

**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

№ 4(19)

2016

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;*

АРІСТОВА 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 філософії (Ph.D.) з юридичних наук, с.н.с.;

КОПАН Олексій Володимирович, доктор юридичних наук, професор;

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

КУЙБІДА 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

КОРЖ І.Ф. Зловживання правом на інформацію: сутність і форми.....	4
ЯРЕМЕНКО О.І. Теоретико-методологічні підходи до юридичної природи інформаційних відносин та їх типологізація.....	13
ПРИМАКОВ К.Ю. Семантичні та правові властивості масової інформації як об’єкту адміністративно-правового регулювання.....	22
РАДЗІЄВСЬКА О.Г. Дитина у глобальному інформаційному просторі: реальні та потенціальні загрози.....	29

Правова інформатика

ЛАНДЕ Д.В. Побудова моделей предметних областей з юриспруденції за даними сервісу Wikipedia.....	39
БРИЖКО В.М. Приватність даних у хмарних технологіях.....	47

Інформаційна і національна безпека

ПИЛИПЧУК В.Г., БРИЖКО В.М. Інформаційна безпека та приватність у сфері захисту персональних даних.....	60
КАЧИНСЬКА К.А. Засоби Інтернет-комунікацій як важливий інструмент масової маніпуляції свідомістю.....	71
СЕМЕНЮК О.Г. Державна таємниця як предмет злочину.....	85
БЄЛЄВЦЕВА В.В. Удосконалення відповідальності за правопорушення у сфері обігу комп’ютерної інформації.....	95

Інформація в інших галузях права

РАДУТНИЙ О.Е. Корупція – інформаційний образ ворога у Кримінальному праві України.....	100
ЛЕОНОВ, Б.Д., ЄВТУШЕНКО Є.В. Публічні закупівлі в електронній системі закупівель “ProZorro” за стандартами ЄС.....	107

До відома авторів	114
--------------------------------	------------

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.

Граматичне коректування – Майстренко І.А. (укр., англ.).

Формат 70 x 108/16. Спосіб друку – різнографія. Ум. друк. арк. 7.4. 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 № 11 від 15.12.16 р.

Інформаційне право

УДК 342.951

КОРЖ І.Ф., доктор юридичних наук, завідувач науковою лабораторією
НДІ інформатики і права НАПрН України

ЗЛОВЖИВАННЯ ПРАВОМ НА ІНФОРМАЦІЮ: СУТНІСТЬ І ФОРМИ*

Анотація. В статті досліджуються питання зловживання правом на інформацію в сучасному українському суспільстві, стан наукового дослідження зазначеної проблеми, розкривається її сутність та форми прояву, напрацьовуються правові механізми її вирішення.

Ключові слова: зловживання, інформація, нігілізм, обмеження, правовідносини, правопорушення, принципи.

Аннотация. В статье исследуются вопросы злоупотребления правом на информацию в современном украинском обществе, состояние научного исследования указанной проблемы, раскрывается ее сущность и формы проявления, наработываются правовые механизмы ее решения.

Ключевые слова: злоупотребление, информация, нигилизм, ограничения, правоотношения, правонарушение, принципы.

Summary. This article explores the issue of abuse of the right to information in the modern Ukrainian society, the state of scientific research of this problem, reveals its essence and forms, develops legal mechanisms to address it.

Keywords: abuse, information, nihilism, limitation, legal relationships, legal violation, principles.

Постановка проблеми. В сучасний період державотворення України, за якого рівень соціальних відносин в середині держави між її суб'єктами часто виходить за межу рівня критичної, інформація часто використовується суб'єктами інформаційних відносин як засіб впливу на суперників, як інформаційна зброя у боротьбі з політичними опонентами. Крім того, не гребують зазначеним і суб'єкти суспільних відносин в інших сферах – в економічній, банківській, бізнесовій, державній тощо. Саме зловживання інформацією, оперування нею без дотримання норм етики і моралі, стало однією з ознак сучасних інформаційних відносин в Україні, що завдає неабиякої шкоди суспільним правовідносинам та іміджу України, яка стала на демократичний шлях політичних і соціальних перетворень.

На відміну від таких публічних галузей права, як кримінальне, адміністративне тощо, де межі поведінки осіб чітко визначені нормативними приписами і зловживання однозначно є правопорушенням, оскільки порушують відповідні заборони, в інформаційному праві межі реалізації суб'єктивних прав у більшості випадків не формалізовані. Складнощі з кваліфікацією виникають саме тоді, коли законом не встановлено прямих заборони.

© Корж І.Ф., 2016

* Робота є продовженням досліджень за темою НДР “Науково-методичне, правове та інформаційне забезпечення формування національної інтегрованої системи нормативно-правових актів в умовах децентралізації в Україні”.

В нинішній час проблема зловживання правом на інформацію притягує увагу багатьох учених, практиків, нормотворців, і це не випадково. Сформульовані законодавцем теоретичні положення щодо недопустимості зловживання правом на інформацію на практиці породжують багато питань, пов'язаних з кваліфікацією згаданих дій у процесі реалізації окремими суб'єктами права на інформацію та зловживання ним. Зазначене породило ряд теоретичних суджень у цьому напрямку, що відображено у відповідних публікацій на дану тему. Існує ряд концептуальних та доктринальних підходів до даної проблеми, які кардинально протилежні за змістом. Однак досягти консолідованої позиції з даного питання дослідникам до цього часу ще не вдалося.

Сьогодні зловживання правом на інформацію в українському суспільстві набуло значної гостроти й є інформаційним феноменом, який часто виявляється в якості активного засобу боротьби з опонентами. Його наукове дослідження є відносно новим та вкрай актуальним для українського інформаційного права напрямком, який потребує нагального комплексного наукового дослідження.

Метою статті є визначення напрямів прояву зловживань правом на інформацію у соціальному середовищі, встановлення мотивацій їх суб'єктів, розкриття сутності цього явища і форм прояву, наслідків його впливу на процес побудови інформаційного суспільства і здійснюваної децентралізації державної влади в Україні та напрацювання відповідних пропозицій, у тому числі законодавчих, щодо запровадження механізмів мінімізації негативного впливу зазначеного на інформаційні відносини в державі.

Виклад основного матеріалу. Якщо говорити про “зловживання правом” загалом, то мова може йти про вжиття суб'єктивного права таким чином, що внаслідок цього суспільним відносинам завдається шкода.

Під зловживанням правом в наукових дослідженнях розуміється головним чином “шикана”, тобто здійснення суб'єктивного права з метою нанесення шкоди другій особі. “Шикана” в даному випадку є такою формою реалізації права, за якою суб'єкт її поширення не співвідносить свою поведінку з принципами розумності і добропорядності.

З другого боку – зловживання правом можна розглядати як протиправні дії, тобто як звичайне правопорушення.

Є думка дослідників, що зазначене може вважатися правомірною діяльністю, однак в даному випадку дана діяльність є аморальною.

Необхідно зазначити, що в наукових дослідженнях поняття “зловживання правом” суттєво відрізняється від поняття “протиправна діяльність”. До того ж випадки зловживання правом складніше розпізнати від випадків протиправної діяльності. Однак зловживання правом, в залежності від його мети, врешті-врешт може призвести до правопорушення. Водночас, якщо протиправна діяльність навіть формально не базується на праві і сама по собі є протиправною в чистому вигляді, то зловживання правом опирається на суб'єктивне право і формально не суперечить об'єктивному праву. Таким чином, якщо у особи немає суб'єктивних прав, зловживати правом вона не зможе. Водночас, вчинити протиправне діяння за відсутності суб'єктивних прав особа може.

Як зазначає Янев Я. [1, с. 181-182], “зловживання правом як явище включає в себе наступні елементи:

- наявність наданих суб'єктивних прав;
- використання цих прав у протиріччі з їхнім суспільним призначенням;
- таке здійснення суб'єктивних прав, яке ще не порушує конкретної, спеціальної правової норми з конкретним складом, конкретним змістом, яка знаходиться за межами загальної принципіальної правової норми, яка відмовляє в охороні і захисту дій, які перевищують межі реалізації цих прав, – норма, яка забороняє зловживання цими правами;

– порушення заборони здійснення чи використання наданих прав або використання їх таким чином, що їм відмовляється в охороні і захисту, про що говориться у відповідній загальній, принципіальній правовій нормі, однак без того, що самі ці дії є правопорушенням не дивлячись на те, що вони мають певну правову значимість;

– здійснення суб’єктивних прав в суперечності з їхнім суспільним призначенням незалежно від волі і свідомості уповноваженої особи чи від того, чи є ці “дії чи бездіяльність” навмисними чи з необережності, чи вони об’єктивно є протиправною наданим правам і покладеним обов’язкам, їх суспільному призначенню, чи направлені вони на те, щоб завдати шкоду іншим особам у власних інтересах чи інтересах другої особи, або не переслідують ніякого визначеного інтересу...”.

Ним же пропонується розрізняти зловживання правом, правомірну поведінку і правопорушення, вважаючи неправильною позицію тих дослідників, які вважають, що зловживання правом є правопорушенням.

Водночас, заслуговує на увагу позиція окремих дослідників, як це зазначає Кірюшкін Р.А. [2, с. 7], що не можна говорити про те, що зловживання – це не порушення конкретних норм права, а порушення принципів права, оскільки принципи права мають конкретний вираз в нормах права, а порушення норм права – це правопорушення, а не зловживання. Таким чином, зловживання має місце тоді, коли особа діє в рамках наданого їй суб’єктивного права; особа вибирає такі способи здійснення права на інформацію, внаслідок застосування яких може бути завдана шкода іншим суб’єктам інформаційних правовідносин, однак прямих заборон на використання таких способів здійснення права на інформацію у законі не передбачено.

Дискусійним серед науковців є і інший елемент об’єктивної сторони. Одні дослідники є прибічниками вчинення зловживання лише активними діями, а інші – як шляхом вчинення активних дій, так і шляхом бездіяльності [3].

Як зазначає Скакун О.Ф. [4, с. 427-429], зловживання правом – це особливий вид правової поведінки, який полягає у використанні громадянами своїх прав у недозволені способи, що суперечать призначенню права, внаслідок чого завдаються збитки (шкода) суспільству, державі, окремій особі. Пізніше нею зроблено наступне визначення – це особливий вид юридично значущої поведінки, яка полягає у соціально шкідливих учинках суб’єкта права, у використанні недозволених конкретних форм у межах дозволеного законом загального типу поведінки, що суперечить цільовому призначенню права. Таким чином зловживання правом є ненормальним (марним, незвичайним, шкідливим, аморальним) здійсненням права, що виражається в недозволених конкретних діях, які завдають шкоди іншій особі або загрожують чужому праву.

Скакун О.Ф. виділяє наступні ознаки зловживання правом:

- наявність в особи суб’єктивного права (зловживати можна тільки суб’єктивним правом);
- діяльність особи, що спрямована нібито на реалізацію цього права, видимість легальності поведінки; відсутність порушення конкретних юридичних заборон (їх додержання) чи невиконання обов’язків (їх виконання);
- використання недозволених засобів і способів здійснення права;
- здійснення права всупереч його соціальному призначенню;
- усвідомлення особою незаконності своїх дій, свідомий вихід за встановлені законом межі (наявність умислу);
- заподіяння шкоди (збитку) інтересам суспільства чи інтересам іншої особи;
- невиразність протиправної поведінки як юридичної ознаки правопорушення;

– нетрадиційність юридичних наслідків – відсутність юридичної відповідальності, що властива правопорушенню. Адже юридична відповідальність настає тільки у разі встановлення факту зловживання суб’єктивним правом, а це можливо, коли зловживання правом заподіює істотну шкоду інтересам, що охороняються законом.

Є й така позиція щодо зловживання правом. Так, Рогач О.Я. у своєму дослідженні [5, с. 253] зазначає, що зловживання правом у будь-яких проявах та видах є однією з форм правового нігілізму. Ним дана позиція аргументується тим, що здійснюючи зловживання правом, суб’єкт правовідносин порушує об’єктивні, зовнішні межі суб’єктивного права: свободи, права та інтереси інших осіб; призначення права, принципи добросовісності; розумності, справедливості, а також суб’єктивні, внутрішні, спеціальні межі його особистої, індивідуальної свободи, які відграють роль меж зовнішнього розсуду суб’єкта правовідносин. Вчиняючи зловживання правом, особа фактично проявляє свою неповагу до свобод інших осіб та права в цілому. Зловживаючи правом, особа скептично, зневажливо, зарозуміло сприймає право, не вірить у можливості і навіть необхідність права як найбільш ефективного регулятора суспільних відносин.

Необхідно зазначити, що правовий нігілізм є багатоліким. Злободенною реалією у сучасному світі правового нігілізму стали так звані “правовий егоїзм” і “подвійні стандарти”. В цих варіантах необхідність дотримання права і законності не заперечується: навпаки – вони декларативно і демонстративно вітаються. При цьому навіть щиро передбачається необхідність дотримання права і закону у суспільстві, проте із застереженням – вони існують для “інших”, для “бидла” тощо. Правовими нігілістами такого підходу виступають, як правило, “сильні світу цього”.

Оскільки протиправність поведінки як юридичної ознаки правопорушення при зловживанні правом явно не виражена, деякі учені не схильні кваліфікувати зловживання правом як правопорушення. Водночас вони не вважають таку поведінку і правомірною, оскільки остання є соціально корисною. Тому вони вважають, що зловживання правом слід віднести до правової поведінки, яка може набути протиправного характеру, стати правопорушенням, але не завжди ним стає. Критерієм оцінки зловживанням правом в рамках правової поведінки є буква закону, а протиправної – дух права. З огляду на зазначене можна навести одне із визначень терміну “зловживання правом”: “Це таке здійснення суб’єктивного права у суперечливості з його призначенням, внаслідок чого суб’єкт завдає шкоду іншим учасникам суспільних відносин” [6, с. 582]. Як видно з наведеного, зловживання правом можливе за умови наявності двох ознак – реалізація суб’єктивного права всупереч призначення права та завдання шкоди суспільним відносинам.

Одним із поширених різновидів зловживання правом в нинішніх умовах є зловживання правом на інформацію, які можна співвідносити як родові та видові поняття. Оскільки питання зловживання правом на інформацію в нинішніх умовах побудови інформаційного суспільства у країні набуло напрочуд актуального характеру, то дослідження механізмів та форм його прояву, а також нормативне врегулювання прогалин і колізій правових норм в галузі інформаційного права, існування яких і породжує згадане зловживання, є одним із невідкладних завдань як правової науки, так і нормотворців, насамперед законодавця.

Нинішні наукові дослідження в галузі інформаційного права, напрацьовані дослідниками висновки та рекомендації дають підстави констатувати, що зловживання правом на інформацію в нинішніх умовах набуло своєрідного лавинного характеру, за якого здійснюється масове порушення прав осіб, а самі порушники відчують певний

комфорт і відчуття вседозволеності. Таким чином особи, які здійснюють зловживання правом на інформацію, і свідомо, і несвідомо використовують сьогоденні правові можливості щодо отримання інформації, здійснюють зазначене не стільки в інтересах більшості суспільства, скільки йому на шкоду, як і на шкоду окремим особам суспільства. Зазначене викликає в українському суспільстві різку негативну реакцію і породжує у людей вимогу, яка набирає соціальної гостроти, щодо необхідності належного правового врегулювання зазначеної проблеми.

Відповідно до напрацьованих концептуальних положень, головною ознакою зловживання правом на інформацію є завдана шкода, як наслідок реалізації особою свого суб'єктивного права. Під суб'єктивними правами розуміються різнобічні права і свободи, владні чи посадові (службові) повноваження, недобросовісне використання яких дуже часто відбувається на практиці. Якщо шкода не була нанесена, то говорити про зловживанням правом на інформацію не доводиться.

Зловживання правом на інформацію здійснюється у відповідних формах, якими є:

- правомірні дії, пов'язані з реалізацією права на інформацію. Дані дії завдають шкоди інформаційним відносинам всупереч призначенню самого права;
- протиправні дії, які здійснюються особою, що реалізує свої права, свободи і владні повноваження, пов'язані з інформацією.

Як правомірні дії, пов'язані з реалізацією права на інформацію, вони є аморальними, недоцільними. Загальновизнано, що реалізація права, наприклад на інформацію, суб'єктами інформаційних відносин не повинна порушувати державні, приватні, громадянські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших суб'єктів інформаційних відносин. Так, у ст. 28 “Неприпустимість зловживання правом на інформацію” Закону України “Про інформацію” від 02.10.92 р. [7] зазначено, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Наприклад, аморальною є діяльність журналіста, який поширює у засобах масової інформації без зазначення свого авторства отриману неофіційними шляхами інформацію про висунуті проти когось звинувачення у правових порушеннях, які нібито були допущені відповідною особою, і які на даний час або ж перевіряються відповідними органами щодо їхньої достовірності, або ж не знайшли свого підтвердження. Тим самим особі завдається моральна шкода, підривається її професійний авторитет. І тут доцільно нагадати працівникам даної сфери положення статті 12 Закону України “Про державну підтримку засобів масової інформації та соціальний захист журналістів” від 23.09.97 р. [8] про специфічні риси їхньої роботи, яких вони мають дотримуватися, а саме: про суспільний вплив за наслідками їхньої роботи; про високу соціальну відповідальність за свою працю та її результати; про необхідність здійснювати власний творчий пошук нової потрібної інформації та її джерел тощо. Крім того, відповідно до статті 20 вказаного Закону [8] протиправні дії керівників недержавних організацій-засновників (співзасновників) засобів масової інформації та керівників самих засобів масової інформації, порушення ними норм цього Закону можуть бути оскаржені відповідно до Цивільного, Цивільного процесуального кодексів України та Кодексу України про адміністративні правопорушення з метою захисту порушеного або оспорюваного права чи охоронюваного законом інтересу, у тому числі і за опублікування інформації, що має за мету підірвати честь, гідність, професійний авторитет тощо фізичної чи юридичної особи.

Здійснюючи аморальні дії, зазначають дослідники [6, с. 585], суб’єкт зловживання правом не співвідносить свою поведінку з конкретно-історичним уявленням про добро і зло, хороше і погане, із загальнолюдськими цінностями, соціально визнаними нормами, які регулюють відносини людей один до одного, у сім’ї, в суспільстві, в державі, тобто суб’єкт діє аморально, безчесно, неблагородно.

Таким чином, зловживання правом на інформацію є недоцільне здійснення такого права, бо такі дії обмежують (утруднюють) можливість реалізовувати права і законні інтереси іншим особам. Наприклад, на Рівненщині одним громадянином було надіслано до Дубенської райдержадміністрації 300 запитів на публічну інформацію, що фактично паралізувало роботу структурного підрозділу, який надає відповіді на запитання [9]. Це трохи менше, ніж Адміністрація Президента України в середньому отримує за місяць. Для підтвердження факту зловживання ним правом на інформацію наведемо три з них:

- кількість безпритульних тварин, що знаходяться на території Дубенського району;
- поголів’я овець у Дубенському районі з 1991 – 2012 роки по роках;
- обсяги роздрібного товарообігу у районі поквартально в кожному з років за період з 1991 – 2012 роки.

Зазначимо, що Закон України “Про доступ до публічної інформації” від 13.01.11 р. [10] дає право будь-кому надсилати запити і не обмежує запитувача у їх кількості. Крім того, не вимагається ідентифікація запитувача (потрібно лише зазначити ім’я) і надається змога спілкування з органами державної влади через електронну пошту. Водночас, спроби працівників знайти автора звернення за зазначений ним телефоном чи вказаним адресом, завершилися невдало. Автор звернення так і не був знайдений за вказаним ним адресом.

Водночас, необхідно звернути увагу на наступний факт, що, за наявності явного зловживання громадянином правом на інформацію, працівники райдержадміністрації, мабуть, не повною мірою володіли знаннями положень Закону. Вони мали б надавати відповідь на запитання за умови наявності у них належної інформації лише за умови, зазначеної у ст. 1 згаданого Закону [10], тобто такої, що була отримана або створена в процесі виконання органом державної влади своїх обов’язків, або яка знаходилася у володінні. А судячи зі змісту запиту та поведінки працівників держоргану, згаданий орган міг і не мати такої інформації.

Наступним прикладом зловживання правом на інформацію є, наприклад, зловживання акціонерами акціонерного товариства наданими законом правом на отримання інформації, переслідуючи, зазвичай, мету:

- отримати документи, що містять таку інформацію, яка в подальшому може бути продана конкурентам або іншим зацікавленим особам;
- змусити акціонерне товариство викупити акції у акціонера за завищеною ціною (примусити здійснити гринмейл).

Зловживання акціонером правом на інформацію є одним із елементів стратегії корпоративного шантажу. Щоб змусити акціонерне товариство викупити акції акціонера за завищеною ціною, акціонер може подавати товариству численні запити щодо надання великої кількості документів. Українське законодавство не передбачає права акціонерного товариства відмовити акціонеру у наданні інформації, якщо інформація вже надавалася такому акціонерові. Тому запити про надання інформації акціонер може подавати хоч кожного місяця або ще частіше. Якщо акціонерне товариство не надасть документи на запит акціонера, це може бути підставою для накладення санкцій Національною комісією з цінних паперів та фондового ринку. На сьогоднішній день така практика дуже поширена.

Також значною є проблема недобросовісного використання інформації отриманої акціонером від товариства. Зазначені проблеми до цього часу не врегульовані законодавством [11]. На нашу думку, вирішення даної проблеми має бути здійснено законодавчим шляхом, що передбачає запровадження так званого кваліфікованого права на інформацію, тобто допускає ознайомлення акціонерів з документацією лише при доведеності того, що представлена ним інформація не буде використана на шкоду інтересам товариства.

Іншим шляхом вирішення згаданої проблеми є введення обмежень щодо:

- наявності необхідного попереднього терміну, протягом якого особи, які бажають отримати бажану для них інформацію, були акціонерами відповідних товариств;
- володіння певним відсотком випущених товариством акцій для отримання певної документації. Зазначені обмеження існують на практиці у багатьох країнах світу. Так в Угорщині, як зазначає експерт Ради Європи з Угорщини Балаш Тот [12], в 2015 році в Угорщині внесли зміни в закон про свободу доступу до інформації. Відповідно до цих змін, можна вимагати одну і ту саму інформацію лише раз на рік. Отже, якщо особа подає повторні запити стосовно тієї самої інформації, стосовно тієї ж самої теми і зміст інформації не змінюється, вона не має права на запит протягом одного року. Кількість людей, які зловживають в Угорщині цим правом, невелика.

Наступною формою зловживання правом на інформацію є, наприклад, перешкоджання в отриманні інформації, тобто зловживання обов'язком на забезпечення одержання відповідної інформації. Так, особі може бути відмовлено у наданні інформації члену товариства з підстав невизначених законом, або ж формально направляється заявнику поштою, але без належного змісту чи в такому вигляді, що зрозуміти інформацію неможливо.

Аналіз фактів зловживання правом на інформацію дозволяє зробити висновок, що проблема зловживання правом на інформацію не є однорідною, вона є різноманітною і може набувати різних форм свого прояву. Тобто, зловживання правом на інформацію можна поділити на певні підвиди, як то:

- зловживання правом на інформацію, яка знаходиться у суб'єкта у володінні (користуванні), тобто зловживання правом володіння (користування) інформацією;
- зловживання правом на доступ до інформації;
- зловживання правом на одержання інформації;
- зловживання правом на пошук і поширення інформації;
- зловживання правом на виробництво і розповсюдження інформації;
- зловживання правом на зберігання інформації;
- зловживання правом на захист інформації тощо.

