягнута.

Наукова цінність монографії полягає в тому, що робота поєднує питання теорії і практики, є комплексним дослідженням фундаментальних положень міжнародно-правових актів, національного законодавства, які присвячені проблематиці забезпечення світової продовольчої безпеки та визначають результативність їх практичного впровадження у процесі подолання масштабів голоду, деталізують роль та місце України в цих процесах. Під час проведення дослідження автором використано офіційні статистичні дані, вітчизняні та зарубіжні наукові праці, публікації, результати соціологічних досліджень, що дає підстави відповідно до обраної парадигми наукової розвідки стверджувати про достовірність отриманих у монографії наукових положень, результатів і висновків. Репрезентативності проведеному Гребенюком М.В. компаративному дослідженню надає використання значної кількості іншомовних (переважно англomовних) джерел, що є неодмінною передумовою проведення порівняльно-правових пошуків на достатньо високому науковому рівні.

Практичне значення результатів і висновків роботи полягає в тому, що вони можуть бути використані для подальших досліджень загальнотеоретичних проблем розвитку правової системи України, вдосконалення інституту правового регулювання продовольчої безпеки України, подальшої гуманізації законодавства у цій сфері.

Дана монографія буде корисна як для фахівців у галузі загальних проблем права, так і практичним працівникам. Робота є сучасним виданням, а її положення можуть використовуватися в науково-дослідній та викладацькій діяльності. Вважається, що монографічне дослідження Гребенюка М.В. буде цікавим для широкого кола читацької аудиторії. Наукові положення, отримані автором монографічного дослідження результати поза сумнівом можуть бути використані у законотворчій та нормотворчій діяльності, передусім у частині внесення змін і доповнень до правових актів, які врегульовують питання гарантування якості та безпечності харчових продуктів.

Вивчення монографії Гребенюка М.В. “Концептуальні засади забезпечення світової продовольчої безпеки: теорія і практика” надає нам ґрунтовні підстави для висновку, що виконане автором дослідження відзначається науковою новизною й актуальністю, має теоретичну цінність і науково-практичне значення та може слугувати основою під час розробки проектів законодавчих та нормативно-правових актів з урахуванням кращих практик позитивного міжнародного й зарубіжного досвіду.

На наше переконання, монографічне дослідження Гребенюка М.В. робить суттєвий внесок у розвиток юридичної науки, є цікавим та змістовним. Підготовлена монографічна робота є цілісним дослідженням, яке з глибокою зацікавленістю буде сприйнята науковим товариством, вченими, політиками та державними службовцями.

Принаймні, обраний автором предмет дослідження, його інструментарій, отримані результати в частині розуміння сутності світової продовольчої безпеки, історичних передумов її виникнення та тенденцій розвитку, засобів становлення високого її рівня в нашій країні та участі України в забезпеченні світової продовольчої безпеки можуть бути віднесені до пріоритетних наукових проблем сьогодення.

Вважаємо, що рецензований рукопис монографії збагатить бібліотеку національних правових видань.

## **РЕЦЕНЗЕНТ**

доктор юридичних наук, професор,  
член-кореспондент НАН України,  
академік НАПрН України,  
заслужений юрист України,  
директор Інституту законодавства Верховної Ради України

**О.Л. КОПИЛЕНКО**

## До відома авторів

“ІНФОРМАЦІЯ І ПРАВО” – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів доктора і кандидата юридичних наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та пояснювати наукове вирішення визначених автором завдань згідно з такими основними напрямками досліджень, як:

**інформаційне право; правова інформатика, інформаційна і національна безпека.**

## Вимоги до оформлення

1) Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:

- у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;
- параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;
- відстань між рядками – 1 інтервал;
- кількість матеріалу однієї статті – не більше 15 стор.

Стаття має передбачати такі обов’язкові структурні елементи:

- УДК.
- Ім’я та прізвище, науковий ступінь, вчене звання автора, місце роботи.
- Назва статті.
- Анотація та ключові слова – укр., рос., англ. мовами.
- **Розв’язання проблеми**, шляхом наукового вирішення завдання:
  - **постановка проблеми** (загальна характеристика) та **результати аналізу наукових публікацій** (досліджень), в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття;
  - **формування мети** (постановка завдання) статті;
  - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
- **Висновки** за результатами розв’язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
- **Використана література** (згідно з наказом ВАК України від 26.01.08 р. № 63).
- Підпис, адреса (е-адреса), телефон автора.

2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- **Актуальність теми.**
- **Новизна та обґрунтованість одержаних наукових результатів.**
- **Наукова (практична) цінність результатів.**
- **Заключення про можливість відкритої публікації.**

- 3) Рукопис статті та Відгук мають бути ретельно вчитаними, виправленими і підписаними відповідними особами.**
- 4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України “Про затвердження порядку формування переліку наукових фахових видань України” від 17.10.12 р. № 1111.**
- 5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов’язаних з публікацією статей та виданням журналу, пропонується здійснити оплату в розмірі 280 грн. на рахунок Інституту.**

**Реквізити для оплати робіт:**

*Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).*

**Адреса редакції:** 01032, м. Київ, вул. Саксаганського, 110-В.

**Копію квитанції прохання направити на е-адресу:** [bvm777@ukr.net](mailto:bvm777@ukr.net)

**Д о у в а г и**

- Редакційна колегія не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
- Редакційна колегія залишає за собою право на:
  - відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
  - внесення до статті змін редакційного змісту у зв’язку зі скороченням обсягу матеріалу.

\* \* \* \* \*

# ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 2(21)

2017

|                                                |                                                                                                                                                                                                                                                               |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Засновники журналу:</b>                     | - Науково-дослідний інститут інформатики і права Національної академії правових наук України;<br>- Національна бібліотека України ім. В.І. Вернадського Національної академії наук України;<br>- Відкритий міжнародний університет розвитку людини “Україна”. |
| <b>Видавець:</b>                               | © Науково-дослідний інститут інформатики і права Національної академії правових наук України.                                                                                                                                                                 |
| <b>Адреса редакції:</b>                        | 01032, м. Київ, вул. Саксаганського, 110-В.<br>НДІ інформатики і права НАПрН України.<br>Тел.: 234-94-56; e-mail: bvm777@ ukr.net                                                                                                                             |
| <b>Веб-сторінки журналу у мережі Інтернет:</b> | //www.ippi.org.ua – НДІ інформатики і права НАПрН України;<br>//www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.                                                                                                                              |