Можна погодитися з думкою Рогач О.Я. про те, що зловживання правом на інформацію є певною формою правового нігілізму. Однак, будь-яке недотримання правових положень про інформацію є однією з відповідних форм правового нігілізму, як то:

- навмисне порушення законів та інших нормативно-правових актів;
- масове недотримання і невиконання юридичних приписів;
- видання суперечливих правових актів;
- підміна законності політичною, ідеологічною чи прагматичною доцільністю;
- конфронтацією представницьких і виконавчих органів державної влади;
- порушення прав людини, як то права на життя, честь, гідність, житло, майно, безпеку тощо;
- теоретична форма (у науковій сфері, в роботі юристів, філософів тощо) [13, с. 141-184].

Науковці пропонують наступні шляхи подолання правового нігілізму:

- реформи соціально-економічного характеру;
- зміна змісту правового регулювання, максимальне наближення юридичних норм до інтересів різних прошарків населення;
- підвищення авторитету правосуддя як за рахунок зміни характеру самої судової діяльності, так і шляхом виховання поваги до суду;
- покращенням правозастосовної практики;
- теоретичні напрацювання у цьому напрямку тощо. Все це разом являє собою процес покращення стану правової культури суспільств, її збагачення [13].

Одним із превентивних механізмів вирішення згаданої проблеми є механізм стримування зловживання правом. Він являє собою боротьбу не з поведінкою особи, яка зловживає правом, а з конкретними проявами правової поведінки, що завдають шкоди суспільству і особі. У разі встановлення факту зловживання правом воно не захищається і не охороняється законом. Залежно від обставин конкретної справи настають наступні наслідки зловживання правом: визнання його наслідків недійсними; заборона дій; припинення здійснення суб'єктивного права без його позбавлення тощо. Запобігання і припинення зловживання правом входить до компетенції усіх державних органів.

Висновки.

У значній кількості наукових досліджень зловживання правом на інформацію і правопорушення є різними за своїм змістом і принципами. Однак, квінтесенцією і зловживання правом, і правопорушення є ігнорування, неповага, недотримання особою інтересів, права більшості суспільства, тих правових норм-принципів, які напрацьовані і формалізовані в інтересах більшості. Водночас, за порушення матеріальних норм законодавством передбачена юридична відповідальність, а за порушення норм-принципів – ні.

З огляду на зазначене, доцільно погодитися з думкою угорського науковця Й. Віга про те, що “надмірне акцентування прав людини при віднесенні на задній план обов’язків або зневага до них, у багатьох випадках призводить до загострення бажання людини здійснити свої права негайно й у повному обсязі” [15, с. 46] і може призвести до порушення свободи інших осіб. З огляду на це, на думку Рогач О.Я., важливим є дотримання балансу між правами і обов’язками. Зазначене потребує внесення відповідних змін в Конституцію України в частині, що стосується розширеного переліку основних обов’язків людини, громадянина, держави, серед яких передбачити й обов’язок – заборони зловживання правом.

Однак, вбачається і інший механізм вирішення зазначеної проблеми. Значна кількість нормативно-правових актів містять норми-принципи, у тому числі і стосовно права на інформацію. Тому, на нашу думку, доцільно концептуально визнати, що порушення принципів права, які мають конкретний вираз в нормах права, нічим не відрізняються від звичайного правопорушення. З огляду на зазначене, в законодавстві доцільно передбачити відповідні правові норми-заборони щодо недопущення порушення правових норм-принципів та норм-санкцій за порушення їхніх вимог і завдання шкоди суспільству чи особі.

Використана література

1. Янев Я.Г. Правила социалистического общежития : их функции при применении правовых норм / Я.Г. Янев ; [пер. с болг. В.М. Сафронова] ; под ред. Ц.А. Ямпольской. – М. : Прогресс, 1980. – 270 с.

2. Кирюшкин Р.А. Злоупотребление правом : монография / Р.А. Кирюшкин. – М. : КНОРУС, 2015. – 192 с.
3. Дерюгина Т.В. Правовая сущность злоупотреблений субъективным гражданским правом // Безопасность бизнеса. – 2013. – № 2. – С. 22-25. – Режим доступа : <http://www.center-bereg.ru/b1316.html>
4. Скаун О.Ф. Теорія держави і права : підручник / О.Ф. Скаун. – Х. : Консум, 2001. – 656 с.
5. Рогач О. Я. Зловживання правом : теоретико-правове дослідження : монографія / О.Я. Рогач. – Ужгород : Ліра, 2011. – 368 с.
6. Общая теория государства и права : академический курс в 3 т. / отв. ред. М.Н. Марченко. – [3-е изд., перераб. и доп.]. – Т. 3. – М. : Норма, 2007. – 712 с.
7. Про інформацію : Закон України від 02.10.92 р. – Режим доступа : <http://zakon2.rada.gov.ua/laws/show/2657-12>
8. Про державну підтримку засобів масової інформації та соціальний захист журналістів : Закон України від 23.09.97 р. – Режим доступа : <http://zakon5.rada.gov.ua/laws/show/540/97-ВР>
9. Перший факт свідомого зловживання правом на свободу інформації. – Режим доступа : <http://blogs.pravda.com.ua/authors/ivanenko/503b959f2432a>
10. Про доступ до публічної інформації : Закон України від 13.01.11 р. // Відомості Верховної Ради України (ВВР). – 2011. – № 32. – Ст. 314.
11. Правове регулювання надання інформації акціонеру. Український та іноземний досвід. Режим доступа : <http://maestrolawgroup.com/ua/publikatsiji/sakhnatskij-andrij/259-pravove-regulyuvannya-nadannya-informatsiji-aktsioneru-ukrajinskij-ta-inozemnij-dosvid>
12. Експерт з Угорщини розповів про зловживання правом щодо публічної інформації. – Режим доступа : <https://hromadskeradio.org/news/2016/09/21/ekspert-z-ugorshchyny-rozpoviv-pro-zlovzhyvannya-pravom-shchodo-publichnoyi-informaciyi>
13. Матузнов Н.И. Актуальные проблемы теории права / Н.И. Матузнов. – С. : Изд. Саратовской государственной Академии права, 2004. – 512 с.
14. Виг Й. Соотношение прав и обязанностей человека и проблемы преступности // Государство и право. – 1995. – № 7. – С. 47-49.

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

УДК 342.951:001.102(477)

**ЯРЕМЕНКО О.І.**, кандидат наук з державного управління, доцент,  
завідувач кафедри правових наук та філософії  
Вінницького державного педагогічного університету

## ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ЮРИДИЧНОЇ ПРИРОДИ ІНФОРМАЦІЙНИХ ВІДНОСИН ТА ЇХ ТИПОЛОГІЗАЦІЯ

**Анотація.** Досліджуються теоретико-методологічні підходи до юридичної природи інформаційних відносин. Проаналізовано відносини виходячи з права на інформацію та інформаційної діяльності. Виділено основні типи відносин в інформаційній сфері.

**Ключові слова:** інформаційні відносини, інформаційна сфера, право на інформацію, інформаційна діяльність, інформаційна інфраструктура.

**Аннотация.** Исследуются теоретико-методологические подходы к юридической природы информационные отношения. Проанализированы отношения исходя из права на информацию и информационной деятельности. Выделены основные типы отношений в информационной сфере.

**Ключевые слова:** информационные отношения, информационная сфера, право на информацию, информационная деятельность, информационная инфраструктура.

**Summary.** The article provides analysis of theoretical and methodological approaches to legal character of information relations. The relations are analysed based on a right to information and information activity. The basic types of relations in an information sphere are determined.

**Keywords:** the information relations, information sphere, the right to information, information activities, information infrastructure.

**Постановка проблеми.** Трансформація інформаційної сфери сучасного соціуму обумовлює необхідність активного використання правових засобів для регулювання інформаційних відносин. Юридична природа цього виду відносин характеризується рядом особливостей, що ускладнює їх нормативне впорядкування. На сьогодні в Україні існує певне протиріччя між бажанням законодавця юридично врегулювати інформаційні відносини, які об'єктивно цього потребують на даному етапі, з ефективністю такого регулювання. Одним із проявів низької ефективності є те, що з однієї сторони, кількісні показники інформаційно – правових норм в системі законодавства України дають підстави констатувати виникнення нової галузі – інформаційного права, з іншої – залишаються не врегульованими багато актуальних аспектів інформаційних відносин. Як зазначає О.М. Селезньова, інформаційні відносини вважаються новими та на сьогодні не є достатньою мірою досліджені і особливої уваги вони заслуговують в контексті того, що виступають предметом інформаційного права, яке, у свою чергу, перебуває на етапі становлення. Вивчення інформаційних правовідносин дає змогу вивести інформаційне право як галузь права на теоретично новий рівень, що зумовлює зосередження наукового інтересу на ознаках, властивостях, видах зазначених суспільних відносин [1, с. 183].

Наукові дослідження в галузі інформаційних правових відносин здійснюються такими науковцями як Ю.П. Андреев, І.В. Арістова, О.А. Баранов, К.І. Беляков, А.Б. Венгеров, Р.А. Калюжний, О.В. Копан, Б.А. Кормич, Т.А. Костецька, О.В. Кохановська, А.І. Марущак, Т.О. Проценко, О.М. Селезньова, Т.А. Семилет, В.Д. Чернадчук та ін.

В той же час, ряд аспектів цієї проблематики залишається дискусійними та малодослідженими і потребують подальшого науково-теоретичного аналізу.

**Метою статті** є методологічно-теоретичний аналіз поняття інформаційних відносин, визначення їх сутності та юридичної природи, а також типологізація суспільних відносин в інформаційній сфері.

**Виклад основного матеріалу.** Суспільні відносини, пов’язані з обігом інформації, виникли одночасно із цивілізацією і в подальшому завжди були невід’ємною складовою життєдіяльності соціальної системи. Поява держави і права та закріплення в перших письмових правових актах відповідальності за порушення усталених відносин в сфері обігу інформації свідчать про актуальність цієї проблеми вже на ранніх стадіях розвитку суспільства. Так, в давньоіндійських законах Ману містилися норми, які встановлювали жорсткі санкції за поширення певних видів інформації – образливої, недостовірної чи аморальної [2, с. 73]. Аналіз інших світових пам’яток права свідчить про те, що фрагментарні інформаційно-правові норми містилися в нормативних актах різних держав і правових систем на всіх історичних етапах розвитку держави і права.

Системне виокремлення інформаційних відносин в самостійний предмет правового регулювання розпочалося в другій половині 20-го століття у зв’язку із трансформацією пріоритетів цивілізаційного розвитку соціуму в напрямку різкого зростання ціннісних характеристик інформації. Це спонукало міжнародні організації та державні органи до правотворчості в інформаційній сфері. При цьому, характерним є те, що процеси юридичного опосередкування інформаційних відносин були започатковані в міжнародних документах у формі закріплення суб’єктивного права, яке складалося з двох основних правомочностей – можливостей поширення інформації та її отримання. Так, Європейська Конвенція про захист прав людини і основоположних свобод передбачає, що кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Аналіз дефініції цієї міжнародно-правової норми свідчить про те, вона ставила за мету надати можливість людині, перш за все, вільно поширювати ідеї, відомості, дані, думки, переконання поза впливом державних інституцій [3].

Дещо ширше розуміння права на інформацію закріплено в Міжнародному пакті про громадянські та політичні права, який трактує це право як свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір [4].

Слід зазначити, що практика регулювання суспільних відносин шляхом нормативного опосередкування суб’єктивних прав базується на положеннях теорії держави і права, основи яких були започатковані ще радянськими вченими. Так, Алексєєв С.С. зазначає, що правовідносини – це засіб трансформації загальних приписів юридичних норм в площину суб’єктивних юридичних прав та обов’язків для конкретних суб’єктів [5, с. 131]. Козлов Ю.М. вважає, що правове відношення є суспільним відношенням, сторони (учасники) якого наділені правами та обов’язками, передбаченими і забезпеченими нормами права, тобто вони є носіями правомочностей і правобов’язків [6, с. 58].

Обґрунтованість цих теоретичних підходів по відношенню до інформаційних відносин підтверджується тим, що процеси їх правового впорядкування здійснювалися шляхом розширення обсягу суб’єктивних прав на інформацію, що і було одним із напрямків формування національного інформаційного законодавства. Це дало підстави

сучасним науковцям трактувати сутність інформаційних правових відносин виходячи із суб'єктивного права на інформацію. Як зазначає Кормич Б.А, сама природа інформаційного права обумовлюється його безпосередньою спрямованістю на реалізацію прав і свобод людини у сфері інформації. І, відповідно, більшість його інститутів спрямовані на створення механізмів реалізації відповідних суб'єктивних прав або безпосередньо громадянами, або на регулювання діяльності суб'єктів владних повноважень та юридичних осіб з метою сприяння реалізації відповідних прав та забезпечення інформаційних потреб суб'єктів інформаційних відносин [7, с. 150].

На основі права на інформацію Арістовою І.В. та Чернадчук В.Д. сформульовано цілком обґрунтовану концепцію інформаційних правовідносин як врегульованих нормами інформаційного права суспільних відносин, що виникають з приводу інформації в процесі реалізації суб'єктивних інформаційних прав та обов'язків, детермінованих інтересами забезпечення своїх інформаційних потреб [8, с. 50].

Водночас, дискусія серед науковців щодо юридичної природи суб'єктивних інформаційних прав проектується і на визначення сутності інформаційних відносин. Так, Кохановська О.В., розглядаючи інформаційні права з позицій суб'єктивного цивільного права, трактує право фізичної особи на інформацію як можливість створювати, виробляти, одержувати, знати, фіксувати, використовувати, поширювати та зберігати інформацію у порядку, передбаченому ЦК України та іншими законами. При цьому, підкреслюється, що інформаційні правовідносини – як особисті немайнові, так і майнові - мають приватноправову природу і не потребують штучного обмеження і безмежного контролю, а права на повагу до інформації як особистого немайнового блага фізичної особи слід дотримуватися ще до моменту народження людини, навіть до того, як вона набуде статусу суб'єкта права [9, с. 187].

Інші вчені вважають за доцільне застосування більш широкого підходу і, оперуючи поняттям “специфіковані інформаційні права”, знаходять різні вияви таких прав в окремих галузях права, в тому числі публічного [10, с. 43].

Суб'єктивні інформаційні права знаходяться в динамічному зв'язку з іншим об'єктивним явищем соціальної реальності – інформаційними процесами, які за останні півстоліття з високою активністю виникають і розвиваються в усіх сферах суспільної життєдіяльності, що обумовлює необхідність їх юридичного опосередкування засобами позитивного права. Як зазначено у [8, с. 47], важливу роль у свідомому проектуванні інформаційних процесів відіграє право, за допомогою якого не лише регулюються відносини, що склалися, а й відбувається розширення сфери інформаційної діяльності, яке обумовлене суспільними потребами .

На думку Венгерова А.Б., спочатку актуалізація впорядкування інформаційних явищ правовими засобами обумовлювалася необхідністю підвищення ефективності управління суспільним виробництвом. Він зазначає, що на певному етапі соціально – економічна та науково – технічна інформація стають одним із важливих факторів і ресурсів розвитку виробничої та управлінської сфери і пропонує розглядати інформаційні відносини як відносини, що виникають в сфері управління народним господарством між працівниками та колективами в процесі реєстрації, збору, передачі, зберігання та обробки інформації [11, с. 17, 27]. В подальшому, за доволі короткий період часу, інформація, поряд з іншими ресурсами і благами, стала основою ефективного функціонування базових соціальних інститутів і, як наслідок, дедалі ширше коло інформаційних об'єктів включалося до системи правових відносин. На цій основі Копилов В.А., пропонує кваліфікувати інформаційні правові відносини як відносини, що виникають при здійсненні інформаційних процесів – процесів

виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, поширення та споживання інформації [12, с. 2].

Водночас, Копилов В.А. застосовує комбіноване визначення інформаційних відносин як відокремленої, однорідної групи суспільних відносин, які виникають в процесі обороту інформації в інформаційній сфері, в результаті здійснення інформаційних процесів в порядку реалізації кожним інформаційних прав та свобод, а також в порядку виконання обов’язків органами державної влади і місцевого самоврядування по забезпеченню гарантій інформаційних прав та свобод [13, с. 102]. Такий підхід підкреслює, що зміст суб’єктивного права на інформацію як сукупності правомочностей щодо вільного збирання, використання та поширення інформації є статичною юридичною конструкцією, яка на практиці динамічно реалізується в конкретних інформаційних процесах – виробництві, зборі, обробці, накопиченні, зберіганні, пошуку, передачі, поширенню та споживанню інформаційних продуктів.

Раціональним є підхід вчених, які застосовують поняття “суспільні відносини в інформаційній сфері” і трактують їх як відносини, пов’язані з інформацією, використанням інформаційних технологій і захистом інформації, які виникають під час здійснення інформаційних процесів – виробництва, збору, оброблення, накопичення, зберігання, пошуку, передання, поширення і споживання інформації [14, с. 2].

Підтримуємо позицію Баранова О.А., який розглядає інформаційні відносини як один із елементів інформаційної сфери, що знайшло свій прояв її дефініції як сукупності інформації та інформаційних ресурсів, інформаційної інфраструктури, суб’єктів, що здійснюють оборот інформації, тобто її створення, поширення (передавання), зберігання, використання та знищення, та забезпечують цей обіг, суспільних відносин, які при цьому виникають, системи її правового забезпечення, а також інституційної системи державного управління та регулювання цією сферою [15, с. 22]. В основу даного визначення покладено динамічну характеристику інформаційної реальності – оборот інформації, який знаходить свій прояв в конкретних видах інформаційної діяльності.

На наш погляд, при дослідженні сутності інформаційних правових відносин слід виходити з того, що саме інформаційна діяльність, у всій своїй багатоманітності, породжує інформаційні процеси і відповідні суспільні відносини. Вторинність інформаційних правових відносин по відношенню до інформаційної діяльності підкреслює і Цимбалюк В.С., який розглядаючи інформаційну діяльність як основну, історично обумовлену форму об’єктивного прояву відносин між людьми щодо інформації, зазначає, що вона проявляється, зокрема, і у статусі інформаційних правовідносин [16, с. 11]. Такий підхід кореспондується із традиційною позицією багатьох науковців, які розглядають суспільні відносини як форму чи спосіб здійснення людської діяльності.

Так, на думку Андрєєва Ю.П., зміст суспільних відносин становлять три складові – привід, який стимулює їх виникнення і розвиток, засоби, за допомогою яких вони реалізуються і набувають об’єктивної форми існування, а також суб’єкти – носії, тобто ті хто створює і підтримує їх існування своєю діяльністю [17, с. 79]. В свою чергу, Семилет Т.А. вважає, що суспільні відносини, будучи самостійними утвореннями, виконують функції соціальних детермінантів, організаторів і регуляторів людської діяльності. Діяльність породжує суспільні відносини, вони ж, у свою чергу, стають необхідною формою діяльності. Суспільні відносини функціонують і розвиваються через свідому діяльність людей, що є одним із проявів їх єдиної родової сутності [18, с. 121]. Застосовувавши цей філософсько-методологічний підхід, вчені-правознавці виводять



загальну конструкцію суспільних відносин як структурної сукупності конкретно історичних соціальних зв'язків, залежностей та обмежень, які виникають в процесі і результаті суспільно значимої предметної діяльності і мають властивість постійно повторюватися [19, с. 84]. Відповідно, при розкритті сутності інформаційних правових відносин, слід відштовхуватися від соціальної діяльності, яку в загальнотеоретичному аспекті можна розглядати як різносторонній процес створення суспільним суб'єктом умов для свого існування і розвитку, як процес перетворення соціальної реальності у відповідності із суспільними потребами, метою і завданнями [20, с. 57]. При цьому, здійснення будь-якого виду людської діяльності призводить до її ідеального відображення шляхом виникнення різних форм інформаційної об'єктивізації, оскільки, ця діяльність супроводжується виникненням, обробкою, акумуляцією інформації. Так, управлінська діяльність чи діяльність, спрямована на створення матеріальних чи інтелектуальних продуктів або надання різноманітних послуг, супроводжується інформаційними процесами, що неминуче призводить до потенційної можливості виникнення суспільних відносин з приводу інформації. Водночас, предметом діяльності конкретної людини чи корпорації може бути безпосередньо інформація, тобто інформаційна діяльність існує як окремий самостійний специфічний вид діяльності.

Таким чином, взявши за основу такий критерій як мета діяльності, можна констатувати наявність двох її видів, предметом яких є інформація – суто інформаційна діяльність і діяльність, де інформація виступає як вторинне явище. Ретрансляція на суспільні відносини цих двох підходів до інформаційної діяльності приводить до висновку про наявність двох видів інформаційних правових відносин. Як зазначають Арістова І.В. та Чернадчук В.Д., суспільні відносини в інтегративній інформаційній сфері можна розглядати як системне утворення, складовими якого постають підсистеми “змішаних” та “чистих” суспільних відносин. До першої підсистеми включені дві групи суспільних відносин, а саме: а) інформаційно-управлінські, інформаційно-майнові, інформаційно-банківські, інформаційно-трудові та ін.; б) управлінсько-інформаційні, майново-інформаційні, банківсько-інформаційні, трудово-інформаційні та ін. Різниця між суспільними відносинами у першій та другій групах полягає у наступному: у першій групі інформаційні відносини постають основними, а усі інші (управлінські, майнові, банківські, трудові та ін.) – забезпечувальними; у другій групі – навпаки: інформаційні відносини є забезпечувальними. Що стосується “чистих” суспільних відносин, то ними постають суто інформаційні відносини [ 8, с. 49].

Безпосередній зв'язок інформаційної діяльності та інформаційних відносин нормативно закріплено і в чинному законодавстві України. Так, в преамбулі Закону України “Про інформацію” зазначено, що цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Водночас, в ст. 9 цього ж закону міститься норма, згідно з якою створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації є основними видами інформаційної діяльності [21].

Аналогічно в Законі України “Про науково-технічну діяльність” зазначено, що ним регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі. Водночас норми цього закону визначають науково-інформаційну діяльність як сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні [22].

Таким чином, інформаційні правові відносини – це особлива група правових відносин, які виникають, розвиваються і припиняють свою дію в процесі здійснення різних видів соціальної діяльності щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, яка регулюється нормами інформаційного права та інших галузей системи національного законодавства, а також міжнародними нормами.

Наявність в соціальному середовищі значних обсягів інформації обумовлює необхідність технічного забезпечення її обігу і, відповідно, правового регулювання цього виду діяльності. Для позначення правовідносин, які виникають під час таких процесів, Баранов О.А. застосовує термін “інформаційно-інфраструктурні відносини”, розуміючи під ними суспільні відносини, що мають місце в процесі забезпечення реалізації інформаційних відносин, тобто пов’язані з функціонуванням суб’єктів інформаційної інфраструктури, які надають інформаційні послуги і виконують роботу в інформаційній сфері, використовують інформаційні технології і ресурси, підтримують інформаційну безпеку тощо. Автор виділяє серед них відносини пов’язані із особливостями життєвого циклу існування суб’єктів інформаційної інфраструктури; наданням інформаційних послуг і виконання інформаційних робіт у процесі створення, поширення, зберігання, використання та знищення інформації; виробництвом і використанням інформаційних технологій і ресурсів; забезпечення інформаційної безпеки [15, с. 126].

Визнаючи обґрунтованість такого підходу, вважаємо за доцільне виокремлення, в системі інформаційно-інфраструктурних відносин, відносин особливого типу, а саме комунікаційно-інформаційних. Закон України “Про телекомунікації” трактує телекомунікації (електрозв’язок) як передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, дровових, оптичних або інших електромагнітних системах [23]. Тобто на відміну від інформаційних відносин, які базуються на інтелектуальній або організаційній діяльності, і зміст яких полягає в цілеспрямованому або опосередкованому створенні тих чи інших інформаційних продуктів та їх подальший оборот і використання, телекомунікаційна діяльність створює технічні умови цього обороту. Телекомунікаційні відносини відрізняються від інших інформаційно-інфраструктурних відносин юридичною природою, суб’єктно-об’єктним складом, підставами виникнення та змістом. Так, діяльність у сфері телекомунікацій має господарський характер і регулюється нормами адміністративного, господарського та цивільного права, які є домінуючими, порівняно з нормами інформаційного права. Це обумовлюється тим, що телекомунікаційна діяльність за своєю суттю не стосується основної характеристики інформації – змісту і не супроводжується створенням нової інформації, а суб’єкти цієї діяльності оперують контентом, який перебуває у власності чи користуванні третіх осіб. Характерним є також те, що значна частина телекомунікаційних відносин виникає на підставі правочинів чи адміністративних актів.

Паралельно, в системі інформаційної інфраструктури, існують інші види діяльності, які можуть передбачати також створення інформаційно-інтелектуальних продуктів з метою їх поширення невизначеному колу осіб. Зокрема, Закон України “Про телебачення і радіомовлення” передбачає, що дія цього Закону поширюється на відносини між суб’єктами діяльності в галузі телебачення і радіомовлення незалежно від їхньої форми власності, мети створення, виду статутної діяльності, а також від способу розповсюдження телерадіопрограм та передач, розрахованих на масове приймання споживачами [ 24].

Таким чином, інформаційно-інфраструктурні відносини можна визначити як суспільні відносини, що виникають, розвиваються і припиняють дію в процесі нормативно врегульованої діяльності щодо надання техніко-організаційних можливостей для соціальних комунікацій, передачі і прийняття різноманітних видів інформації, створення і поширення інформаційних продуктів та об'єктів інтелектуальної власності, а також при охороні та захисті інформації.

Наявність інституту інформаційних прав, інформаційної діяльності як самостійного виду соціальної діяльності, а також інформаційної інфраструктури обумовлює необхідність врегулювання порядку обігу інформації. У зв'язку з цим слід відзначити наявність інформаційно-процедурних та інформаційно-процесуальних правових відносин.

Інформаційно-процедурні правові відносини мають місце при реалізації права на інформацію і зміст їх полягає у певному порядку дій з метою отримання різних видів інформації. Наприклад, Закон України “Про доступ до публічної інформації” визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації та інформації, що становить суспільний інтерес [25]. Аналогічно, Закон України “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації” визначає порядок всебічного і об'єктивного висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації і захисту їх від монопольного впливу органів тієї чи іншої гілки державної влади або органів місцевого самоврядування, є складовою частиною законодавства України про інформацію [26].

Що стосується інформаційно-процесуальних відносин, то вони виступають складовою інших процесуальних відносин – цивільних, господарських, адміністративних, кримінальних і регулюються нормами відповідного процесуального законодавства. Їх зміст складають окремі процесуальні дії суб'єктів правовідносин з метою отримання чи надання інформації, що має значення для вирішення тієї чи іншої справи.

Слід зазначити, що в окремих випадках відмінність між інформаційно-процедурними та інформаційно-процесуальними має умовний характер. Так, відносини, що виникають в процесі реалізації Закон України “Про доступ до судових рішень”, можуть мати як процедурний, так і процесуальний характер [27].

### **Висновки.**

Інформаційні відносини існували на всіх етапах цивілізаційного розвитку, оскільки, інформація, в різних формах, є невід'ємною складовою життєдіяльності суспільства. Тривалий час інформаційно-правові норми містилися в правових актах різноманітних галузей права, а інформація не розглядалася як самостійний об'єкт правового регулювання. Виокремлення інформаційних відносин в самостійний предмет було обумовлено значним підвищенням ролі інформації в соціумі та виникненням високого попиту на неї.

Початковий етап юридичного опосередкування інформаційних відносин характеризується закріпленням суб'єктивного права на інформацію в міжнародних документах та актах національного законодавства країн світу. В подальшому високий рівень динамізму інформаційних процесів призвів до ускладнення відносин в цій сфері і обумовив необхідність нормативного регулювання багатьох видів інформаційної діяльності. В процесі здійснення інформаційної діяльності виникають, розвиваються і припиняють дію відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Складна юридична природа суспільних відносин в інформаційній сфері передбачає необхідність їх типологізації, тобто виділення із загального масиву цих відносин окремих складових, об'єднаних типовими характеристиками. На цій основі можна виокремити інформаційні правові відносини, інформаційно-інфраструктурні, інформаційно-процедурні та інформаційно-процесуальні правові відносини. Кожен із цих видів, в свою чергу, потребує класифікації та ґрунтового аналізу, що може бути предметом подальших досліджень в цьому напрямку.

### Використана література

1. Селезньова О.М. Теоретико-методологічні основи інформаційного права України : монографія / О.М. Селезньова. – Чернівці: Місто, 2014. – 407 с.
2. Законы Ману ; [пер. (с санскрит.) С.Д. Эльмановича, провер. и испр. Г. Ф. Ильиным]. – М. : Изд-во вост. лит., 1960. – 121 с.
3. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. // Офіційний вісник України. – 1998. – № 13. – № 32.
4. Міжнародний пакт про громадянські та політичні права від 16 грудня 1966 р. – Режим доступу: [http://zakon3.rada.gov.ua/laws/show/995\\_043](http://zakon3.rada.gov.ua/laws/show/995_043)
5. Алексеев С.С. Механизм правового регулирования в социалистическом государстве / С.С. Алексеев. – М. : Юрид. лит. – 1966. – 188 с.
6. Козлов Ю.М. Административные правоотношения / Ю.М. Козлов. – М. : Юрид. лит. – 1976. – 201 с.
7. Кормич Б. Конституційно-правове регулювання інформаційних відносин // Юридичний вісник. – 2013. – № 3. – С. 46-51.
8. Арістова І.В., Чернадчук В.Д. Концепція інформаційних правовідносин : сутність та особливості використання у сфері банківської діяльності // Інформація і право. – № 3(6)/2012. – С. 47-56.
9. Кохановська О. Основні теорії у сфері інформаційних правовідносин : концепція інформаційних прав як приватноправового інституту і теорія інформаційного права як галузі права у сучасній правовій доктрині України // Приватне право. – 2013. – № 1. – С. 186-200.
10. Проценко Т.О., Селезньова О.М. Особливості розмежування понять “інформаційні права” та “право на інформацію” // Науковий вісник Херсонського державного університету. – Вип. 6-1. – Т. 3. – 2014. – С. 39-42. – (Серія : Юридичні науки).
11. Венгеров А.Б. Право и информация в условиях автоматизации управления (Теоретические вопросы) / А.Б. Венгеров . – М., Юрид. лит., 1978. – 208 с.
12. Копылов В.А. О системе информационного права // Научно-техническая информация. – (Серия 1. Организация и методика информационной работы). – 2000. – № 4. – С. 1-9.
13. Копылов В.А. О структуре и составе информационного законодательства // Государство и право . – 1996 . – № 6 . – С. 101-111.
14. Попов Л.Л. Информационное право : учебник / Л.Л. Попов. Ю.И. Мигачев, С.В. Тихомиров. – М., 2010. – 496 с.
15. Баранов О.А. Правове забезпечення інформаційної сфери : теорія, методологія і практика : монографія / О.А. Баранов. – К. : Едельвейс, 2014. – 433 с.
16. Цимбалюк В.С. Інформаційне право : визначення сутності та змісту як комплексної галузі права // Правова інформатика. – № 2. – 2005. – С. 5-14
17. Андреев Ю.П. Категория “общественные отношения” : автореф. дис. на соискание учен. степени к.ф.н. – Свердловск : Изд-во УрГУ. – 18с.
18. Семилет Т.А. Проблема регуляции деятельности общественными отношениями : дис. на соискание учен. степени к.ф.н. – Л., 1984. – 176 с.
19. Ткаченко Ю.Г. Методологические вопросы теории правоотношений / Ю.Г. Ткаченко. – М.: Юрид. лит., 1980. – 176 с.
20. Боева Л.П. Человек : деятельность и общение / Л.П. Боева. – М. : Мысль. – 216 с

21. Про внесення змін до Закону України “Про інформацію”: Закон України від 13.01.11 р. № 2938-VI // Відомості Верховної Ради України (ВВР). – 2011. – № 32. – Ст. 313.
22. Про науково-технічну діяльність : Закон України від 25.06.93 р. № 3322-XII // Відомості Верховної Ради України (ВВР). – 1993. – № 33. – Ст. 345.
23. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/1280-15>
24. Про телебачення і радіомовлення : Закон України від 21.12.93 р. № 3759-XII. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/3759-12>
25. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI // Відомості Верховної Ради України (ВВР). – 2011. – № 32. – Ст. 314.
26. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон України від 23.09.97 р. № 539/97-ВР // Відомості Верховної Ради України (ВВР). – 1997. – № 49. – Ст. 299.
27. Про доступ до судових рішень : Закон України від 22.12.05 р. № 3262-V. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/3262-15>

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

УДК 342.951

ПРИМАКОВ К.Ю., здобувач наукового ступеня кандидата юридичних наук,
Класичний приватний університет

СЕМАНТИЧНІ ТА ПРАВОВІ ВЛАСТИВОСТІ МАСОВОЇ ІНФОРМАЦІЇ ЯК ОБ’ЄКТУ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

***Анотація.** В статті досліджуються семантичні та правові властивості масової інформації як об’єкту адміністративно-правового регулювання суспільних відносин, визначаються критерії розмежування масової інформації від іншої інформації, а також функції масової інформації як об’єкту адміністративно-правового регулювання.*

***Ключові слова:** інформація, масова інформація, адміністративно-правове регулювання, засоби масової інформації, органи державної влади, функції інформації.*

***Аннотация.** В статье исследуются семантические и правовые свойства массовой информации как объекта административно-правового регулирования общественных отношений, определяются критерии разграничения массовой информации от другой информации, а также функции массовой информации как объекта административно-правового регулирования.*

***Ключевые слова:** информация, массовая информация, административно-правовое регулирование, средства массовой информации, органы государственной власти, функции информации.*

***Summary.** The article examines the legal and semantic properties of the mass information as an object of administrative and legal regulation public relations, defines criteria of differentiation of the mass information from other information, and also mass information functions as an object of administrative and legal regulation.*

***Keywords:** information, mass information, administrative and legal regulation, media, public authorities, information functions.*

Постановка проблеми. Правове регулювання суспільних відносин у сфері масової інформації має принципове значення для становлення в Україні інформаційного суспільства, забезпечення оптимального функціонування демократичних інститутів, за допомогою яких реалізуються конституційні права громадян на свободу думки і слова, право вільно збирати, зберігати, використовувати і поширювати інформацію. Саме через доступ до масової інформації у першу чергу сучасне суспільство здатне контролювати діяльність органів державної влади та місцевого самоврядування, політичних партій та інших суб’єктів публічного права. При цьому діяльність суб’єктів правовідносин, що складаються у сфері масової інформації, потребує комплексного правового регулювання, яке у цивілізованих країнах здійснюється переважно нормами адміністративного права.

У сучасних умовах питання оптимального адміністративно-правового регулювання суспільних відносин у сфері масової інформації в Україні має особливе значення у зв’язку із загальносвітовими процесами глобалізації, формування глобального інформаційного суспільства, становлення економіки, заснованої на знанні, і прогресуючою гармонізацією загальноєвропейського правового простору. У такому контексті проблеми теоретичного аналізу семантичних та правових якостей масової інформації як об’єкту адміністративно-правового регулювання в Україні набувають стратегічного значення для розвитку вітчизняної правової науки.

Аналіз останніх публікацій. Інформація як філософська категорія розглянута у багаточисленних наукових і публіцистичних роботах зарубіжних та вітчизняних авторів. За кордоном дослідження інформаційної тематики можна зустріти у працях К. Шеннона, Е. Тоффлера, М. Кастельса, Ф. Уебстера, М. Маклюєн, Н. Лумана, Г. Харріса та ін. У вітчизняній науці, а також науці пострадянських країн, питання масової інформації з різних точок зору досліджувалися у працях таких вчених як Г.В. Атаманчук, В.Г. Афанасьєв, І.Л. Бачило, В.В. Белєвцева, Ю.П. Битяк, В.М. Брижко, М.С. Вертузасєв, В.В. Галуцько, В.В. Зуй, О.Л. Копиленко, О.Г. Комісаров, О.О. Кукшинова, В.Д. Малков, В.Г. Машликін, В.А. Мінаєв, В.С. Михалевич, В.Ф. Опришко, Н.С. Полевой, Г.Х. Попов, М.Ф. Савюк, Д.Н. Узнадзе, А.Д. Урсул, О.В. Харенко, М.Я. Швець, В.В. Цветков, Л.П. Юзьков та ін. Водночас в сучасній вітчизняній і зарубіжній науці рівень дослідження питань масової інформації, окремих аспектів її правового регулювання, залишається досить низьким, а проблематика регулювання правовідносин у сфері масової інформації за допомогою адміністративно-правових засобів в Україні взагалі не отримала гідної уваги у науковому середовищі, що й обумовлює актуальність обраної теми.

Метою статті є визначення семантичних та правових властивостей масової інформації як об’єкту адміністративно-правового регулювання.

Виклад основних положень. Основні поняття, що відносяться до масової інформації, досліджуються науковцями на рівні двох масивів знань: законодавчому та теоретико-правовому. Законодавчий масив знань щодо адміністративно-правового регулювання у сфері масової інформації в Україні міститься в нормах міжнародного права, інкорпорованих в національне законодавство у визначений законом спосіб, та, звісно, у нормативно-правових актах, які входять до системи національного права відповідно до певної його галузі.

У міжнародно-правових актах не надається визначення масової інформації, проте існують відповідні механізми регулювання цих процесів міжнародними засобами. Вони витікають із загальних зобов’язань щодо забезпечення, гарантування та захисту всесвітньо визнаних прав людини, закріплених в Загальній декларації прав людини, Міжнародному пакті про громадянські та політичні права, в інших визначальних міжнародних документах у галузі прав людини універсального та регіонального значення.

В національному законодавстві існує певний рівень уявлень про масову інформацію, регулювання процесів, які пов’язані з її виготовленням, розповсюдженням та використанням, проте навіть без глибокого, комплексного аналізу можна зрозуміти, що ці знання потребують доповнень та вдосконалення, хоча б за тією підставою, що інформація як безмежний потік відомостей за своєю природою є надрухливим явищем, знаходиться у постійному русі, втягуючи у воронку власного розвитку нові якості правових взаємовідносин між суб’єктами, які її виготовляють, розповсюджують та вживають. Ця необхідність у модернізації категорійного апарату у першу чергу стосується безпосередньо таких понять, як “інформація”, “масова інформація”, а також визначення правового змісту поняття “адміністративно-правове регулювання” по відношенню до такого об’єкту, як масова інформація.

Дослідження масової інформації як головного об’єкту адміністративно-правового регулювання доцільно починати із з’ясування сенсу, який вкладається у філософську категорію “інформація”. Питання про природу інформації широко обговорюється в філософській літературі, причому з різних теоретичних позицій і методологічних підходів.

Інформація являє собою структурно-складне явище, що включає в себе два типи природних властивостей. Одна з них пов'язана із дуалістичністю структури, її цілісністю і єдністю. Ця природна властивість інформації характеризує її з позиції двох нерозривних між собою елементів: первинного сигналу (повідомлення) і відображеного його образу (концепту або відомості). Друга властивість природи інформації має прояв у динаміці і постійному русі інформаційної взаємодії існуючої дійсності. Відмінності у поглядах дослідників на природу інформації тільки підкреслюють складність цієї проблеми, але не вичерпують всі шляхи її вирішення.

У концепціях і теоріях про природу інформації наводяться різні за змістом підходи до її значення (семантичний, семіотичний, статистичний, атрибутивний, функціональний, правовий, енергетичний тощо). У світлі заявленої мети дослідження, найбільш важливим постає визначення правових характеристик інформації, а також її властивостей як об'єкту адміністративно-правового регулювання. З цих позицій інформацію у вітчизняному науковому середовищі розглядають як продукт відображення світу у свідомості людини, що існує в реальній дійсності у придатній для сприйняття формі, коли її створення, зберігання, використання та знищення регулюються нормами адміністративного права [1, с. 9]. За думкою О.О. Кукшинової, інформація – це відомості та/або дані про події або явища, які відбуваються в суспільстві, державі та навколишньому середовищі, викладені в будь-якій організаційній формі, вигляді та на будь-яких носіях [2]. Правовий характер інформації досліджує В.В. Белевцова, яка вважає, що інформація є сукупністю певних відносин, які за своєю суттю є однорідними, але згідно з певними особливостями поділяються на відкриті та закриті (з обмеженим доступом) [3, с. 9].

Правова характеристика інформації міститься у визначеннях, закріплених у чинному законодавстві України, де інформація має свої різноманітні прояви у суспільних відносинах. Орієнтиром при визначенні інформації вважають її поняття, закладене у Законі України “Про інформацію”, ст. 1 якого визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [4]. Але це не єдине визначення інформації, що зустрічається у вітчизняному законодавстві. Так, Законом України “Про захист економічної конкуренції” інформація визначена як відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [5, п. 2 ст. 1].

Цивільний кодекс України трактує інформацію як “відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді” [6, ст. 200]. Електронний вигляд інформації законодавчо визначається й в Законі України “Про телекомунікації”, за логікою цього нормативного акту для того, щоб “дані” стали інформацією у формі, придатній для її автоматизованої обробки засобами обчислювальної техніки, необхідно перетворення та обробка інформації за допомогою електронно-обчислювальних машин (ЕОМ) [7]. Таку позицію законодавця доповнює В.М. Брижко, який висловлює думку про те, що в електронному середовищі функціонує не “інформація” як така, а “дані”, до яких вона “пристосована”, “прикріплена” і т.д. Дані можна розглядати як формалізовані знаковокодові комбінації, що надають інформацію та призначені для їх автоматичної обробки; цифрові дані – це закодовані електричні сигнали й електронні структури [8, с. 19].

З наведених тлумачень випливає, що інформація, у тому числі й масова, володіє такими правовими властивостями: 1) інформація – це відомості про події та явища, що відбуваються у суспільстві та державі; 2) інформація – це відомості, які є документованими або публічно оголошеними у порядку, встановленому законом; 3) інформація є об’єктом цивільних та управлінських відносин, вона зараховується до категорії нематеріальних благ; 4) джерелами інформації є суб’єкти її виготовлення та поширення за допомогою технічних пристроїв та комунікативних систем.

Безумовно, інформація як соціальна та правова категорія має багато якостей, проте необхідно зупинитися на категорії *масовості* по відношенню до інформації.

Відповідно до Закону України “Про інформацію”, масовою є інформація, що поширюється з метою її доведення до необмеженого кола осіб [4]. З.В. Партико слушно зазначає: якщо якась інформація призначена для всього суспільства чи якоїсь його групи (без обмеження доступу до неї інших), таку інформацію називають масовою [9, с. 132-133]. О.О. Кукшинова визначає таке поняття, як відкрита інформація – відомості та/або дані, одержання, використання, поширення та зберігання яких відповідно до законодавства не може бути обмеженим [2], яке можна вважати синонімічним по відношенню до масової інформації. О.В. Харенко пропонує визначати масову інформацію як вид інформації, призначений для численного кола осіб та для поширення, яке здійснюється у загальнодоступній формі. Авторка виділяє такі особливості масової інформації: 1) масова інформація є видом інформації; 2) критерій для її класифікації – призначення інформації; 3) масова інформація призначена для численного кола осіб: необмеженого у верхній межі, але ні в якому випадку не до однієї, двох або до жодної особи; 4) масова інформація призначена для поширення; 5) оприлюднення масової інформації здійснюється у такій формі, що дає можливість користуватися і бути достатньо зрозумілою усім зацікавленим особам; 6) масова інформація не прив’язана до матеріального інформаційного продукту [10, с. 166].

На наш погляд визначення масової інформації повинне включати філософський та правовий вимір цього явища, відтак *масову інформацію* можна розглядати як сукупність призначених для необмеженого кола осіб відомостей, які адекватно відображають еволюційні процеси суспільного буття та розповсюджуються засобами масової інформації за допомогою спеціальних технічних систем і пристроїв.

Масова інформація відображає дійсність, зафіксовану у певній матеріальній формі, що виготовляється за визначеними технологіями у вигляді інформаційного продукту, який поширюється засобами масової комунікації в інформаційному просторі. Тобто масова інформація завжди є певним продуктом, зафіксованим у визначеній формі (друкованій або електронній). Згідно із ст. 23 Закону України “Про інформацію”, інформаційна продукція – це матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб’єктів інформаційних відносин [4]. До видів інформаційної продукції слід відносити друковані журнали і газети, їх електронні аналоги, книги, наукові фахові видання (як надруковані, так і електронні), рекламні брошури та каталоги, музичні компакт-диски, прокатні художні фільми у кінотеатрах, концертні виступи, театральні вистави тощо. Також під масовою інформацією слід розуміти не тільки новинні повідомлення, а будь-які тексти, презентації, медіaproграми, в яких відображено життєво важливі явища, актуальні події, соціальні групи, інститути, процеси, суспільно значущі постаті, їх діяльність тощо.

Масову інформацію від немасової відрізняє те, що вона здатна виконувати функцію засобу масифікації або керування масами (публікою, натовпами). В.В. Різун справедливо зауважує, що масова інформація не є “відображенням дійсності”, оскільки

масова інформація може бути неповною, неточною, недостовірною або взагалі вигаданою, тобто такою, що не відповідає дійсності. Масова інформація може бути рекламою певного товару, роботи чи послуги або прогнозом погоди у ненаселених пунктах, а тому не нестиме здатність до “масифікації або керування масами” [11, с. 169-170]. Г. Харріс в роботі “Психологія масових комунікацій” відзначає, що сучасну комунікацію роблять масовою три фактори: по-перше, обмеженість точності при адресації інформації; по-друге, наявність інституту засобів масової інформації – джерела самостійної комунікації; по-третє, залучення і за можливості довге утримання максимально широкої аудиторії в інтересах рекламодавців [12]. Варто додати, що запропоновані Г. Харрісом фактори, які роблять сучасну комунікацію масовою, сконцентровані у публічних комунікативних мережах загального користування, серед яких особливе місце посідає Інтернет.

Важливим є питання визначення критеріїв розмежування масової інформації від іншої інформації. О.В. Каплій зауважує, що головним критерієм розмежування масової інформації є критерій публічної поширюваності, який означає масове розповсюдження цієї інформації для відносно великого, невизначеного кола осіб [13, с. 37]. Критерій публічної поширюваності, звертає увагу О.В. Харенко, може застосовуватися у класифікації інформації, але не в цілому, а щодо відкритої інформації, оскільки конфіденційна, таємна та службова поширенню, тим більше публічному, не підлягають. За таким критерієм відкрита інформація може поділятися на поширювану публічно, поширювану не публічно і таку, що надається на інформаційні запити [10, с. 165].

У ст. 22 Закону України “Про інформацію” зазначено, що масова інформація поширюється серед необмеженого кола осіб [4]. Але під необмеженим колом осіб можна розуміти як величезну кількість людей, так і одну особу або жодної взагалі. О.В. Харенко стверджує, що задекларована Законом України “Про інформацію” мета створення і поширення масової інформації – доведення її змісту до необмеженого кола осіб, не є її обов’язковою кваліфікаційною ознакою на відміну від масовості її призначення, тому більш коректним буде застосування замість “необмежений” ознаки “численний”, тобто такий, що стосується багатьох осіб, а не просто певної невизначеної кількості [10, с. 165]. Однак і в цьому випадку категорія “численний” вимагає певного числа, підрахунку осіб, для яких призначена інформація, що, знову ж таки, можна розуміти як величезну кількість людей, так і одну особу або жодної взагалі. Тому масовою можна вважати інформацію, яка вже розміщена (або транслюється) у публічному просторі шляхом її оприлюднення у друкованому або електронному вигляді через комунікативні мережі. При цьому немає значення, скільки осіб ознайомились з цією інформацією – сам факт її оприлюднення зазначеними способами можна визнавати критерієм масовості. За таких умов можна погодитися з висновком К.В. Шурупової [14, с. 171] про те, що абсолютно вся інформація, що розміщується в мережі Інтернет, автоматично стає масовою.

Розвиваючи ідею застосування категорії “численний” відносно осіб-споживачів інформації як своєрідного критерію її масовості, О.В. Харенко припускає, що поширена численному колу осіб інформація не є масовою сама по собі. Авторка наводить приклад: може бути оприлюдненою злочинним способом одержана державна таємниця, але така інформація не була призначена для ознайомлення з нею численної кількості людей і не підлягала поширенню [10, с. 165]. Однак, на наш погляд, мотивація суб’єкта розповсюдження інформації не є важливою для визнання оприлюдненої інформації масовою, достатньо того, що вона потрапила у публічний простір, стала громадським надбанням та гіпотетично поінформувала велику кількість осіб. Отже, відштовхуючись

від наведеного прикладу, суб’єкт розповсюдження державної таємниці має бути притягнутий до відповідальності у встановленому законом порядку.

Масову інформацію як *об’єкт адміністративно-правового регулювання* слід розглядати як складну систему, що складається з трьох великих і відносно самостійних підсистем: комунікативної, інституційної та технічної. Масова інформація як об’єкт адміністративно-правового регулювання виконує функції, які відповідають змісту цих підсистем (комунікативної, інституційної та технічної).

Комунікаційна (лат. communication – роблю загальним, зв’язуюся, спілкуюся) функція визначає спосіб спілкування між людьми. Масова інформація дозволяє індивідуумам незалежно від їх місцезнаходження обмінюватися між собою різного роду відомостями. Комунікативна функція створює “комуну”, оскільки охоплює інформаційним впливом всіх членів суспільства. Завдяки її здійсненню, відомості про будь-які суспільно значимі події стають надбанням суспільства. Інформація, що адекватно відображає процеси суспільного буття, формує суспільну свідомість. Таким чином, масова інформація (комунікативна підсистема) виступає як засіб спілкування і виконує інформаційну функцію.

До функцій *інституційної* підсистеми відносяться: виготовлення, пошук, отримання, передача і поширення інформації. Це означає, що будь-який із засобів (суб’єктів) масової інформації має право у визначених законом рамках виготовляти, шукати, отримувати, зберігати, використовувати і поширювати інформацію.

Технічні функції масової інформації здійснюються спеціальними підприємствами і службами. До них відносяться: видавництва, друкарні, телерадіослужби, ретрансляційні станції, супутникові системи тощо. Найважливішою технічною функцією є поширення продукції засобів масової інформації. Під поширенням продукції засоби масової інформації розуміється продаж (підписка, доставка) періодичних друкованих видань, аудіо- або відеозаписів програм, трансляція радіо-, телепрограм (мовлення), демонстрація кінохронікальних програм, розміщення інформації в комунікаційних мережах загального користування. Для здійснення цієї функції телерадіослужби або підприємства друку повинні отримати ліцензію (на мовлення) або дозвіл (на видавничу діяльність) від компетентних державних органів в порядку, передбаченому законом.

Висновки.

Масова інформація – це сукупність призначених для необмеженого кола осіб відомостей, які адекватно відображають еволюційні процеси суспільного буття та розповсюджуються засобами масової інформації за допомогою спеціальних технічних систем і пристроїв. Масова інформація володіє такими правовими властивостями: 1) інформація – це відомості про події та явища, що відбуваються у суспільстві та державі; 2) інформація – це відомості, які є документованими або публічно оголошеними у порядку, встановленому законом; 3) інформація є об’єктом цивільних та управлінських відносин, вона зараховується до категорії нематеріальних благ; 4) джерелами інформації є суб’єкти її виготовлення та поширення за допомогою технічних пристроїв та комунікативних систем.

Масову інформацію як об’єкт адміністративно-правового регулювання можна розглядати як складну систему, що складається з трьох великих і відносно самостійних підсистем: комунікативної, інституційної та технічної. Масова інформація як об’єкт адміністративно-правового регулювання виконує функції, які відповідають змісту цих підсистем. Функціями масової інформації є основні напрямки впливу масової інформації на індивіда, суспільство і державу. До функцій комунікативної підсистеми

відносяться обмін інформацією між індивідуумами як спосіб спілкування, а також вплив інформаційних повідомлень на суспільну свідомість. До функцій інституційної підсистеми належать виготовлення, пошук, отримання, передача інформації. До головної функції технічної підсистеми відноситься поширення продукції масової інформації.

Використана література

1. Савюк М.Ф. Адміністративно-правові засади інформаційного суспільства : монографія / [М.Ф. Савюк, В.В. Галуцько, Ю.О. Фрицький]. – Херсон : Грінь Д.С., 2016. – 176 с.
2. Кукшинова О.О. Правове регулювання доступу до відкритої інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / О.О. Кукшинова. – К. : Ін-т держави і права ім. В.М. Корецького, 2012. – 20 с.
3. Белєвцева В.В. Теоретико-правові підходи до визначення поняття “інформація” через інформаційні правовідносини // Інформація і право. – № 3(15)/2015. – С. 5-10.
4. Про інформацію : Закон України від 02.10.92 р. ; в ред. від 25.06.16 р. // Відомості Верховної Ради України (ВВР). – 1992 р. – № 48. – Ст. 650.
5. Про захист економічної конкуренції : Закон України від 11.01.01 р. // Відомості Верховної Ради України (ВВР). – 2001. – № 12. – Ст. 64.
6. Цивільний кодекс України : Закон України від 16.01.03 р. ; в ред. від 01.01.14 р. // Відомості Верховної Ради України (ВВР). – 2003. – 40-44. – Ст. 356
7. Про телекомунікації : Закон України від 18.11.03 р. // Відомості Верховної Ради України (ВВР). – 2004. – № 12. – Ст. 155.
8. Брижко В.М. До гносеології категорії “інформація” // Інформація і право. – № 2(2)/2011. – С. 13-20.
9. Партико З.В. Теорія масової інформації та комунікації : навч. посіб. / З.В. Партико. – Львів : Афіша, 2008. – 290 с.
10. Харенко О.В. Друкована масова інформація як вид інформації : правовий аспект // Вісник Харківського національного університету внутрішніх справ. – 2014. – № 4(67). – С. 162-170.
11. Різун В.В. Теорія масової комунікації : підручник / В.В. Різун. – К. : Просвіта, 2008. – 260 с.
12. Харрис Р. Психология массовых коммуникаций. / Р. Харрис. – СПб. : ПРАЙМ-ЕВРОЗНАК, 2002. – 448 с.
13. Каплій О.В. Класифікація засобів масової інформації : конституційно-правові питання // Актуальні проблеми політики. – 2013. – Вип. 50. – С. 35-46. – Режим доступу: http://nbuv.gov.ua/j-pdf/appol_2013_50_5.pdf
14. Шурупова К.В. Перспективи удосконалення правового регулювання доступу та поширення інформації за допомогою мережі Інтернет // Учёные записки Таврического национального университета им. В.И. Вернадского. – (Серия “Юридические науки”). – 2012. – Т. 25(64). – № 2. – С. 166-174.

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

УДК 342.7:316.4

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

## **ДИТИНА У ГЛОБАЛІЗОВАНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ: РЕАЛЬНІ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ**

**Анотація.** Стаття присвячена аналізу сучасного стану та наукових поглядів щодо загроз інформаційній безпеці дитини. Досліджено окремі аспекти уразливості дитини в інформаційній сфері.

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

**Аннотация.** Статья посвящена анализу современного состояния и научных взглядов относительно угроз информационной безопасности ребенка. Исследованы отдельные аспекты уязвимости ребенка в информационной сфере.

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

**Summary.** This article analyzes the current state and scientific views on threats to information security of children. Author considers some aspects of child's vulnerability in the information sector.

**Keywords:** information security of children, threats to information security, vulnerability of the child in the information sphere.

**Постановка проблеми.** Збільшення технологічних і програмних можливостей новітніх інформаційно-комунікаційних платформ, швидкості їх впровадження, суб'єктів та об'єктів інформаційної діяльності, що об'єктивно сприяє глобалізації інформаційного простору, збільшує й спектр загроз інформаційній безпеці особи в сучасному суспільстві. Безпека дитини в інформаційному просторі напряму залежить від ефективності запобігання інформаційним загрозам. Досконалий аналіз загроз, їх джерел, механізмів дії та вірогідності заподіяння шкоди дозволить створити систему превентивних заходів убезпечення дитини в інформаційному просторі, що підвищить її інформаційну безпеку, гарантовану їй статтею 17 Конституції України [1].

Питаннями інформаційної безпеки особи в контексті вивчення інформаційних загроз займалися ряд вчених, зокрема І. Арістова, О. Баранов, І. Бачило, К. Бесяков, В. Брижко, В. Богуш, 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 торкалися такі вчені як Д. Брайт, О. Золотар, Г. Красноступ, О. Петрунько, С. Томпсон, О. Яременко. У той же час комплексного дослідження щодо загроз інформаційній безпеці дитини не проводилось. Питання інформаційної безпеки дитини в сучасному інформаційному суспільстві набуває дедалі більшої актуальності та потребує ґрунтового, всебічного і комплексного опрацювання фахівцями різних галузей наук.

**Метою статті** є аналіз сучасного стану, узагальнення наукових підходів щодо викликів і загроз інформаційній безпеці та визначення факторів ризику для дитини в інформаційному просторі.

**Виклад основного матеріалу.** Конституція України у ст. 17 гарантує будь-якому громадянину забезпечення його інформаційної безпеки [1], а сама інформаційна безпека особи відповідно до Закону України “Про основи національної безпеки України” віднесена до сфери національної безпеки і є пріоритетним напрямом державної політики [2]. Відсутність інформаційних загроз відповідає стану інформаційної безпеки, а їх наявність характеризує небезпеку.

Поняття “загрози” є прототипом поняття “впливи”, тобто пасивним явищем, яке потенційно може перетворитись на активне явище (дію) – впливи [3, с. 155]. Загрози є об’єктивним “демонстратором можливості потенційних дій” [4, с. 89]. При неефективності системи забезпечення інформаційної безпеки загрози в інформаційному середовищі почнуть перетворюватись у впливи та створювати небезпеку для дитини, порушуючи стан її захищеності та стійкості основних стримуючих захисних механізмів. Таке перетворення зумовлює необхідність ретельного вивчення існуючих і потенційно можливих загроз в інформаційному просторі для ефективності їх локалізації та недопущення перетворення їх в негативні та деструктивні інформаційні впливи. Саме на основі досконалого аналізу загроз, їх джерел, механізмів дії та вірогідності заподіяння шкоди слід створювати систему моніторингу і протидії негативним факторам, що можуть становити небезпеку для дитини в інформаційному середовищі та заважати забезпеченню її інформаційної безпеки.

У загальній теорії безпеки загроза трактується як “можливість чи неминучість виникнення соціальних, природних чи техногенних явищ із прогнозованими, але неконтрольованими небажаними подіями, що можуть статись у певний момент часу... спричинити смерть людей чи завдати шкоду їхньому здоров’ю, призвести до матеріальних і фінансових збитків” [5, с. 14].

В.М. Фурашев трактує загрози інформаційній безпеці як “1) обставини, події, дії (штучні або природні) які негативно впливають на стан та рівень інформаційної безпеки або перешкоджають їх зміцненню та підвищенню; 2) наявні та потенційно можливі явища та чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері” [6, с. 7]. Також вчений зазначає, що інформаційна загроза – це з одного боку такий внутрішній чи зовнішній інформаційний вплив, що створює небезпеку зміни напрямку, темпів прогресивного розвитку індивідуумів чи суспільних утворень, а з іншого боку – це небезпека для останніх стати жертвою негативного інформаційного впливу [7, с. 19].

Такої ж думки дотримується і О.О. Золотар, виділяючи два аспекти інформаційних загроз: технічний та гуманітарний, а самі загрози інформаційній безпеці людини трактує як “сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості” [8, с. 71].

Поняття *загроз інформаційній безпеці* в контексті розгляду убезпечення дитини в інформаційному просторі та забезпечення її інформаційної безпеки, на наш погляд, слід трактувати як сукупність умов, факторів та явищ, під дією яких можливе порушення стану інформаційної безпеки дитини, її психофізичного стану, або створення небезпеки його життєво важливим інтересам.

Як зазначається у [5, с. 11-13; 9], не існує єдиного підходу до визначення поняття “загрози”. Загрози інформаційній безпеці особи розглядаються у різних аспектах і класифікуються за різними параметрами.

За масштабністю дії інформаційні загрози поділяють на зовнішні (глобальні) і внутрішні (внутрішньодержавні) [7, с. 19], або на глобальні, регіональні та локальні [10, с. 69].

За видовою ознакою розрізняють політичні, економічні, суспільні, військові, організаційно- та науково-технічні загрози [11, с. 14-15; 12, с. 106], а серед внутрішніх факторів, які мають значний вплив на інформаційну безпеку, за своїм характером відповідно поділяють: на фактори політико-економічного, правового, безпекового і оборонного та гуманітарного характеру [13, с. 112-114].

За причинами виникнення (джерелами) виділяють еволюційні загрози, що об'єднують ті ризики, які несе з собою розвиток суспільства і інформаційно-комунікативних технологій, і штучні, викликані суспільним або політичним запитом.

За засобами реалізації загроз – загрози у сфері масмедіа і загрози у сфері Інтернет-технологій.

За ступенем сформованості інформаційні загрози можна розділити на потенційні (виклики) – “зародження небезпеки, формування передумов, можливість завдання шкоди” та реальні – ті, що завдають шкоди, “остаточно сформоване явище” [14, с. 57; 5, с. 25-26].

За спрямованістю дії загрози інформаційній безпеці особи подвляють на цілеспрямовані та випадкові.

*Цілеспрямованими загрозами інформаційній безпеці*, на наш погляд, є такі події, дії, обставини, фактори які заздалегідь заплановані і скеровані на об'єкт чи групу об'єктів впливу з використанням методів цілеспрямованого інформаційного-психологічного або технічного впливу задля дестабілізації їх психофізичних чи морально-вольових характеристик, що стане причиною різного роду девіацій.

*Випадкові загрози інформаційній безпеці* – це наслідок побічних дій подій, обставин, факторів, випадковий ефект від іншого інформаційного впливу, при якому спостерігається відсутність мети, певного алгоритму дій і конкретизації об'єкта впливу.

Загрози інформаційній безпеці за їх спрямованістю та наслідками відповідно до об'єктів впливу доцільно розділити на індивідуальні (суб'єктні) та суспільні (загальнооб'єктні). Індивідуальні інформаційні загрози становитимуть небезпеку безпосередньо для особи, а суспільні – для суспільства загалом.

Розглядаючи загрози інформаційній безпеці дитини в контексті дослідження негативних інформаційних впливів на її свідомість та підсвідомість, ми дійшли до визначення окремих понять, а саме: “індивідуальних загроз для дитини в інформаційному просторі” та “суспільних загроз для дитини в інформаційному просторі”.

*Індивідуальні ризики та загрози для дитини в інформаційному просторі*, на наш погляд, – це такі ризики і загрози, що викликані негативними інформаційними впливами, направленими на індивідуальну свідомість та підсвідомість дитини, які можуть призводити до деструктивних наслідків, негативно впливати на формування особистості, її фізичне, психічне чи моральне здоров'я, та викликати девіантну поведінку у дитини.

*Суспільні ризики та загрози для дитини в інформаційному просторі* – це такі ризики і загрози, що викликані негативними інформаційними впливами, спрямованими на суспільну свідомість, які можуть призвести до дисбалансу у суспільних відносинах, порушувати суспільні норми та викликати девіантну поведінку особистості у соціумі через дію деструктивного інформаційного впливу на її індивідуальну свідомість, що призводить до формування хибних світоглядних позицій, видозмінених моральних, етичних та загальнолюдських цінностей й порушення її комунікативних навичок.

За методом впливу можна виділити прямі загрози (становлять загрозу індивідуальній інформаційній безпеці особи) та опосередковані загрози (за наявності

посередника). Посередником у даному випадку може виступати як технічний засіб, так і інший суб’єкт суспільних відносин.

Загрози інформаційній безпеці особи, основуючись на виділенні О. Олійником трьох структурних елементів інформаційної безпеки [15, с. 133], можна поділити на: 1) загрози у сфері основних прав і свобод людини; 2) загрози інформаційно-психологічній безпеці особи і суспільства; 3) загрози з використанням інформаційно-технічних засобів. Такої думки дотримується і О.А. Баранов, поділяючи інформаційну безпеку на три складові: “1. Неповнота, невчасність та невірогідність інформації, що використовується; 2. Негативний інформацій вплив; 3. Негативні наслідки застосування інформаційних технологій”, і виокремлює з них у четвертий пункт – несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності й доступності інформації [16, с. 30-34].

Водночас поняття “загрози” є антиподом поняття “впливи”, оскільки вони ще не є діянням по нанесенню шкоди чи вчиненню злочину, а лише потенційною можливістю реалізації певного сценарію. З точки зору Б.А. Кормича, загрозою або замахом на інформаційну безпеку є лише ті дії, за які передбачена відповідальність. Коли відповідальність відсутня, то немає і загроз [17, с. 122-126]. В інформаційній сфері будь-яка інформація може мати як позитивний, так і негативний вплив на особу, а ступінь інформаційної безпеки залежить від ряду факторів, основними з яких є психофізичні особливості індивідуума та його емоційно-психологічний стан [18, с. 122; 19; 20; 21]. У загальному плані, “інформаційно-психологічний вплив на розум і поведінку будь-якої людини може здійснюватися різними шляхами, одні з яких вимагають лише специфічної підготовленості (у переконанні, навіюванні, підкупі, маніпулюванні свідомістю та сприйняттям), а інші – радіо-, телепристроїв, або спеціальної апаратури (технотронні пристрої, зомбування)” [21, с. 70-82].

Б.А. Кормич вважає за недоцільне визначати всі реальні та потенційні загрози на законодавчому рівні, а їх виявлення рекомендує покласти на відповідні компетентні органи державної влади. Проте виявлення загроз в інформаційній сфері є складнішим, ніж в інших сферах, через те, що:

- заподіяння шкоди відбувається у ментальному просторі;
- практично неможливо визначити ступінь заподіяння шкоди;
- ступінь заподіяння шкоди залежить від індивідуальних психофізичних особливостей людини та її емоційно-психологічного стану;
- настання наслідків заподіяння шкоди відтерміновано в часі;
- визначення деяких загроз можливе лише постфактум, після виявлення наслідків діяння;

не існує єдиного інструментарію виявлення загроз, лише опосередковані методи комплексного аналізу психофізичного, суспільно-політичного та інформаційно-технічного чинників.

На думку Б.А. Кормича, концепцію інформаційної безпеки потрібно будувати “виходячи з виявлення найбільш незахищених (вразливих) параметрів існування об’єктів безпеки”, а не на основі теорії загроз [17, с. 124-131]. Тому розглянемо стан захищеності дитини в інформаційному просторі з точки зору її уразливості.

Усі види небезпек, які чатують на дитину в інформаційному просторі, на наш погляд, доцільно було б розкласти на дві великі групи: індивідуальні ризики та загрози (суб’єктивні) та суспільні ризики (об’єктивні). Це корелюється з думкою О. Петрунько, яка аналізуючи роботи М. Назарова, П. Фролова [22; 23] в контексті вивчення та прогнозу деструктивних наслідків медіавпливу на дітей, дійшла висновку, що



розглядати загрози інформаційній безпеці необхідно “...у двох вимірах – індивідуально-особистісному (вплив на психіку і поведінку окремих індивідів) і суспільному (надіндивідному, соцієтальному, соціалізаційному)” [24, с. 202].

Перше, на що слід звернути увагу, вивчаючи індивідуальну інформаційну безпеку дитини – це великі об’єми інформації та швидкість її обігу. Якщо говорити загалом, то великі об’єми спожитої інформації викликають втому та перенапруження, що у подальшому може стати причиною порушення фізичного чи психічного здоров’я дитини. Через відсутність критичного мислення, дитина не повною мірою може відрізнити правдиву інформацію від неправдивої. А це, поряд із недостатньою обізнаністю та відсутністю досвіду, є фактором ризику, що може призводити до маніпулювання особою [18, с. 122]. В силу недостатнього фізичного розвитку дитяча свідомість не здатна сприймати, а головне аналізувати й екстрагувати головне із великого інформаційного потоку. Це послаблює аналітичні здібності та формує у дитини поверхневність сприйняття, що негативно впливатиме на навчальний процес та освітній рівень загалом [25, с. 13].

Один з засновників теорії комунікацій Г.М. Маклуен [26] розділяє джерела інформації на гарячі (зручні) – для прикладу телебачення та холодні (незручні) – книги. На його думку, зручними є ті джерела, які охоплюють якомога більше елементів сенсативного сприйняття інформації (наприклад – телебачення), а незручні – це ті, які примушують людину докладати додаткових зусиль для її отримання. Наприклад, для отримання інформації з книги необхідно зосередитись при читанні, створити образні елементи, додати недостатні частини і т. д. Такий вид отримання інформації спонукає до розумової діяльності, що автоматично тренуватиме та удосконалюватиме усі когнітивні функції дитини, зокрема: увагу, сприйняття, гносис, пам’ять, інтелект, мову та навіть праксис. Однак сучасні діти перевагу віддають більш зручному способу отримання інформації: готовій нарізці матеріалів, які пропонує телебачення, без додаткових зусиль на його опрацювання та переосмислення. У цьому може критися небезпека, адже усі когнітивні функції дитячого організму знаходяться на етапі формування і від того, наскільки часто дитина змушує свій мозок оперативно працювати, залежить її інтелектуальний рівень, змога аналізувати інформацію, здатність формувати власні механізми захисту від негативних інформаційних впливів на її свідомість і вміння протистояти маніпулюванню та інформаційній агресії. Проте частина вчених вважають, що кліпове (мозаїчне) сприйняття інформації, яке було започатковане в телебаченні, нині стає новоутворенням сучасного суспільства й дозволить наступним поколінням справлятися з інформаційним перенасиченням, швидше аналізувати інформацію, виокремлювати головне та синтезувати необхідне. Однак це лише теоретичне припущення, а необхідність розвитку й удосконалення когнітивних функцій організму дитини при становленні її особистості підтверджено досвідом психологів.

Отже, великі об’єми інформації та сучасні способи її подачі мають негативну дію на когнітивні функції організму дитини. Великі об’єми інформації не дають можливості зосереджувати увагу дитини на заданій тематиці, змінюють рівень її психічної активності, що призводить до психофізичного виснаження, втомленості та зміни емоційного стану (збудження чи заторможення). Відсутність достатнього рівня концентрації уваги разом з мозаїчністю (кліповістю) подачі інформації сучасними зручними або гарячими (за Г.М. Маклуеном) засобами передачі інформації на кшталт телебачення або мережі Інтернет, призводить до поверхневого сприйняття, що не дає можливості повною мірою оволодіти здатністю до побудови цілісних образів і уявлень. Це може призвести до фрагментарності у запам’ятовуванні та ускладнить відтворення цих образів, у тому числі й у соціально-комунікативній сфері.

Нездатність самостійно моделювати власні образи приведе до заміщення їх у свідомості дитини чужорідними, запозиченими ззовні, або нав'язаними пропагандою. Із-за швидкості обігу великої кількості інформації на сучасному етапі розвитку суспільства дитина для формування власної системи цінностей та ідеологічних поглядів вимушена використовувати ярлики і образи нав'язані ззовні через засоби комунікації. Зовнішнє інформаційне середовище не завжди пропонує істинні цінності, а переважно підмінює їх системою символів та ілюзорних норм. Найяскравішим прикладом такої підміни понять є реклама, особливо – політична, де істина підміняється красивим образом, створюється ілюзія позитиву і приховується інша його сторона. Через відсутність аналітичних фільтрів, дитина такі образи сприймає як істинні та вбудовує їх у власну систему поглядів та цінностей. В подальшому ці образи слугуватимуть їй як еталонні. Це призведе до видозміни свідомості дитини, викривлення її світосприйняття та основних цінностей. Дитина з видозміненою свідомістю, вступаючи у суспільні відносини, змінюватиме і саме суспільство.

Таким чином, можемо сказати, що інформаційне середовище, що оточує дитину має значний вплив на формування її особистості. При відсутності, або недостатній кількості інших комунікаційних зв'язків та позитивних (кореляційних) інформаційних впливів авторитетних для дитини осіб, її внутрішній світ формується з ілюзорних, створених штучно образів, які підмінюють справжні цінності та спотворюють, викривляють погляди дитини.

Низький рівень концентрації уваги та поверхневого сприйняття інформації у подальшому призведуть до зниження інтелектуального рівня дитини. Тобто її вміння опрацьовувати інформацію, а саме: аналізувати, зіставляти, оцінювати, узагальнювати та використовувати для вирішення завдань, буде надто низьким. В площині розгляду питання протидії негативним інформаційним впливам на дитину такі вміння будуть недостатніми для протидії цілеспрямованим маніпулятивним впливам на її свідомість та не дозволять створити достатньо дієвих механізмів протидії зовнішнім впливам, що становитимуть небезпеку. Тому беззаперечними методами протидії негативним інформаційним впливам на дітей в контексті перенасичення їх інформаційного простору є обмеження кількості інформації, яку вони споживають. Особливо актуальним це питання є на початкових етапах становлення особистості поки у дитини ще не сформовані власні механізми протидії інформаційному впливу ззовні. Необхідно знизити рівень інформаційного потоку на дитячу свідомість з врахуванням контекстних змістів повідомлень. Інформаційне середовище, що оточує дитину, повинно бути водночас цікавим, з врахуванням вікових запитів та інтересів, і безпечним. Також слід звести до мінімуму споживання інформації, що не потребує додаткового опрацювання свідомістю дитини. Основним джерелом такої інформації за поширеністю, популярністю та масовістю споживання є телебачення. Обмеження перегляду телевізійного продукту у розрізі вікового діапазону дитини та часу, проведеного біля екрану, дозволить не лише підвищити показники особистісного розвитку, але й знизить вірогідність завдання шкоди негативними інформаційними впливами на її свідомість та можливість виникнення медіаадикцій.

Ще одним фактором, що несе суттєву загрозу для формування особистості у дитини, є екранна агресія. Екранне насилля, жорстокість та порнографія теж чинять певний тиск на свідомість та підсвідомість дитини. Загалом цю групу загроз прийнято називати медіанасиллям. Хоча частина науковців і вважає за доцільне використовувати дозовану кількість екранної агресії, проте беззаперечним є й той факт, що збільшення

агресії на екрані провокує підвищення агресивної поведінки дитини в реальному житті, а відтак – збільшення агресії у суспільстві [19, с. 193-214, 237-254].

В контексті інформаційного насилля слід виокремити ще й агресивні комп’ютерні ігри, що становлять загрозу не лише психологічному, але й фізичному здоров’ю дитини та викликають залежність. Діти, які часто грають в агресивні комп’ютерні ігри, не до кінця усвідомлюють нереальність подій у грі і, перебуваючи у стресовій ситуації під дією психологічного навантаження, можуть переносити здобуті тут навички у реальне життя. Зважаючи на захоплення в іграх вбивства призами і подарунками, у дитини створюється хибне враження: що насилля – це добре. Це значно спотворює у неї уявлення про основні моральні цінності [27]

Іншим аспектом індивідуальної небезпеки дитини в інформаційному просторі є негативний вплив інформації на її підсвідомість. Підсвідоме сприйняття інформації відбувається переважно на емоційному рівні. Дитина, в силу вікових особливостей, є більш емоційно сприйнятливою, характеризується частими змінами настрою. Оскільки, сприйняття нею інформації відбувається переважно в симплексному режимі та в основному на емоційному рівні, велика кількість інформації не сприймається дитячою свідомістю, а переходить відразу у підсвідоме. Це стає можливим через низку причин, серед основних з яких:

- а) неналежна фільтрація змістів інформації;
- б) відсутність вибіркової споживання інформаційного продукту;
- в) велика частка пасивного споживання інформації.

Природні фільтраційні механізми, які покликані оберігати психіку людини від негативного впливу інформації, особа набуває в процесі пізнання та з досвідом. Чим менша дитина, тим менше у неї досвіду і тим недосконаліші ці механізми. Перші такі природні фільтри з’являються у неї лише на другому, а подекуди і на третьому етапі становлення її особистості. Це переважно період середнього та старшого шкільного віку. Коли дитина накопичила певний об’єм знань, вона починає релаксувати, намагаючись застосувати на практиці ці здобутки. У цей період вона отримує певний досвід: як позитивний, так і негативний. Лише тоді можна говорити про здобуття певних навичок та вмінь у питанні убезпечення власного інформаційного простору, тобто формування так званого “інформаційного щита”, або фільтраційних механізмів захисту від негативних інформаційних впливів. Відповідно, на початкових етапах становлення особистості спостерігається практично відсутність таких механізмів та цілкова незахищеність свідомості а особливо підсвідомості дитини від дії негативних інформаційних впливів.

Без фільтрації через відсутності чи недосконалість природного індивідуального інформаційного фільтру, виробленого в процесі пізнання, та відсутність вибіркової споживання, а також враховуючи те, що дитина, як правило, є пасивним споживачем інформації (наприклад, увімкнений у фоновому режимі телевізор, фонові реклами на інтернет-сторінці та ін.) велика частина інформації не аналізується свідомістю, а відразу переходить у підсвідоме. Наразі підсвідомість людини мало вивчена і процеси, що з нею пов’язані, знаходяться у сірій зоні сучасної науки. Тому визначити рівень інформаційного навантаження на дитину дуже складно. Емпіричні дослідження впливу інформації, що коли-небудь потрапила у підсвідомість людини, не дають чіткої відповіді на запитання, чи впливатиме така інформація в подальшому на неї і наскільки цей вплив буде дієвим. Проте такі дослідження фіксують ряд випадків, коли негативна інформація, зафіксована у підсвідомості дитини, мала суттєвий вплив на психічні стани як у коротко- так і у довгостроковій перспективі [19] Враховуючи той

факт, що ступінь інформаційної вразливості кожної дитини індивідуальний і залежить від багатьох обставин: віку, емоційного стану дитини, місця перегляду, контенту, і найголовніше – від індивідуального сприйняття побаченого свідомістю окремої дитини [19, с. 78], можемо зробити висновок, що у питаннях забезпечення інформаційної безпеки дитини слід іти від загальних методів до індивідуальних підходів.

Розглядаючи загрози інформаційній безпеці дитини, ми торкнулися лише тієї частини існуючих викликів, де дитина є споживачем інформації та інформаційного продукту. Існує й ряд інших загроз, що виникають через неналежний захист дитиною її конфіденційною інформації, ризики у сфері комунікації з використанням сучасних технологій, “цифрова нерівність” серед дітей та інше.

Немає сумнівів у тому, що дитина, будучи найактивнішим учасником суспільних відносин в інформаційній сфері, є найбільш незахищеним їх суб’єктом в силу вікового онтогенезу та підвищеної вікової інформаційної віктимності. Вона потребує особливого захисту з боку держави. Усі наявні ризики та загрози інформаційного простору дитини необхідно розглядати з врахуванням її віку, характерних для нього психофізичних особливостей розвитку та етапів соціального становлення. Прогнозування інформаційних викликів та загроз є вкрай важливим елементом забезпечення інформаційної безпеки дитини, яка знаходиться в процесі дорослішання, тобто лише набуває статусу суб’єкта інформаційних відносин повною мірою, проходячи поступові етапи від об’єкта соціального впливу, у тому числі інформаційного, до повноцінного суб’єкта суспільних відносин.

### **Висновки.**

Чим швидше розвиваються технології в інформаційному суспільстві, тим інтенсивніше з’являються нові загрози інформаційній безпеці. Чим більш залучена людина до використання інформаційно-комунікаційних технологій, тим більше вона незахищена в інформаційній сфері. Загрози інформаційній безпеці видозмінюються разом із трансформаційними процесами у суспільстві. Не існує на сьогодні єдиної уніфікованої класифікації інформаційних загроз. Вона залежить від мети та методів наукового пізнання. З точки зору убезпечення дитини в інформаційному просторі класифікація дозволила б не лише впорядкувати понятійно-категоріальний апарат інформаційного права, але й допомогла б заздалегідь виявляти та локалізувати інформаційні загрози. Це дозволило б превентивно убезпечувати інформаційний простір дитини за рахунок системи раннього моніторингу та реагування. Досконало вивчені інформаційні загрози спроектовані на уразливість дитини в інформаційній сфері, з врахуванням її вікового онтогенезу, виявили б слабкі місця в системі інформаційної безпеки дитини на кожному з етапів її дорослішання. Це дало б можливість побудувати модель інформаційних ризиків для дитини на всіх етапах її індивідуального та суспільного становлення. Маючи таку модель, було б зрозуміло, яких саме організаційних та правових заходів мусить вжити держава для убезпечення дитини в інформаційному просторі на всіх стадіях її дорослішання: від об’єкта соціального впливу до повноцінного суб’єкта суспільних відносин.

Поняття загроз інформаційній безпеці в контексті розгляду убезпечення дитини в інформаційному просторі та забезпечення її інформаційної безпеки слід трактувати як сукупність умов, факторів та явищ, під дією яких можливе порушення стану інформаційної безпеки дитини, її психофізичного стану, або створення небезпеки його життєво важливим інтересам.

### Використана література

1. Конституція України : Закон від 28.06.96 р. № 254к/96-ВР – Режим доступу : <http://zakon4.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. № 964-IV. – Режим доступу : <http://zakon4.rada.gov.ua/laws/show/964-15>
3. Савінова Н.А. Правове забезпечення соціальної політики України в умовах розвитку інформаційного суспільства / Н.А. Савінова, А.О. Ярошенко, Л.А. Литва. – К. : Вид-во НПУ імені М.П. Драгоманова, 2012. – 270 с.
4. Савінова Н.А. Кримінально-правова політика та убезпечення інформаційного суспільства в Україні : монографія / Н.А. Савінова. – К. : Ред. журн. “Право України” ; – Х. : Право, 2013. – 292 с.
5. Горбулін В.П. Засади національної безпеки України : підручник / В.П. Горбулін, А.Б. Качинський. – К. : Інтертехнологія, 2009. – 272 с.
6. Фурашев В.М. Про деякі принципові моменти у сфері інформаційної безпеки / В.М. Фурашев : матеріали XV Международной научно-практической конференции ИТБ-2015 [“Информационные технологии и безопасность”]. – К. : ИПРИ НАН Украины, 2015. – 250 с.
7. Фурашев В.М. Державно-правові проблеми інформаційної безпеки людини і суспільства в умовах інтеграції України у світовий інформаційний простір / В.М. Фурашев : матеріали наук.-практ. конференції [“Запобігання новим викликам і загрозам інформаційній безпеці України : правові аспекти”], (6 жовтня 2016 р., м. Київ) / НТУУ “КПІ ім. Ігоря Сікорського”; упоряд. В.М. Фурашев. – К. : Вид-во “Політехніка”, 2016. – 204 с.
8. Золотар О.О. Загрози інформаційній безпеці людини // Правова інформатика. – № 2(42)/2014. – С. 70-79.
9. Горбулін В.П. Інформаційні операції та безпека суспільства, загрози, протидія, моделювання : монографія / В.П. Горбулін, О. Г. Додонов, Д. В. Ланде ; ІПНБ при РНБОУ. – К. : Інтертехнологія, 2009. – 164 с.
10. Манжук І.В. Інформаційна безпека держави: поняття сучасні загрози / : зб. матер. наук.-практ. конф. [“Актуальні проблеми управління інформаційною безпекою держави”], (19 березня 2015 р., м. Київ). – К. : Центр навчальних, наукових та періодичних видань НА СБУ України, 2015. – 512 с.
11. Погребняк А.В. Технології комп’ютерної безпеки. – Кн. 3 / А.В. Погребняк. – Рівне, 2011. – 117 с.
12. Соснін О.В. Інформаційна політика України : проблеми розбудови електронних ресурсів. – Режим доступу : <http://www.niisp.gov.ua/vydanna/panorama>
13. Корж І.Ф. Проблемні аспекти забезпечення безпеки людини, суспільства, держави ; матеріали XV Международной научно-практической конференции ИТБ-2015 [“Информационные технологии и безопасность”]. – К. : ИПРИ НАН Украины, 2015. – 250 с.
14. Арістова І.В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія / І.В. Арістова, Д.В. Сулацький. – К. : Ред журн. “Право України” ; – Х. : Право, 2013. – 184 с.
15. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні // Право і суспільство. – 2012. – № 3. – С. 132-137.
16. Баранов О.А. Базові принципи інформаційного права – забезпечення інформаційної безпеки : зб. матер. наук.-практ. конф. [“Запобігання новим викликам і загрозам інформаційній безпеці України : правові аспекти ”], (6 жовтня 2016 р., м. Київ) / НТУУ “КПІ ім. Ігоря Сікорського”; упоряд. В.М. Фурашев. – К. : Вид-во “Політехніка”, 2016. – 204 с.
17. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. на здобуття наук. ступеня д.ю.н. за спец. 12.00.07 / Борис Анатолійович Кормич. – Харків : НУВС, 2004. – 427 с.
18. Прибутко П.С. Інформаційні впливи : роль у суспільстві та сучасних воєнних конфліктах / П.С. Прибутко, І.Б. Лук’янець. – К. : ПАЛИВОДА А.В., 2007. – 252 с.

19. Брайант Д. Основы воздействия СМИ / Д. Брайант, С. Томпсон. – М.-К., 2004. – 424 с.
20. Петрунько О.В. Діти і медіа : соціалізація в агресивному медіасередовищі : монографія. – Полтава : ТОВ НВП “Укрпромторгсервіс”, 2010. – 480 с.
21. Брижко В. е-боротьба в інформаційних війнах та інформаційне право : монографія / В. Брижко, М. Швець ; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2007. – 218 с.
22. Назаров М.М. Массовая коммуникация в современном мире : методология анализа и практика исследований / М.М. Назаров. – М.: Едиториал УРСС, 2003. – 240 с.
23. Фролов П.Д. Критерії експертної оцінки впливу інформації з елементами насильства, жахів та порнографії на дитячу, підліткову і юнацьку психіку / Наукові студії із соціальної та політичної психології : зб. статей. – К. : ТОВ “Міленіум”, 2003. – Вип. 7 (10). – С. 162-173.
24. Петрунько О.В. Психологічні захисти від деструктивного медіавпливу / Культура народів Причорномор'я. – 2007. – № 101. – С. 201-205.
25. Николас Дж. Карр. Пустышка. Что Интернет делает с нашими мозгами. – (The Shallows: What the Internet is Doing to Our Brains ; переводчик Павел Миронов). – СПб. : BestBusinessBooks, 2012. – 256 с.
26. McLuhan : Hot & Cool. – Signet Books. – NY : The New American Library Inc., 1967. – С. 286.
27. Медиа-насилие: детям прививают страсть к убийству. Интервью с полковником Дэвидом Гроссманом ; [перевод Т. Шишовой]. – Режим доступа : <http://www.pravoslavie.ru/jurnal/783.htm>

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

Правова інформатика

УДК 004.7:001.8

ЛАНДЕ Д.В., доктор технічних наук,

Інститут проблем реєстрації інформації НАН України,

Науково-дослідний інститут інформатики і права НАПрН України

ПОБУДОВА МОДЕЛЕЙ ПРЕДМЕТНИХ ОБЛАСТЕЙ З ЮРИСПРУДЕНЦІЇ ЗА ДАНИМИ СЕРВІСУ WIKIPEDIA

Анотація. У роботі наводиться алгоритм побудови моделей різних предметних областей з юриспруденції на базі автоматичного аналізу даних сервісу Wikipedia. Показано, як виявляється термінологічна база, що динамічно змінюється при розвитку сервісу-першоджерела, формується мережева структура, розраховується вага різних термінів-понять за двома різними критеріями – ступенями вузлів і PageRank. На прикладах показана адекватність підходів, що пропонуються, а також, що кластери в термінологічних мережах можуть розглядатися як основа для виявлення окремих наукових напрямків.

Ключові слова: модель предметної області, термінологічна база, Wikipedia, зв'язки понять, юриспруденція, сканування мережевого сервісу.

Аннотация. В работе приводится алгоритм построения моделей предметных областей по юриспруденции на основе автоматического анализа данных сервиса Wikipedia. Показано, как определяется терминологическая база, динамически изменяемая при развитии сервиса-первоисточника, формируется сетевая структура, рассчитывается вес разных терминов-понятий по двум разным критериям – степеням узлов и PageRank. На примерах показана адекватность предлагаемых подходов, а также то, что кластеры в терминологических сетях могут рассматриваться как основа для выявления отдельных научных направлений.

Ключевые слова: модель предметной области, терминологическая база, Wikipedia, связи понятий, юриспруденция, сканирование сетевого сервиса.

Summary. The algorithm of creation of models of subject domains on jurisprudence on the basis of automatic data analysis Wikipedia service is offered in the article. It is shown how the terminology database is defined, the network structure is created, weight of different terms-concepts is calculated by two different criteria – node degree and PageRank. 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, Wikipedia, links of concepts, jurisprudence, scanning of network service.

Постановка проблеми. Сьогодні під моделлю предметної області, зокрема, розуміють спеціальним чином сформовану мережу понять, онтологію. Побудова великої галузевої онтології – складна науково-практична проблема [1; 2]. Перший етап цього процесу – побудова термінологічної основи онтології і визначення семантичних зв'язків [3].

Аналіз останніх публікацій. Вивченню моделей предметних областей, так само як і сервісу Wikipedia (<http://wikipedia.com>), присвячена велика кількість робіт, що підтверджує актуальність проведених досліджень [4]. Серед них, зокрема, методи побудови мереж співавторів, визначення значущих вузлів, структури мережі, дослідження цитування, а також відповідних корпусів [5].

Пропонується методика побудови інформаційних мереж – моделей предметних областей на основі автоматичного моніторингу і аналізу мережевих інформаційних ресурсів довідкового характеру. Як така мережа в роботі розглядається мережа понять, що відповідають термінам-заголовкам статей мережевої енциклопедії Wikipedia.

Метою роботи є опис теоретичних принципів і методології та оцінка алгоритмічних засад побудови моделей предметних областей, зокрема, галузі юриспруденції шляхом моніторингу і аналізу мережевих інформаційних ресурсів довідкового характеру. Для досягнення цієї мети розроблено спеціальний алгоритм сканування ресурсів сервісу Wikipedia з метою отримання репрезентативного набору термінів-понять як основи (вузлів) майбутньої мережі.

Виклад основного матеріалу. Очевидно, мережа понять може мати досить великі розміри, якщо її не обмежувати певною тематикою, що відповідає предметній області. Ця властивість значно ускладнює сприйняття сформованої мережі і призводить до такого ефекту, як зсув тематики. Для подолання цього ефекту застосовується елементарна тематична фільтрація – для аналізу використовуються лише ті статті з Wikipedia, які містять базовий термін, що визначається експертом-аналітиком. Відповідність до цих дескрипторів і визначає розмір сформованих мереж – моделей предметних областей, а також динаміку їх формування. Крім того, розпізнавання кластерів в таких мережах може розглядатися як основа для виявлення окремих наукових напрямків [1].

Методика досліджень.

До розгляду було взято систему Wikipedia, що є доступною в глобальній мережі і не передбачає передплати, крім того, доступна для завантаження у повному обсязі. Для первинного доступу до системи було застосовано спеціальні терміни з юридичної проблематики, за якими існують відповідні статті, що створюються і редагуються експертами-авторами (Рис. 1).

З огляду на ці базові терміни (теги), що відповідають певній предметній області, визначено представлення інформації в цій системі. Також було визначено, що вільний перехід за гіперпосиланнями веде до ефекту так званого “зсуву тематик” (Topic Drift).

Розглядався наступний алгоритм побудови моделей предметних областей за даними сервісу Wikipedia, який передбачає уникнення цього ефекту:

1. Обирається перший термін-поняття, з якого починається зондування.
2. Відкривається сторінка веб-сервісу (стаття Wikipedia), що відповідає обраному терміну-поняттю. До створюваної мережі додаються всі терміни-поняття, що відповідають гіперпосиланням на обраній сторінці. Формуються ребра-зв'язки до цих вузлів з вихідного вузла.
3. Статті, що відповідають гіперпосиланням на попередній сторінці, визначаються як базові, якщо на них міститься гіперпосилання на статтю, що відповідає першому терміну-поняттю, з якого починалось зондування.
4. Із списку вузлів мережі, що формується, визначається той, за яким ще не здійснювалося переходу, на сторінку якого планується перейти для подальшого аналізу. Цей вузол має відповідати вимозі, наведений у попередньому пункті, та не входить до складу тих вузлів, до сторінок яких вже був здійснений перехід.
5. Якщо такий вузол-автор обрано, то здійснюється перехід до пункту 2.
6. Якщо такого вузла не існує, то вважається, що мережу, що відповідає моделі предметної області, побудовано.

Відповідно до наведеного алгоритму процес збирання інформації з Wikipedia, починаючи з певного вузла-поняття, припиняється, коли відповідно до алгоритму вже неможливий перехід до нового вузла (базових вузлів для переходу вже не лишається), тобто “зациклювання” неможливе.



Рис. 1 – Інтерфейс користувача системи Wikipedia, розглядається стаття за терміном-поняттям **Criminal Law**

Відповідно до наведеного алгоритму процес збирання інформації з Wikipedia, починаючи з певного вузла-поняття, припиняється, коли відповідно до алгоритму вже неможливий перехід до нового вузла (базових вузлів для переходу вже не лишається), тобто “зациклювання” неможливо.

Фрагмент траси виконання програми визначення термінологічної основи предметної області, що відповідає наведеному алгоритму і базовому терміну **Family Law**, наведено на Рис. 2.

Отримані результати.

Побудовано відповідно до наведеного алгоритму мережі співавторів за базовими термінами-поняттями **Constitutional law**, **Family Law**, **Criminal Law** без обмежень на кількість сканованих вузлів. За допомогою програмного засобу Gephi отримана візуалізація мереж, що відповідають вибраним предметним областям (Рис. 3 – 5).

Отримані такі характеристики [5] побудованих мереж: **Constitutional law** – вузлів: 209, зв’язків: 1535, щільність: 0,035; **Family Law** – вузлів: 250, зв’язків: 3871, щільність: 0,062; **Criminal Law**: вузлів: 1050, зв’язків: 64739, щільність: 0,059. Найбільш вагомими за двома критеріями (ступенями вузлів і PageRank) терміни-поняття, що відповідають вибраним предметним областям, наведено у Додатку.

Використання методів кластерного аналізу дозволяє виявляти найбільш тісно пов’язані між собою групи термінів-понять, що можуть застосовуватися для визначення нових наукових областей. На Рис. 3 показано приклад процесу виявлення кластерів шляхом застосування спеціального алгоритму, що застосовується в системі Gephi.

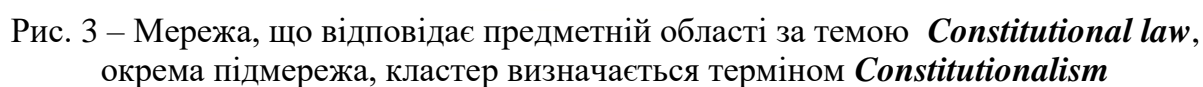
```

Family_law
1: Family_law
>!: Types_of_marriages
>!: Prenuptial_agreement
>!: Cohabitation
>!: Civil_union
>!: Domestic_partnership
>!: Void_marriage
>!: Voidable_marriage
>!: Annulment
>!: Dissolution_of_marriage
>!: Divorce
>!: Adultery
>!: Grounds_for_divorce
>!: Legal_separation
>!: Alimony
>!: Parenting_plan
>!: Custody_Evaluator
>!: Parenting_coordinator
>!: Child_custody
>!: Legal_guardian
>!: Child_support
>!: Grandparent_visitation
>!: Emancipation_of_minors
>!: Parental_child_abduction
>!: Conflict_of_divorce_laws
>!: Conflict_of_marriage_laws
>!: Paternity_fraud
>!: Bigamy
>!: Child_Protective_Services
>!: Child_abuse
>!: Incest
>!: Domestic_relations
><: Civil_union
><: Domestic_partnership
><: Child_abuse
>!: Child_abduction
    
```

Рис. 2 – Фрагмент траси виконання програми

Висновки.

У роботі запропоновано і реалізовано алгоритм формування моделей предметних областей шляхом автоматичного аналізу мережевого сервісу Wikipedia. Від статичних моделей предметних областей такий підхід відрізняється урахуванням динамічної зміни контенту бази даних цього сервісу, урахуванням нових понять, феноменів, що з’являються, зокрема в юридичній області, що розглядається. При цьому підході визначальними елементами є назви нових статей як маркери знань (теги), що доповнюються авторами матеріалів – учасниками проекту Wikipedia.



Можна зауважити, що система Wikipedia, як і система Google Scholar Citations, що розглядалася раніше [6; 7], є зручною щодо доступу до інформації, не передбачає створення власного профілю користувача для доступу до інформації, доступ є необмеженим.

Слід відзначити принципову відмінність запропонованої моделі автоматичного формування термінологічних мереж від існуючих, що базуються на особистій участі експертів при виборі конкретних вузлів і зв'язків. У випадку, що описується в роботі, дослідник для побудови мережі використовує лише крипицю знань, представлену у вигляді назви першого, ключового терміну-поняття. Після цього програма використовує знання, закладені авторами (редакторами) статей в Wikipedia, теги, що визначаються внутрішніми гіперпосиланнями. У цьому випадку експертне середовище істотно розширюється.

Модель застосовувалася для юридичної науки в рамках сервісу Wikipedia, але запропонований підхід можна використовувати і для інших наукових областей, або для інших текстових масивів, зокрема, баз даних нормативно-правової інформації. Враховуючи дослідження та розробку алгоритмів для системи Wikipedia постає питання застосування цього алгоритму для інших сервісів, зокрема у галузі права, що потребує проведення порівняльного аналізу ресурсів.

Додаток.

Найбільш вагомні терміни-поняття, що відповідають вибраним предметним областям

Constitutional law

| № | Сортування за вагою | Переклад | Сортування за PageRank | Переклад |
|----|---------------------------|--------------------------------------|---------------------------|-----------------------------|
| 1 | Judiciary | Судова влада | Constitutionalism | Конституціоналізм |
| 2 | The_Crown | Корона | Judiciary | Судова влада |
| 3 | Constitutional law | Конституційне право | The_Crown | Корона |
| 4 | Constitution_of_Canada | Конституція Канади | Constitutional law | Конституційне право |
| 5 | Parliament_of_Canada | Парламент Канади | Constitution_of_Australia | Конституція Австралії |
| 6 | Monarchy_of_Canada | Монархія Канади | Constitution_of_Canada | Конституція Канади |
| 7 | Prime_Minister_of_Canada | Прем'єр-міністр Канади | Parliament_of_Canada | Парламент Канади |
| 8 | Court_system_of_Canada | Судова система Канади | Monarchy_of_Canada | Монархія Канади |
| 9 | Elections_in_Canada | Вибори в Канаді | Prime_Minister_of_Canada | Прем'єр-міністр Канади |
| 10 | Canadian_electoral_system | Електоральна система Канади | Court_system_of_Canada | Судова система Канади |
| 11 | Chief_Justice_of_Canada | Головний суддя Канади | Elections_in_Canada | Вибори в Канаді |
| 12 | Constitutionalism | Конституціоналізм | Canadian_electoral_system | Електоральна система Канади |
| 13 | Canadian_federalism | Канадський парламентаризм | Chief_Justice_of_Canada | Головний суддя Канади |
| 14 | Canadian_Senate_divisions | Підрозділи Сенату Канади | Canadian_federalism | Канадський парламентаризм |
| 15 | Public_Service_of_Canada | Державна служба Канади | Canadian_Senate_divisions | Підрозділи Сенату Канади |
| 16 | Prorogation_in_Canada | Переєра у роботі парламенту в Канаді | 29th_Canadian_Ministry | 29-а Рада міністрів Канади |

| | | | | |
|----|----------------------------|----------------------------|------------------------|--|
| 17 | 29th_Canadian_Ministry | 29-а Рада міністрів Канади | 28th_Canadian_Ministry | 28-а Рада міністрів Канади |
| 18 | Cabinet_of_Canada | Кабінет міністрів Канади | Act_of_Settlement_1701 | Акт про спадкування престолу |
| 19 | Governor_General_of_Canada | Генерал-губернатор Канади | Prorogation_in_Canada | Перерва між парламентськими сесіями в Канаді |
| 20 | Patriation | Патріація | Statute | Статут |

Family Law

| № | Сортування за вагою | Переклад | Сортування за PageRank | Переклад |
|----|---------------------------|---------------------------------------|--------------------------|---------------------------------------|
| 1 | Cohabitation | Сожительство | Extended_family | Розширена сім'я |
| 2 | Emancipation_of_minors | Емансипація неповнолітніх осіб | Cohabitation | Сожительство |
| 3 | Conflict_of_divorce_laws | Конфлікт законів про розлучення | Emancipation_of_minors | Емансипація неповнолітніх осіб |
| 4 | Extended_family | Розширена сім'я | Conflict_of_divorce_laws | Конфлікт законів про розлучення |
| 5 | Adultery | Подружня зрада | Adultery | Подружня зрада |
| 6 | Incest | Інцест | Incest | Інцест |
| 7 | Infidelity | Невірність | Infidelity | Невірність |
| 8 | Domestic_partnership | Домашнє партнерство | Child_custody | Опіка над дітьми |
| 9 | Child_custody | Опіка над дітьми | Domestic_partnership | Домашнє партнерство |
| 10 | Child_support | Аліменти | Child_support | Аліменти |
| 11 | Family_law | Сімейне право | Child_neglect | Невиконання обов'язків щодо дитини |
| 12 | Child_abuse | Жорстоке поводження з дитиною | Family_law | Сімейне право |
| 13 | Divorce | Розлучення | Child_abuse | Жорстоке поводження з дитиною |
| 14 | Annulment | Анулювання | Divorce | Розлучення |
| 15 | Legal_separation | Роздільне проживання за рішенням суду | Annulment | Анулювання |
| 16 | Child_Protective_Services | Державне агентство в США CPS | Legal_separation | Роздільне проживання за рішенням суду |
| 17 | Conflict_of_marriage_laws | Конфлікт законів про розлучення | Child_neglect | Невиконання обов'язків щодо дитини |
| 18 | Paternity_fraud | Шахрайство з батьківством | Family_law | Сімейне право |
| 19 | Parental_child_abduction | Батьківське викрадення дітей | Child_abuse | Жорстоке поводження з дитиною |
| 20 | Custody_Evaluator | Оцінка, необхідна для опіки | Divorce | Розлучення |

Criminal Law

| № | Сортування за вагою | Переклад | Сортування за PageRank | Переклад |
|---|---------------------|-------------------|------------------------|-------------------|
| 1 | Contract | Контракт | War_crimes | Військові злочини |
| 2 | Property_law | Право власності | Forensic_psychology | Судова психологія |
| 3 | Criminal_law | Кримінальне право | Crime | Злочин |

| | | | | |
|----|-----------------------|---------------------------------------|------------------------|---------------------------------|
| 4 | Tort | Делікт | Law | Закон |
| 5 | Damages | Відшкодування збитків | Manslaughter | Вбивство |
| 6 | Trust_law | Довірча власність | Cohabitation | Співжиття |
| 7 | Product_liability | Відповідальність виробника | Contract | Контракт |
| 8 | Vicarious_liability | Субсидіарна відповідальність | Emancipation_of_minors | Емансипація неповнолітніх осіб |
| 9 | Trespasser | Правопорушник | Tort | Делікт |
| 10 | Criminal_conversation | Перелюбство | Property_law | Право власності |
| 11 | Malicious_prosecution | Зловмисне судове переслідування | Trust_law | Довірча власність |
| 12 | Eggshell_skull | Правило підвищеної вразливості | Criminal_law | Кримінальне право |
| 13 | Invasion_of_privacy | Порушення приватності | Damages | Відшкодування збитків |
| 14 | Malpractice | Недобросовісна практика | Product_liability | Відповідальність виробника |
| 15 | Negligent_entrustment | Недбале ввірення | Vicarious_liability | Субсидіарна відповідальність |
| 16 | Medical_malpractice | Відповідальність медичних працівників | Trespasser | Правопорушник |
| 17 | Breach_of_promise | Порушення обіцянки | Criminal_conversation | Перелюбство |
| 18 | Legal_malpractice | Незаконна судова практика | Malicious_prosecution | Зловмисне судове переслідування |
| 19 | Invitee | Запрошений | Eggshell_skull | Правило підвищеної вразливості |
| 20 | Duty_to_rescue | Обов'язок порятунку | Invasion_of_privacy | Порушення приватності |

Використана література

1. Онтологии и тезаурусы. Модели, инструменты, приложения / [Б.В. Добров, В.Д. Соловьев, Н.В. Лукашевич, В.В. Иванов]. – М. : Бином, 2009. – 173 с.
2. Ландэ Д.В., Снарский А.А. Подход к созданию терминологических онтологий // Онтология проектирования. – 2014. – № 2(12). – С. 83-91.
3. Чанышев О.Г. Автоматическое построение терминологической базы знаний : сб. трудов 10-й Всероссийской научной конференции [“Электронные библиотеки : перспективные методы и технологии, электронные коллекции” – RCDL’2008”]. – Дубна (Россия), 2008. – С. 85-92.
4. Zareen Saba Syed, Tim Finin, Anupam Joshi. Wikipedia as an Ontology for Describing Documents / Proc. 2nd Int. Conf. on Weblogs and Social Media. – Seattle (USA) : AAAI Press, March 2008. – Pp. 136-144.
5. Ландэ Д.В. Интернетика : навигация в сложных сетях : модели и алгоритмы / Д.В. Ландэ, А.А. Снарский, И.В. Безсуднов. – М. : Либроком (Editorial URSS), 2009. – 264 с.
6. Ландэ Д.В., Андрущенко В.Б. Побудова мереж співавторства фахівців з юриспруденції за даними сервісу Google Scholar Citations // Правова інформатика. – № 1(46)/2016. – С. 146-150.
7. Ландэ Д.В. Построение модели предметной области путем зондирования сервиса Google Scholar Citations // Онтология проектирования. – 2015. – Т. 5. – № 3(17). – С. 328-335.

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

УДК 343.211.3:004.738.5: 681.3.06

**БРИЖКО В.М.**, доктор філософії (Ph.D.) з юридичних наук,  
старший науковий співробітник

## ПРИВАТНІСТЬ ДАНИХ У ХМАРНИХ ТЕХНОЛОГІЯХ

**Анотація.** Про приватність та захист персональних даних в умовах розвитку новітніх технологій. Надано пропозиції щодо запровадження в Україні інституту права приватної власності людини на свої персональні дані.

**Ключові слова:** приватність, захист персональних даних, цифрові технології, приватна власність, інформаційне суспільство.

**Аннотация.** О приватности и защите персональных данных в условиях развития новейших технологий. Предоставлены предложения относительно внедрения в Украине института права частной собственности человека на свои персональные данные.

**Ключевые слова:** приватность, защита персональных данных, цифровые технологии, частная собственность, информационное общество.

**Summary.** On the privacy and personal data protection in terms of modern technologies development. Suggestions are provided in relation to introduction of institute of right of private ownership of a person on the personal information in Ukraine.

**Keywords:** privacy, personal data protection, digital technologies, information relations, information right, information society.

**Постановка проблеми.** Останніми роками в Інтернет-сфері поряд з “розумними” технологіями типу Інтернет речей [1], які характеризують те, що кількість матеріальних об’єктів, підключених до Інтернету, стала збільшуватися по відношенню до кількості людей, що взагалі користуються всесвітньою павутиною, набувають поширення й інші ІТ-технології, так звані “хмарні обчислення” або “хмарні сервіси-послуги”. Вони, в умовах збільшення об’ємів інформації та завдяки Інтернет, надають можливості обробки та зберігання значних обсягів даних не на жорстких дисках комп’ютерів, а на віддалених серверах [2]. Їх застосування свідчить про новий етап розвитку Інтернету, а разом з тим – про нові проблеми в сфері захисту персональних даних стосовно прав людини на недоторканність особистого (у європейському розумінні – “приватного”) життя.

Враховуючи те, що “спостерігається певна тенденція щодо спроб нівелювати право людини розпоряджатися власними персональними даними” [3], продовжує існувати поблажливе ставлення різних організацій до створення належних організаційно-правових умов захисту баз персональних даних, а також нерідка несанкціонована комерціалізація у їх збиранні та продажу, яка пропонується у Інтернеті<sup>1</sup>, проблеми захисту приватності людини, зокрема щодо сфери персональних даних, все більше ускладнюються та потребують удосконалення, про що йдеться, зокрема, у [4].

© Брижко В.М., 2016

<sup>1</sup> У наш час маркетинг персональних даних стає найбільшим посяганням на особисте життя. За оцінкою американських фахівців річний ринок персональних даних складає не менш як 3 мільярдів доларів [5]. Це означає, що в рамках інформаційного бізнесу сформувався сектор, що спеціалізується на зборі, обробці і продажу персональних даних. Комерційний успіх даного сектора полягає у тому, що зібрані у окремих осіб, нерідко не санкціоновано, персональні дані дозволяють мінімізувати витрати щодо цілеспрямованої реклами та продажу. Про становлення маркетингу персональних даних в Україні див. у [6].

**Аналіз досліджень.** У країнах Заходу, пострадянського простору та в Україні дослідження загального нормативно-правового впорядкування інформаційних відносин сфери обробки та використання персональних даних здійснювало багато осіб, про результати робіт деяких з них йдеться, зокрема, у [7 – 12].

Стосовно поширення та застосування хмарних (інформаційно-обчислювальних) технологій (послуг, сервісів) провідні позиції у світі займають країни США, Європейського Союзу. В Україні ці проблеми досліджували такі вчені, як Гнатюк С.Л., Гриценко В.И., Сейдаметова З.С., Темненко В.А., А.А. Урсатьєв [13 – 15] та ін. Так щодо захисту персональних даних, Гнатюк С.Л. справедливо визначає що: “Розглядати індустрію хмарних послуг ....в контексті захисту персональних даних спонукають два моменти: 1) завдяки особливостям свого функціонування хмарні сервіси створюють цілком специфічне середовище, в якому традиційні нормативно-правові механізми, практики та підходи стають здебільшого неефективними; 2) у глобальному вимірі індустрія хмарних обчислень вже зараз перетворилася на критично важливий ресурс ІТ-сфери, але, за однастайними прогнозами, найближчими роками її питома вага в бізнесі і багатьох інших сферах життя зросте в рази” [13].

**Метою статті** є узагальнення поглядів та розробка пропозицій у забезпеченні приватності в умовах застосування хмарних технологій.

**Виклад основного матеріалу.** Поняття “приватність” походить від англ. слова privacy (“прайвесі”), хоча має глибокі історичні корені. Численні посилання на це суспільно-соціальне явище можна знайти у Біблії. Приватність була об’єктом загального захисту людини за часів давньоєврейської культури, класичної Греції, древнього Китаю. Захист, головним чином, зводився до можливостей “усамітнення”.

У наш час “приватність” тісно пов’язана з людською гідністю й іншими цінностями, такими як свобода слова та свобода доступу до інформації, таємницею кореспонденції тощо. У певному розумінні, усі права людини є аспектами права на приватність.

Разом з зазначеним, узагальненого тлумачення слова “приватність” немає. У останніх документах ЄС стосовно захисту персональних даних, зокрема у Регламенті ЄС 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних та про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)” [16], слово “приватність” не використовується. Чинне українське законодавство поняття “приватність” в контексті “персональні дані” або “інформація” не застосовує. При цьому, згідно ст. 271 Цивільного кодексу України “приватне життя” віднесено до “особистих немайнових прав”, а згідно ст. 325 ЦК України “приватність” стосується лише права власності на майно, тобто на матеріально-речові об’єкти [17].

Нещодавно прийнято Закон України “Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль” від 31.08.16 р. № 0108, де у ст. 8 сформульовано, що мова йде про “сферу охорони приватних персональних даних з метою захисту персональних даних” [18].

Зміст вищезазначеної фрази створює загальне розуміння про що мова, але, на жаль, не дає ясного уявлення, у чому полягає різниця між “приватними персональними даними” і просто “персональними даними”.

В українській “Юридичній енциклопедії” 2003 р. [19] слово “приватність” відсутнє.

У тлумачному словнику Ожегова С.І. [20, с. 585] є слово “приватный”, яке тлумачиться як “частный”, що визначається як “личный, не общественный, не государственный”, “принадлежащий отдельному лицу, не обществу, не государству” та



“относящийся к личному, индивидуальному владению” [20, с. 875]. Згідно українсько-російського словнику українське слово “приватний” перекладається на рос. як “частный (относящийся к одному лицу)”, “личный” [21, с. 454] та навпаки [21, с. 267]. При цьому, у “приватних” відносинах суб’єкти самостійно їх упорядковують, діють на власний розсуд, який підпорядковується принципу “дозволено все, що не заборонене законом”. Тобто мірилом диспозитивності (упорядкованості) відносин є насамперед закон.

Стосовно словосполучення “персональні дані”, то воно походить від старогрецького слова “*prosopon*” – “маска актора”, Потім, під впливом латині, цим словом стали позначати соціальний аспект людини, як біосоціальної істоти, і з’явилося слово “*persona*” – “особа”, від якого утворилося слово “*personalitas*” – “особистість” [7, с. 20-22], що визначає індивідуально виражені якості окремої людини.

Виходячи з зазначеного, можна, на наш погляд, зробити висновок про те, що “приватні персональні дані” – це персональні дані які належать відповідній людині (особі), як продукту суспільних відносин, у будь-яких галузях публічного та приватного права. У цьому аспекті можна вести мову про наявність у них якості власності.

Сьогодні зустрічаються різні узагальнення категорії (поняття) “приватність”: таємниця, відокремленість або самотність приватного життя, право на приватне життя, недоторканність приватного життя. На наш погляд, філософський зміст цього слова включає, зокрема, наступне: *“приватність – це право бути наданим самому собі. Кожна людина має право на свій “куточок” в просторі, захищений від довільних посягань з боку інших. ...Можливо, з юридичної точки зору, найточніший варіант змістової сутності зазначеного терміну – це право на недоторканність приватного життя”* [24, с. 9].

В 1999 році, у звіті “Приватність і права людини”, зробленому суспільними організаціями “Privacy International and Electronic Privacy Information Center” [18], було запропоновано поділити приватність на такі чотири види: *фізична приватність* – стосується захисту людини від фізичного насильства, тортур, примусових медичних втручань та ін.; *територіальна приватність* – стосується недоторканності житла людини, обмежень на втручання в домашнє та навколишнє її середовище; *інформаційна приватність* – передбачає встановлення правил збору, використання, поширення та захисту відомостей про особу (персональних даних); *приватність комунікацій* – розуміється все те, що пов’язано з техніко-технологічними засобами та способами у аспекті телефонних розмов, електронних повідомлень, поштового листування та інших видів інформаційно-комунікаційних зв’язків.

В умовах програмно-технологічного розвитку Інтернету приватність комунікацій дедалі більше пов’язується з інформаційною приватністю, тобто з тим, що передбачає захист персональних даних людини, інформаційної безпеки суспільства та держави. Ця тенденція безпосередньо стосується нових поглядів у застужанні Інтернету – за його допомогою, організації переходу від використання окремих програмно-апаратних засобів, що належать окремим суб’єктам (компаніям), на модель створення та використання “відкритого об’єднання хмарних обчислень” [26], тобто “хмарних технологій”, “хмарних сервісів” тощо.

Концепція “хмарних” (інформаційно-обчислювальних) технологій (послуг, сервісів) з’явилася в 1960 році, коли американський учений, фахівець з теорії ЕОМ, Джон Маккарті виказав припущення, що “коли-небудь комп’ютерні обчислення (обчислювальні потужності) стануть надаватися подібно комунальним послугам” [27].

Метафора “хмара” давно використовується фахівцями з технологій для зображення на мережових діаграмах складної обчислювальної інфраструктури (або ж Інтернету як такого), що приховує свою внутрішню організацію за певним інтерфейсом. Проте термін “хмарні обчислення” з’явився на світ відносно недавно.

Згідно з результатами аналізу пошукової системи Google, термін “хмарні обчислення” (“Cloud Computing”) почав поширюватися з кінця 2007 року, поступово витісняючи словосполучення “грід-обчислення” (“Grid Computing”). Однією з перших компаній, що дала світу даний термін, стала компанія IBM, яка розгорнула на початку 2008 року проект “Blue Cloud” і спонсорувала Європейський проект “Joint Research Initiative for Cloud Computing” [28].

У 2011 році у Лабораторії інформаційних технологій Національного інституту стандартів і технологій (NIST) Міністерства торгівлі США були розроблені “Рекомендації NIST (спеціальна публікація 800-145)” для використання федеральними відомствами та неурядовими організаціями – “Визначення хмарних обчислень” (автори Петр Мелл і Тимоти Гренс) [29].

У п. 1.2 Рекомендацій NIST зазначається, що хмарні обчислення є новою парадигмою. Вона визначає нову глобальну архітектурну моделі функціонування всесвітньої мережі та її можливості щодо доступу до загального пулу (“об’єднання”) обчислювальних ресурсів, що конфігуруються (наприклад, серверів, систем зберігання, обробки, додатків і послуг). Тобто, згідно наданого NIST визначення, *хмарні обчислення – це інформаційно-технологічна концепція, що має на увазі забезпечення повсюдного і зручного мережевого доступу на вимогу до загального пулу обчислювальних ресурсів (мереж передачі даних, серверів, пристроїв зберігання даних, додатків і сервісів – як разом, так і окремо), що конфігуруються, які можуть бути оперативно надані і звільнені з мінімальними експлуатаційними витратами або зверненнями до провайдера.*

Як ми розуміємо та іншими словами, поява хмарних технологій є свідченням переходу інформатизації суспільства від насиченості інформаційної інфраструктури апаратними і програмними продуктами до світової інформаційної кооперації – об’єднання напрацьованого інформаційно-ресурсного і програмного потенціалу в єдине віртуальне інформаційне середовище із намаганнями збереження індивідуальної автономії.

Визначення NIST вказує на важливі аспекти хмарних обчислень і покликане служити основою для широкого обговорення того, що таке хмарні обчислення (сервіси) та які стратегії їх розгортання, щоб найкращим чином їх використовувати, без обмежень конкретних методів надання послуг або бізнес-операцій. Основні характеристики хмарних обчислень передбачають:

*самообслуговування на вимогу.* Споживач може самостійно та без взаємодії з постачальником послуг (провайдером) визначати обчислювальні потреби (серверний час, швидкість доступу до мережевого пристрою обробки та зберігання даних);

*універсальність доступу до мережі.* Передбачає для споживача можливість доступу у мережу завдяки використанню різних цифрових пристроїв (мобільні телефони, планшети, ноутбуки та ін.);

*об’єднання ресурсів.* Передбачає об’єднання ресурсів постачальником послуг в єдиний пул, з метою обслуговування декількох споживачів для динамічного перерозподілу потужностей між ними. Споживач не має можливості контролювати розподіл ресурсів, який здійснює постачальник послуг, але має можливість вказувати на потребу підключення до відповідного центру обробки та зберігання даних;

*гнучкість (еластичність) надання послуг.* Передбачають їх автоматичне надання з можливостями змін у кількості та часі, згідно потреб споживача;

*обчислення послуг (облік споживання).* Передбачає автоматичне обчислення наданих постачальником послуг згідно відповідного типу сервісу та тарифу (обсяг даних, що зберігаються та обробляються, кількість транзакцій, пропускна спроможність, кількість користувачів).

До основних видів послуг щодо хмарних обчислень Рекомендації NIST відносять:

*програмне забезпечення як послуга* (з англ. – Software-as-a-Service). Споживачу надається можливість використання прикладного програмного забезпечення (далі – ПО) провайдера, що працює в хмарній інфраструктурі і доступного з різних клієнтських пристроїв. Контроль і управління основною фізичною і віртуальною інфраструктурою хмари, зокрема мережі, серверів, операційних систем, зберігання, або індивідуальних можливостей додатку здійснюється хмарним провайдером;

*платформа як послуга* (з англ. – Platform-as-a-Service). Включає надання послуг з сукупності застосування апаратних засобів та ПО. Споживачу надається можливість використання хмарної інфраструктури для розміщення базового ПО для подальшого розміщення на ньому інших додатків (власних, розроблених на замовлення або придбаних). До складу таких платформ (набору утиліт, що забезпечують надання хмарних сервісів) входять інструментальні засоби створення, тестування і виконання прикладного ПО (систем управління базами даних, зв'язку, середовища виконання мов програмування), що надаються провайдером. Контроль і управління основною фізичною і віртуальною інфраструктурою хмари, зокрема мережі, серверів, операційних систем, зберігання здійснюється провайдером, за винятком раніше встановлених додатків, а також параметрів платформної конфігурації середовища;

*інфраструктура як послуга* (з англ. – Infrastructure-as-a-Service). Надається як можливість використання хмарної інфраструктури для самостійного управління ресурсами обробки, зберігання даних, мережами і ін. обчислювальними ресурсами. Споживач може встановлювати і запускати інше програмне забезпечення, яке включає операційні системи, платформне і прикладне ПО. Споживач може контролювати операційні та віртуальні системи зберігання даних і встановлені додатки, а також володіти обмеженим контролем за набором доступних мережевих сервісів (наприклад, між мережевим екраном). Контроль і управління основною фізичною і віртуальною інфраструктурою хмари, зокрема мережі, серверів, типів операційних систем та систем зберігання даних здійснюється провайдером.

Згідно Рекомендацій NIST основними схемами (моделями) розгортання хмарних обчислень є:

*приватна хмара.* Стосується послуг для виключного використання однією організацією, що може забезпечувати декількох споживачів (бізнес-одиниць);

*співтовариство хмари.* Стосується послуг для використання конкретним співтовариством споживачів (організаціями), що мають загальні проблеми;

*відкрита хмара.* Стосується послуг для відкритого використання широкою громадськістю. Вона функціонує на території постачальника послуг та може знаходитися у власності будь-якої організації;

*гібридна хмара.* Є композицією з двох або більшої кількості інфраструктур (приватних, суспільних або державних), пов'язаних між собою стандартизованими або запатентованими технологіями.

У квітні 2012 року Міжнародна робоча група, у складі Комісарів захисту даних різних країн [30], з метою підвищення захисту даних у сфері телекомунікацій і засобів масової інформації, представила робочий документ з питань конфіденційності і захисту даних хмарних технологій (“Сопотський меморандум”) [31]<sup>2</sup>.

На основі цього документу у вересні 2012 року Європейська Комісія опублікувала прес-реліз “Нова стратегія для управління європейського бізнесу та продуктивності уряду за допомогою хмарних обчислень” [32]. Стратегія призначена для прискорення та збільшення використання хмарних обчислень у всіх галузях економіки. Основні положення стратегії, яка отримала назву “Розв’язання потенціалу хмарних обчислень в Європі” [33; 34], передбачають:

- створення для хмарних обчислень єдиних технічних та інших стандартів щодо можливостей функціональної сумісності та обігу даних;
- створення загальноєвропейських схем сертифікації для хмарних провайдерів;
- розвиток безпечних і справедливих моделей умов контракту для хмарних обчислень, включаючи домовленості про рівень обслуговування.

У прес-релізі до “Сопотського меморандуму” прямо зазначається, що сьогодні, в умовах відсутності загальних стандартів і чітких контрактів, багато потенційних користувачів утримуються від прийняття хмарних рішень. Вони не впевнені, які стандарти і сертифікати громадяни повинні шукати, щоб задовольнити їхні вимоги і правові зобов’язання, наприклад, щоб гарантувати, що їх персональні дані або дані їх клієнтів перебувають у безпеці, або що додатки сумісні один з одним. Хмарні провайдери і користувачі бажають мати більш чіткі правила щодо постачання хмарних сервісів, наприклад, щодо питань юрисдикції правових спорів, переміщення даних і програмного забезпечення між різними постачальниками хмарних технологій та ін.

Існують різні думки та висновки фахівців щодо переваг, недоліків та проблем у застосуванні хмарних послуг, див. [13 – 15; 35 – 39]. Наведемо основні з них.

*Доступність.* У принципі, хмарні сервіси доступні всім, хто має підключення комп’ютера до Інтернету. Це дозволяє користувачам (звичайно компаніям) економити на закупівлі високопродуктивних, дорогих комп’ютерів. Немає необхідності в придбанні ліцензійного ПО, його налаштуванні і оновленні – споживач має нагоду через браузер зайти на сервіс і, заплативши за фактичне використання, користуватися його послугами. Також співробітники компаній стають мобільнішими, оскільки можуть отримати доступ до свого робочого місця, використовуючи ноутбук, планшет або смартфон. З іншого боку, хмарні сервіси потребують постійного з’єднання з Інтернет, а також можуть обмежувати у використанні ПО провайдера, яке споживач не завжди може пристосувати під свої цілі.

*Вартість.* Передбачає можливість зниження витрат та зменшення штату на обслуговування інфраструктури у окремих компаніях, економії на придбанні ліцензій на ПО, що дозволяє користувачам зменшити витрати на закупівлю дорогого устаткування.

---

<sup>2</sup> Першим документом ЄС про упорядкування суспільних відносин у телекомунікаціях є Директива 97/66/ЄС Європейського Парламенту і Ради “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” від 15.12.97 р. [40, с. 337-334] (призначення – захист мереж від спаму і гарантій таємниці зв’язку загального користування), яка є доповненням до Директиви 95/46/ЄС Європейського Парламенту і Ради “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.95 р. ([40, с. 273-293] (призначення – захист усіх типів персональних даних за будь-яких засобів їх обробки тощо), що скасовані згідно нових правил і порядку захисту персональних даних (див. [4; 16]).

Однак, для побудови малими компаніями власної хмари необхідні значні початкові матеріальні ресурси.

*Обчислювальні потужності.* При аналізі великих обсягів даних користувач хмарної системи використовує її обчислювальні здібності, заплативши тільки за фактичний час використання.

*Надійність функціонування.* Хмарна система може мати надійність, оскільки звичайно обладнана в центрах обробки даних, які мають резервні джерела живлення, охорону, професійних працівників, регулярне резервування даних, високу пропускну спроможність Інтернет-каналу, певну стійкість до несанкціонованого доступу при належному її забезпеченні. Проте при недбалому ставленні ефект може бути цілком протилежним. Більш того, що стосується надійності зберігання інформації, то фахівці стверджують, що якщо інформація, що зберігається в хмарі, втрачена, то вона втрачена назавжди.

Разом з зазначеним, є ствердження про те, що “плюси хмари” полягають у: а) легкості у користуванні – інформація відкривається лише тим, хто має на це відповідний дозвіл, та б) існує повний захист конфіденційної інформації – можливості послуги дозволяють клієнту чітко регламентувати коло користувачів серверу та маніпуляції, які здійснюються з його даними. Тобто, в разі, коли хтось із співробітників провайдера вирішить скопіювати чи відправити якийсь файл з серверу, не маючи на те дозволу, його дії будуть заблоковані [38].

Як узагальнюється в [27], з точки зору провайдера, завдяки об’єднанню ресурсів і непостійному характеру споживання з боку споживачів, хмарні обчислення дозволяють економити на масштабах, використовуючи значно менші апаратні ресурси, аніж у моделі “один споживач – один пристрій”, а за рахунок автоматизації процедур виділення ресурсів істотно знижуються витрати на абонентське обслуговування. З точки зору споживача, хмарні технології в принципі дозволяють отримати послуги з високим рівнем доступності і низькими ризиками непрацездатності, забезпечити швидке масштабування обчислювальної системи завдяки еластичності без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури і, нарешті, заощадити на абонентській платі, оскільки в хмарних сервісах вона нараховується лише за використанні ресурси.

*Недоліки хмарних рішень* відносяться, в основному, до проблеми довіри до постачальника сервісу, від якого залежить як безперебійна робота, так і збереження даних користувача. Існує побоювання того, що з поширенням цієї технології виникне проблема неможливості контролю даних, коли інформація, залишена користувачем, буде зберігатися роками, або без його відома, або він буде не в змозі змінити якусь її частину. Прикладом є сервіси Google, де користувач не в змозі видалити не потрібні йому сервіси і навіть видалити окремі дані, створені в деяких з них (FeedBurner, Google Friend Connect). Поки споживач послуг не має засобу видалення своїх власних даних на подібних серверах [27].

Загалом, до головних недоліків у застосуванні хмарних послуг можна віднести проблеми інформаційної безпеки, конфіденційності та захисту персональних даних.

*Інформаційна безпека.* Хмарні сервіси, як вважають деякі фахівці, самі по собі є надійною системою. Проте, при проникненні до неї зловмисник може отримати доступ до величезного сховища даних. Ще один мінус – це використання систем віртуалізації, в яких застосовують ядра стандартних ОС таких, як Windows та ін., що може сприяти проникненню вірусів.

*Конфіденційність та захист даних.* Захист даних, що зберігаються у публічних хмарах, в теперішній час викликає багато суперечок, але в більшості випадків експерти сходяться у тому, що не слід зберігати цінніші документи у публічній хмарі, оскільки поки немає технології, яка б гарантувала 100 % захист даних. Як зазначається у роботі Гнатюка С.Л. [13], сьогодні саме проблеми захисту персональних даних на ринку хмарних послуг є найбільш серйозним бар’єром для його подальшого розвитку й про те мова йде у “Сопотському меморандумі” [31], а саме:

- технологія все ще у стадії розробки і не апробована остаточно;
- досі немає міжнародної угоди про єдину термінологію, хоча технологія є транскордонною, а обробка даних фактично стала глобальним процесом;
- діяльність провайдерів є недостатньо прозорою і не може бути повністю відстеженою. Це значно ускладнює оцінку ризиків і створення єдиних правил гри;
- дотримання конфіденційності, недоторканності інформації та режиму доступу до неї не може бути проконтрольоване у хмарах;
- під час передачі персональних даних вони потрапляють під юрисдикції, в яких не передбачено їх адекватного захисту;
- провайдери та їх партнери можуть використовувати дані у своїх інтересах без повідомлення про це володільця та його згоди; локальні (національні) контролюючі інститути з захисту даних фактично не мають можливості нагляду за процесом їх обробки провайдерами хмарних послуг.

До цього, як вказується у [41], має місце значний відсоток не добросовісних гравців на ринку хмарних послуг. Так, 77 % опитаних в рамках дослідження організацій щонайменше один раз стикалися з шахрайськими сервісами, а 40 % з цього числа стали жертвами викрадення конфіденційних даних.

Наведений, зокрема, перелік підштовхує до попереднього висновку: сьогодні захист приватності не має однозначного організаційно-нормативного вирішення. В кращому разі він закінчується рекомендаціями і побажаннями, як необхідно будувати систему захисту. І більшою мірою це пов’язано з давно відомою проблемою складнощів упорядкування відносин в Інтернеті. Також зрозуміло, що традиційні норми упорядкування відносин в віртуальному середовищі не бажають слідувати тим юридичним канонам, які створені століттями раніше й лише для світу матеріальних речей. Й сьогодні це наочно демонструють так звані “хмарні технології” та слабке, взагалі, упорядкування відносин у віртуальності, яке, на превеликий жаль, продовжує мати повчальний, а не юридичний характер, що відповідав би реаліям змін у сучасності.

Про необхідність нових підходів у створенні системи нормативно-правового регулювання відносин у сфері захисту персональних даних мова йдеться давно, зокрема у [7 – 10; 42]. Основна пропозиція передбачає надання суб’єкту персональних даних специфічного та фіктивного для інформаційно-електронного середовища “права приватної власності” на його дані, але лише на визначених законом умовах (обмеженнях). Важливо підкреслити, що інститут власності на майно<sup>3</sup> завжди був та є потужним (якщо не основним) юридичним інструментом, який реально в змозі

---

<sup>3</sup> З кінця позаминулого століття в юриспруденції існує ще інститут “власності”, у якому застосовується термін “інтелектуальна власність”, хоча “власності” як такої він не передбачає. Він був запроваджений для задоволення насамперед економічних потреб. Прийнято, що вживання цього терміну правомірне, якщо поставитися до нього як до умовної категорії – “юридичної фікції”, яка має економічний сенс. Строго кажучи, термін “інтелектуальна власність” визначає не права власності, а права по використанню результатів творчої праці.

стримувати негативні соціально-економічні фактори у суспільних відносинах, якщо він обов’язково забезпечений чітко визначеними заходами притягнення до відповідальності порушників власності.

Виходячи з головних принципів захисту персональних даних, відзначимо два аспекти:

а) Обробка персональних даних допускається, якщо на те є згода суб’єкта персональних даних. Згода суб’єкта-людини на обробку її персональних даних передбачає, як ми вважаємо, наявність у неї специфічно-унікального права, а саме – права на володіння, користування і розпорядження своїми персональними даними. А це ніщо інше як тріада повноважень традиційного права власності – згідно ст. 2 Закону України “Про власність” від 07.02.91 р. № 697-12: “Право власності – це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження майном”. Якщо персональні дані збирають та торгують ними, як і де забажається, то в такому разі вони стають майном, що надає прибуток. Звідси й виникає специфічність “власності” на персональні дані, яке можна розглядати у якості “позитивного змісту прав людини на свої персональні дані”.

б) З іншого боку, для задоволення потреб забезпечення державних, суспільних та комерційних інтересів не може існувати монополії людини на свої персональні дані (тобто, абсолютна власність). Щоб це врахувати, обробка персональних даних допускається, якщо це дозволяє Закон. Іншими словами, за визначених Законом умов право власності людини на свої персональні дані скасовується, що визначає, у цьому випадку, “негативний зміст прав людини на свої персональні дані”.

Сполучення позитивного і негативного змісту прав людини на свої персональні дані дозволяє ввести категорію “право приватної власності людини на свої персональні дані”. Людина має право повного (виключного) користування своїми персональними даними. При передачі персональних даних іншим суб’єктам може переходити тільки право обмеженого їх використання. Таким чином, у сенсі нового підходу у юридичному захисті персональних даних, ми замкнули принцип недоторканності особи з принципом, який свідчить про те, що основою свободи є власність і замах на неї рівнозначний обмеженню свободи та будь-яких видів приватності.

В якості додаткового пояснення головної суті пропозиції щодо запровадження в законодавство категорії “право приватної власності людини на свої персональні дані” зазначимо наступне.

Єдиною реальною системою, здатною упорядковувати відносини в будь-якому суспільстві, була і є “система власності”. Виходячи з цього, слід в основу всієї системи захисту персональних даних покласти “стрижень” власності і виходячи з її змістовної сутності врахувати це у нормах законодавства, які стосуються прав людини. Ось тоді і можна говорити про дотримання ст. 3 Конституції України, яка визначає пріоритетність прав людини, і про можливість “регуляції у віртуальності”. Тільки коли у людей виникає звичайне питання – “моє це або не моє”, прокидається свідомість, інтерес і починають функціонувати сформульовані в нормах положення, вимоги моралі і культури.

### **Висновки.**

1. Поява хмарних технологій є свідченням переходу інформатизації суспільства від насиченості інформаційної інфраструктури апаратними і програмними продуктами до світової інформаційної кооперації – об’єднання напрацьованого інформаційно-ресурсного і програмного потенціалу в єдине віртуальне інформаційне середовище із намаганнями збереження індивідуальної автономії. Проте, останнє досить складно здійснити в окремих малих компаніях. Для побудови власної (приватної) хмари, або участі у побудові так званого “співтовариства хмари” чи “гібридної хмари”, необхідні

значні початкові матеріальні ресурси. Тому можна вважати, що на сьогодні хмарні технології привабливіші для тих великих компаній, яким необхідно обробляти значні обсяги даних та тим, які можуть отримувати більш значні вигоди від їх застосування, в умовах звичайної потреби в зміцненні бізнес-позиції (можливо, посиленні монополізації) на відповідному ринку, зокрема, за допомогою маркетингу та збору будь-яких приватних (персональних) даних.

2. Враховуючи те, що у розвинених країнах поширюється пропаганда новітніх цифрових технологій та здійснюються техніко-технологічні та нормативні пошуки в упорядкуванні суспільних відносин в телекомунікаційних мережах, що зумовлює зростання ризиків, пов'язаних з автоматичною обробкою та зберіганням даних, та необхідністю врахування нових міжнародних правил щодо невтручання не лише у сферу захисту персональних даних, але, взагалі, у сферу приватного життя, постає потреба у розробці спеціальних правових, регулятивних та технічних положень щодо застосування в Україні нових технологій у телекомунікаціях та Інтернеті. Це може визначати потребу у внесенні змін до законів “Про телекомунікації” та “Про захист персональних даних”.

3. Вважаємо, що при розробці нормативно-правових змін, у законодавство України мають бути імплементовані положення не тільки “Пакету захисту даних” Європейського Парламенту і Ради від травня 2016 року (див. [4]), але й деякі положення, які стосуються принципів упорядкування відносин у телекомунікаціях, про що йде мова у Директиві 97/66/ЄС Європейського Парламенту і Ради від 15.12.97 р. “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” [25, с. 337-334].

Вбачається, що найбільш важливим може вважатися необхідність встановлення конкретних обов'язків провайдерів, що забезпечують роботу з персональними даними. Для створення умов забезпечення приватності у хмарних технологіях, постачальник (провайдер) послуг повинен вживати відповідних техніко-технологічних та організаційних заходів для гарантування інформаційної безпеки при наданні послуг в тому, що стосується функціонування мережі, яку він використовує (застосовує). Він також повинен обов'язково повідомляти споживачів послуг про існуючі ризики порушення захисту персональних даних та можливі засоби захисту.

4. Щодо культури захисту персональних даних в Україні, про що у статті зазначалося раніше (див. [3]), на превеликий жаль, говорити багато не доводиться. Можливо, кодекси поведінки, запровадження яких передбачене вказаним “Пакетом”, хоч якось будуть спрямовувати до формування в організаціях більш відповідальної поведінки до захисту приватних та, зокрема, персональних даних.

5. В контексті сутності категорії “приватність”, як вважаємо, “приватні персональні дані” – це персональні дані які належать відповідній людині (особі), як продукту суспільних відносин, у будь-яких галузях публічного та приватного права. Звідси витікає можливість вести мову про наявність у них якості власності.

Проте, головне в питаннях нормативного упорядкування відносин щодо приватності для будь-яких видів персональних даних – це співвідношення свободи і захисту.

Аргументи на користь абсолютної свободи та демократії звичайно переконливі, але не самоочевидні.

Пріоритетами держави є порядок, стабільність, безпека. Але необмежена свобода “сильної” влади веде до свавілля, деградування суспільства і людини, фальшивого морального стану, де звичайно застосовуються різні інформаційно-психологічні засоби впливу на розум і поведінку людини з метою маніпулювання її свідомістю.



З іншого боку, пріоритетами індивідуума є свобода, ініціатива і захищеність. Придушення або суб'єктивне обмеження свободи веде суспільство до поглиблюванню адміністративного зловживання і корупції, нігілізму у сприйнятті обіцянок влади.

Характер об'єктивної суперечливості та необхідність врахування як одного, так і іншого пріоритету, вимагає пошуку компромісу, пошуку балансу у правах та інтересах особи, суспільства та держави.

6. У контексті відміченого вище та виходячи з положень ст. 3 Конституції України, яка визначає природні права людини “найвищою соціальною цінністю”, персональним даним може бути наданий специфічний та унікальний статус права власності, що юридично виступає у формі “приватного права власності людини на свої персональні дані”, монополія на яку обмежується законом в інтересах дотримання прав та основоположних свобод інших осіб, а також – дотримання балансу прав людини, суспільства і держави.

У основі цього твердження лежить те, що справжня демократія та правова держава – це не розподіл благ (через, зокрема, субсидії, тарифи тощо), а встановлення і регулювання права власності, орієнтованого на розвиток малого підприємництва. Питання лише в ідейній сутності механізму політико-соціального застосування цього права, з якого витікають рівень демократії, свободи та реального захисту прав людини.

### Використана література

1. Баранов О., Брижко В. Захист персональних даних в сфері Інтернет речей // Інформація і право. – № 2(17)/2016. – С. 75-81.
2. Cloud computing. – Режим доступу : [https://en.wikipedia.org/wiki/Cloud\\_computing](https://en.wikipedia.org/wiki/Cloud_computing)
3. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві : зб. матеріалів виступів на наук.-практ. конференції [“Проблеми захисту прав людини в інформаційному суспільстві”], (Київ, 1 липня 2016 р.) / НДІП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ “КПІ” ; упорядн. Фурашев В.М., Петряев С.Ю. – К. : Вид-во “Політехніка”, 2016. – С. 6-8.
4. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах // Інформація і право. – № 3(18)/2016. – С. 45-57.
5. Михеев В. Проблема правовой защиты персональных данных. – Режим доступу : <http://www.kiev-security.org.ua/box/4/136.shtml> ; Цена персональных данных. – Режим доступу : <http://www.i2r.ru/article.shtml?id=1384>
6. Брижко В. Економічні та правові аспекти захисту персональних даних // Правова інформатика. – № 1(29)/2011. – С. 25-33.
7. Права человека и защита персональных данных / А. Баранов. В. Брыжко, Ю. Базанов. – Харьков : Фолио, 2000. – 280 с.
8. Брижко В. Правовий механізм захисту персональних даних : монографія ; за ред. М. Швеця та Р. Калюжного. – К. : Парлам. вид-во, 2003. – 120 с.
9. Інформаційне право та правова інформатика в сфері захисту персональних даних / В. Брижко, М. Швець [та ін.] ; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2005. – 451 с.
10. е-майбутнє та інформаційне право / [В. Брижко, Ю. Базанов та ін.] ; за ред. д.е.н., проф. М. Швеця. – [2-е вид., доп.]. – К. : ТОВ “ПанТот”, 2006. – 234 с.
11. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / [В. Брижко, А. Радянська, М. Швець]. – К. : Триумф, 2006. – 256 с.
12. Електронний банкінг у контексті захисту персональних даних / В. Брижко, Ю. Базанов [та ін.] : за ред. чл.-кореспондента АПрН України М. Швеця. – К. : ТОВ “ПанТот”, 2008. – 141 с.

13. Гнатюк С.Л. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів “хмарного” обчислення) : аналітична записка. – Режим доступу : <http://www.niss.gov.ua/articles/1090>
14. Гриценко В.И., Урсатьев А.А. Cloud computing и облачная модель представления ИТ-услуг // Кибернетика и вычислительная техника. – 2013. – Вып. 171. – С. 5-19.
15. Сейдаметова З.С., Темненко В.А. Cloud computing : основные концепции и тенденции развития // Ученые записки Крымского инженерно-педагогического университета. – Вып. 28. – Симферополь : НИЦ КИПУ, 2011. – С. 43-48.
16. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу : <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>
17. Цивільний кодекс України : Закон України від 16.01.03 р. № 435-IV // Відомості Верхової Ради України (ВВР). – 2003. – №№ 40-44. – Ст. 271, 325.
18. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль : Закон України від 31.08.16 р. № 0108. – Режим доступу : [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=59911](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59911)
19. Юридична енциклопедія : в 6 т. / редкол. : Ю.С. Шемшученко (голова редкол.) та ін. – К. : Видавництво “Українська енциклопедія, 2003. – Т. 5 : П–С. – 736 с.
20. Ожегов С.И. Словарь русского языка : 70000 слов / С.И. Ожегов ; под ред. Н.Ю. Шведовой. – [21-е изд., перераб. и доп.]. – М. : Рус. яз., 1989. – 924 с.
21. Там же, с. 875.
22. Галич Д.І. Російсько-український і українсько-російський словник / Д.І. Галич, Олійник І.С. – [6-е вид. стереотипне]. – К.: МП “Феникс”, 1993. – 560 с.
23. Там же, с. 267.
24. Смирнов С. Приватность / С. Смирнов. – (Межрегиональная группа “Правозащитная сеть”). – М. : “Права человека”, 2002. – 96 с.
25. Priacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. – Режим доступу : <http://www.epic.org>
26. Модель коллектора и архитектура для открытого объединения облачных вычислений / [В. Рохвергер, Д. Брейтланд, Е. Леви, А. Галис, К. Нагин, И. Льюренте, Р. Монтеро, Ю. Вульфсталь, Е. Елтрох, Ю. Касерес, М. Бен-Иегуда, В. Эммерих, Ф. Галан] // Журнал исследований и разработок IBM, 2009. – 53 (4): 4:1-4:11.DOI:10.1147 / JRD.2009.5429058.
27. Хмарні обчислення. – Режим доступу : [https://uk.wikipedia.org/wiki/%D0%A5%D0%BC%D0%B0%D1%80%D0%BD%D1%96\\_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F](https://uk.wikipedia.org/wiki/%D0%A5%D0%BC%D0%B0%D1%80%D0%BD%D1%96_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F)
28. Joint Research Initiative for Cloud Computing. – Режим доступу : [http://www.k504.xai.edu.ua/html/ucheba/rss/RSS\\_Lekciya\\_10.pdf](http://www.k504.xai.edu.ua/html/ucheba/rss/RSS_Lekciya_10.pdf)
29. The NIST Definition of Cloud Computing. – Recommendations of the National Institute of Standards and Technology. – Special Publication 800-145. – Gaithersburg, MD : National Institute of Standards and Technology, January 2011. – 7 p. – Режим доступу : [http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145\\_cloud-definition.pdf](http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf)
30. International Working Group on Data Protection in Telecommunications (IWGDPT). – Режим доступу : <http://clck.ru/8aXVe>; <https://datenschutz-berlin.de//content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>
31. Working Paper on Cloud Computing – Privacy and data protection issues (“Sopot Memorandum”). International Working Group on Data Protection in Telecommunications 51st meeting, 23-24 April 2012, Sopot (Poland). – Режим доступу : <http://clck.ru/8aJ9c>
32. Нова стратегія для управління європейського бізнесу та продуктивності уряду за допомогою хмарних обчислень : прес-реліз Європейській Комісії, 2012 р. – Режим доступу : [http://europa.eu/rapid/press-release\\_IP-12-1025\\_en.htm?Locale=en](http://europa.eu/rapid/press-release_IP-12-1025_en.htm?Locale=en)

33. Unleashing the Potential of Cloud Computing in Europe. European Commission / Brussels, 27.9.2012 COM(2012) 529 final. – Режим доступу : [http://ec.europa.eu/information\\_society/activities/cloudcomputing/docs/com/com\\_cloud.pdf](http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf)
34. European Commission. Unleashing the Potential of Cloud Computing in Europe – What is it and what does it mean for me? Мемо. – Режим доступу : [http://www.abbl.lu/sites/abbl.lu/files/FAQCloud\\_Computing.pdf](http://www.abbl.lu/sites/abbl.lu/files/FAQCloud_Computing.pdf)
35. Хмарні технології. Переваги і недоліки. – Режим доступу : <http://valtek.com.ua/ua/system-integration/it-infrastructure/clouds/cloud-technologies>
36. Облачные вычисления : лекция. – Режим доступу : [http://www.k504.xai.edu.ua/html/ucheba/rss/RSS\\_Lekciya\\_10.pdf](http://www.k504.xai.edu.ua/html/ucheba/rss/RSS_Lekciya_10.pdf);
37. Що корисного принесли хмарні CRM-системи? – Режим доступу : <http://j.parus.ua/ua/379>
38. Хмарні технології на захисті бізнесу. – Режим доступу : <http://www.epravda.com.ua/publications/2012/05/7/322884>
39. Digital Agenda : New strategy to drive European business and government productivity via cloud computing. – Режим доступу : [http://europa.eu/rapid/press-release\\_IP-12-1025\\_en.htm?Locale=en](http://europa.eu/rapid/press-release_IP-12-1025_en.htm?Locale=en)
40. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв'язку з автоматизованою обробкою даних : посіб. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.
41. Мошеннические облачные сервисы – бич 77 % компаний. – SecurityLab.ru. 23.01.13. – Режим доступу : <http://www.securitylab.ru/news/436587.php>
42. Персональні дані та право власності // Українське право. – 2002. – № 1. – С. 152-157; Про економічний аспект захисту персональних даних у контексті права власності на інформацію // Правова інформатика. – № 1(9)/2006. – С. 45-54; До питання е-торгівлі та захисту персональних даних // Правова інформатика. – № 1(13)/2007. – С. 14-27; Інформаційна безпека : економічні та правові аспекти проблеми захисту персональних даних // Інформація та безпека. – № 1-2(5-6)/2011. – С. 67-72. – (Інформ.-аналіт. журнал ТОВ “Академпрес”); Захист персональних даних : реалії та практика сучасності // Інформація і право. – № 3(9) 2013. – С. 31-48; Особливості ознак та матеріальна специфічність у сфері інформаційного права // Інформація і право. – № 1(13)/2015. – С. 15-26.

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

Інформаційна і національна безпека

УДК 343.211.3:004.738.5:681.3.06

ПИЛИПЧУК В.Г., доктор юридичних наук, професор,
член-кореспондент НАПрН України
БРИЖКО В.М., доктор філософії (Ph.D.) з юридичних наук,
старший науковий співробітник

**ІНФОРМАЦІЙНА БЕЗПЕКА ТА ПРИВАТНІСТЬ
У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ**

Анотація. *Стаття присвячена проблемі інформаційної безпеки приватності у сфері захисту персональних даних в умовах формування інформаційного суспільства. Здійснено теоретичне опрацювання пропозиції щодо запровадження в Україні інституту права приватної власності людини на свої персональні дані.*

Ключові слова: *права, свободи і інформаційна безпека людини, приватність, право власності, захист персональних даних.*

Аннотация. *Статья посвящена проблеме информационной безопасности приватности в сфере защиты персональных данных в условиях формирования информационного общества. Осуществлена теоретическая проработка предложения относительно внедрения в Украине института права частной собственности человека на свои персональные данные.*

Ключевые слова: *права, свободы и информационная безопасность человека, приватность, право собственности, защита персональных данных.*

The article is devoted to the problem of information safety of privacy in the field of personal data protection in the conditions of forming of information society. The further theoretical work on suggestions in relation to introduction of institute of right of private ownership of a person on the personal information in Ukraine is carried out.

Keywords: *right, freedoms and information safety of person, privacy, right of ownership, personal data protection.*

Постановка проблеми. Сучасне розуміння демократичного, соціального, правового суспільства виходить з поваги і потреби захисту прав, свобод та безпеки людини на основі принципів законності та верховенства права. Повага і неухильне забезпечення прав, свобод і безпеки людини – гарантія від несанкціонованого втручання у її приватне життя та одна із головних функцій держави. Дотримання права на приватність – основа справедливості та злагоди в суспільстві.

Відповідно до статті 32 Конституції України “Ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини” [1].

Вказаний конституційний припис отримав конкретизацію в 2010 році у Законі України “Про захист персональних даних”, який призначений для упорядкування інформаційних відносин у сфері обігу персональних даних, та визначає його “спрямованість на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних” [2].

Таким чином, право людини на недоторканність особистого (у європейському розумінні – “приватного”) життя відповідно до законодавства України передбачає правовий захист відомостей про неї, за якого основним об’єктом правовідносин є персональні дані. Вирішення проблеми забезпечення інформаційної безпеки приватності персональних даних в усіх сферах життєдіяльності людини, суспільства і держави в сучасних умовах формування інформаційного суспільства та євроінтеграції України постає одним із найважливіших чинників становлення інформаційного права та розвитку правової системи держави.

Аналіз досліджень і публікацій. Питання впорядкування суспільних відносин у сфері захисту персональних даних досліджувалися низкою вітчизняних та іноземних вчених, про яких див. зокрема [3 – 13]. Водночас, в Україні ця проблема залишається вкрай актуальною.

Метою статті є узагальнення поглядів щодо проблеми забезпечення приватності та права власності у сфері захисту персональних даних в умовах інформаційного суспільства.

Виклад основного матеріалу. В сучасних умовах, як свідчить аналіз, найбільшого прогресу у розбудові інформаційного суспільства досягли США, Японія і держави-члени Європейського Союзу. Саме у цих країнах поряд із стрімким розвитком інформаційних технологій, інформаційних ресурсів, продукції та послуг велика увага приділяється забезпеченню прав і безпеки людини в інформаційній сфері, насамперед, захисту персональних даних.

Зокрема, у розробленому в США ще 1973 року Кодексі сумлінного поведіння з інформацією було сформульовано основні принципи роботи з персональними даними [7]:

- не повинно існувати жодної системи накопичення відомостей про індивіда, саме існування якої тримається в таємниці;
- індивід повинен мати можливість дізнатися, які відомості наявні про нього та як вони використовуються; запобігати тому, щоб інформація, одержана про нього з однією метою, надавалася для іншої мети без його згоди; виправити або доповнити відомості про себе;
- будь-яка організація, що збирає, зберігає, використовує або поширює відомості стосовно конкретних осіб, зобов’язана забезпечити достовірність даних для наміченої мети та вжити розумних пересторог для запобігання неправомірного використання даних.

Впровадження в усі сфери життєдіяльності людини, суспільства, держави та міжнародної спільноти інформаційно-комунікаційних технологій, електронних систем і баз даних поступово трансформувало американське розуміння поняття “приватність” у бік “права на інформаційний суверенітет особи”, тобто, право людини визначати ким, коли, з якою метою та яким чином інформація про неї буде використовуватися іншими особами.

У наш час право на “приватність” розглядається як фундаментальне (але не абсолютне) право людини в Загальній декларації прав людини ООН (1948 р.), Європейській Конвенції “Про захист прав людини та основоположних свобод” (1950 р.), Міжнародному пакті про громадянські й політичні права (1966 р.) та в ін. актах [4, с. 37-48]. Приватність тісно пов’язана з людською гідністю та іншими ключовими цінностями, такими як свобода слова, свобода доступу до інформації, захистом персональних даних, таємницею кореспонденції тощо. У певному розумінні, усі права людини є аспектами права на приватність.

Разом з цим, загальноприйнятого визначення терміна “приватність” поки не існує. У документах ЄС стосовно захисту персональних даних, зокрема у Регламенті ЄС 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних та про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)”, слово “приватність” не використовується [14].

Проте, у статті 8 Закону України “Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль” від 31.08.16 р. № 0108 йдеться про “сферу охорони **приватних персональних даних** з метою захисту персональних даних” [15].

Зустрічаються різні узагальнення терміну “приватність”, зокрема: відокремленість, таємниця або самотність приватного життя, право на приватне життя, недоторканність приватного життя тощо. Заслужують на підтримку висновки, що сутність цього слова передбачає наступне: *“приватність – це право бути наданим самому собі. Кожна людина має право на свій “куточок” у просторі, захищений від довільних посягань з боку інших. З погляду права найточніший варіант змістової сутності зазначеного терміну – це право на недоторканність приватного життя”* [5].

У 1999 році був запропонований поділ приватності на чотири види [6]:

1) **фізична приватність** – стосується захисту людини від фізичного насильства, тортур, примусових медичних втручань, записів та ін.;

2) **територіальна приватність** – стосується недоторканності житла людини, обмежень на втручання в домашнє та навколишнє її середовище. Певним захистом володіють не тільки будинки і квартири людей, але і робочі місця, готельні номери, купе потягу і т.д.;

3) **інформаційна приватність**. Під цим розуміється встановлення правил збору, використання, поширення та захисту відомостей про особу (персональних даних) від їх нецільового та несанкціонованого використання, що визначає: а) право людини бути захищеною від втручання в її особисте життя та стосунки чи її родини через публікацію інформації; б) право людини знати, ким, коли, яким чином і в яких межах інформація про неї може бути або буде використовуватися іншими особами.

4) **приватність комунікацій** – усе, що пов’язано з техніко-технологічними засобами і способами забезпечення телефонних розмов, електронних повідомлень, особистого поштового листування та інших видів інформаційно-комунікаційних зв’язків. При цьому, в умовах програмно-технологічного розвитку Інтернету приватність комунікацій все більше пов’язується з інформаційною приватністю, тобто з тим, що передбачає захист персональних даних людини, а також інформаційної безпеки людини, суспільства і держави. Ця тенденція безпосередньо стосується нових поглядів у застужанні Інтернету, які отримали назву “Інтернет речей” [10] та “хмарні технології” [16]. Технології типу “Інтернет речей” характеризують те, що кількість матеріальних об’єктів, підключених у світі до Інтернету, стала збільшуватися по відношенню до кількості людей, які взагалі користуються глобальними комунікаційними мережами. А “хмарні технології” визначають перехід від використання окремих програмно-апаратних засобів, що належать окремим суб’єктам (компаніям), на модель створення та використання “відкритого об’єднання хмарних обчислень”, тобто “хмарних технологій”, “хмарних сервісів”.

До основних проблем новітніх технологій, що набувають активного поширення, також слід віднести інформаційну безпеку і захист персональних даних. Інформаційно-комп’ютерні технології значно посилюють ризики порушення приватності персональних даних внаслідок того, що вони передбачають накопичення і зберігання даних не на жорстких дисках комп’ютерів, а на віддалених серверах, з наступною можливістю використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних, забезпечення їх захисту від несанкціонованого доступу і використання та необхідність формування нової системи правового регулювання.

Європейська Комісія намагається удосконалювати міжнародну систему захисту персональних даних не тільки на базі директивних вказівок, але і шляхом встановлення правил прямої дії (Регламенту), що визначає безпосередній порядок регулювання цієї діяльності [11]. Однак, аналіз нормативного забезпечення захисту приватності продовжує мати неоднозначне і складне організаційно-правове вирішення. Часто усе закінчується рекомендаціями про те, як необхідно будувати систему захисту даних. Більшою мірою це пов'язано з проблемою упорядкування відносин в Інтернеті. Як відомо, традиційні норми упорядкування відносин у віртуальному середовищі не бажають слідувати юридичним канонам, створеним століттями раніше для світу матеріальних речей. Нині це наочно демонструють так звані “хмарні технології” і досить слабе врегулювання відносин у віртуальній сфері, яке не відповідає реаліям сучасності.

Історія XX сторіччя була історією подальшого просування людства на шляху індивідуальних свобод. Нині немає жодної демократичної конституції у світі, яка б не містила положень щодо забезпечення природних і невід’ємних прав людини та основоположних свобод, включаючи і висуваючи на перший план свободу *приватної власності*.

Приватна власність – основа економіки та життєдіяльності людини та суспільства. У соціально-економічному сенсі вона означає відносини щодо розподілу та володіння матеріальними чи нематеріальними благами. У правовому сенсі – це сукупність норм, які юридично закріплюють і захищають приналежність будь-яких благ визначеній фізичній особі-власнику, а також передбачають обсяг і зміст її прав, способи та межі їх здійснення. Від законодавчого забезпечення захисту права власності та механізмів його реалізації значною мірою залежить фактичне додержання прав, свобод і безпеки людини, а також збалансованість прав людини та законних інтересів суспільства і держави.

Вперше загальна ідея прав людини на життя, приватну власність і свободу була висловлена англійським вченим Дж. Локком (1632 – 1704 рр.) як природне право індивідуума [17]. Вона визначала *передумову позитивних прав людини* – належності їй права володіння, користування і розпорядження своїм майном. Не заперечуючи за суттю, генерал-комісар Генрі Айртон, зять Олівера Кромвеля, у роки кардинальної політичної перебудови XVII століття, стверджував: “*Ні закони Бога, ні закони природи не дають мені власність. Власність устанавлюється людською конституцією*” [4, с. 170]. Надалі філософське обґрунтування ідей Конституції США 1787 року визначило сутність приватної власності: “*Право на життя, свободу і власність – найважливіші природні права, без яких люди не мають можливості забезпечити собі повноцінне існування*” [18].

Право власності має більш давню історію, ніж конституціоналізм. Конституційні ідеї та конституційна практика, як відомо, виникли в епоху революцій в США, Англії і Франції у XVII – XVIII століттях. А зміст права власності бере початок із Стародавнього Риму та розкривається через *тріаду повноважень: володіння, користування і розпорядження майном*. Механізм одержання права власності на майно ґрунтується на можливості володіти речами, тобто фактично “тримати їх у руках”. Цей механізм у прямому сенсі не придатний для регулювання інформаційних відносин, пов’язаних із результатами інтелектуальної (творчої) діяльності (раніше вона визначалася як “духовна творчість”), тобто – з інформацією або відомостями.

Якщо інформація відповідає критеріям охороноспроможності, то вона здійснюється на засадах надання власнику виключного права використання (згідно патентного чи авторського права). Виключність права використання, зокрема винаходу, додає правам патентовласника обмежений монопольний статус.

На відміну від права “абсолютної” власності на майно виключне право використання має предметну межу, що передбачає обмеженість дії патенту в часі і території. Це також означає, що на дії (збирання, зберігання, введення в господарський обіг), вчинені по відношенню до об’єктів *авторського права* (ст. 8 Закону України “Про авторське право і суміжні права” від 23.12.93 р. № 3792-ХІІ – книги, брошури, статті, виступи, лекції, комп’ютерні програми, бази даних тощо) та *патентного права* (ст. 5 Закону України “Про правову охорону прав на винаходи і корисні моделі” від 15.12.93 р. № 3687-ХІІ – пристрої, способи, речовина та ін.) державою встановлена заборона, якщо на те немає згоди особи, якій належать авторські чи патентні права. Тобто, зміст категорії “*виключне право*” визначається як право не давати будь-яким іншим суб’єктам можливість використання, насамперед, інформації чи відомостей, що одержали від держави право охороноспроможності (патентоспроможності). Такі засади сформульовані в Мюнхенській Конвенції “Про видачу європейського патенту” (1973 р.), Люксембурзькій Конвенції “Про європейський патент держав-членів Європейського Співтовариства” (1975 р.), патентних законах США, Великої Британії, Скандинавських країн.

Звісно, що основними складовими інтелектуальної власності є авторське і патентне право. Але, як зазначалося, об’єкти охорони у них різні. Це пов’язано з тим, що авторське право призначене для охорони “форми”, тобто зовнішнього вигляду об’єкту (його не цікавить про що мова). А патентне право призначене для охорони “змісту”, тобто внутрішнього функціонального наповнення об’єкта, для відтворення у майно, яке визначається формулою винаходу у вигляді інформації. Й хоча “інтелектуальна власність” розглядається єдиною сферою права, насправді вона займається охороною різних об’єктів. Ця охорона об’єктів має аналогічний, але далеко не тотожний зміст. Саме тому навряд буде створена загальна конвенція для сфери інтелектуальної власності.

Згідно з нормами міжнародного права і законодавства України щодо захисту персональних даних, персональні дані – це відомості чи сукупність відомостей про людину. Ці відомості ототожнюють відповідну інформацію, до якої окремо застосувати “право власності” на речові об’єкти і “виключне право використання” щодо інтелектуальної власності не уявляється можливим. Персональні дані (інформація, відомості, дані про особу) через свою унікальність, можливість застосування у різних сферах життєдіяльності і потребою делікатного поводження з ними розміщуються мовби на “перетині” (на межі) вказаних юридичних інститутів. Схематично це може бути представлено за допомогою логічних кругів Ейлера [19]:



В основу зазначеного покладено категорію “*право приватної власності людини на свої персональні дані*” Запропонована категорія уособлює правовий статус людини (фізичної особи) щодо права володіти, користуватися і надавати згоду на використання (розпорядження) своїми персональними даними, а також щодо обмеження цього права у випадках, визначених Конституцією і законами України.

Сумісність змісту повноважень людини на свої персональні дані у контексті розглянутих інститутів “права власності на майно” (де інформація розглядається як об’єкт права на майно) та інституту “виключного права використання” (де інформація розглядається як об’єкт права на захист і обробку творів) дозволяє запропонувати нову юридичну категорію і створити новий інструмент правового регулювання інформаційних відносин (інститут) у сфері захисту персональних даних.

Інститут права приватної власності фізичної особи на свої персональні дані має сенс не завдяки автоматичному перенесенню юридичних інструментів, що визначають право власності на майно і право на використання інформації про твори, у сферу інформаційних відносин, а внаслідок використання принципів (основних ідей, підходів), що містяться у цих інструментах. Їх спільне застосування, як видається, може надавати персональним даним правовий статус (оболонку) права власності, тобто – нову якість у сфері захисту прав, свобод і безпеки людини. За такого підходу можна вести мову і про підвищення рівня захисту прав людини та її основоположних свобод.

Необхідно до вказаного додати, що одним із перших цільових законів про захист персональних даних був закон німецької Землі Гессен (1970 р.). На його основі, у § 3 Федерального Закону Німеччини “Про захист даних” від 20.12.90 р. було зазначено, що *“інформація про особу – це конкретні дані про особисті чи майнові відносини встановленої або установлюваної особи”* [4, с. 120].

Тут варто звернути увагу на досить важливий аспект. У формулюванні німецького законодавця має місце думка про те, що чинність закону поширюється не лише на особисту (приватну) інформацію, здатну ідентифікувати фізичну особу, але й на економічні, майнові відносини. Положення вказаного закону Німеччини про те, що *“інформація про фізичну особу – це конкретні дані про ...майнові відносини”* важливе тим, що воно ще у 1990 році визначило тенденції і перспективи розвитку права у сфері захисту персональних даних, а також вказало на принципову можливість захисту персональних даних за допомогою правового засобу, що використовує *принцип регулювання суспільних відносин на основі права власності*.

Це дуже важливе законодавче посилення передбачило складні сучасні і майбутні події, пов’язані з процесами подальшої трансформації індустріального суспільства в інформаційне суспільство та суспільство знань. Наслідком цих подій є кардинальні зміни соціально-економічних відносин, що вже вимагає нових, не традиційних підходів і засобів захисту інформації та персональних даних.

У контексті зазначеного заслуговують на увагу висновки американських вчених С. Уоррена і Л. Брандейса [8], які стверджують про наявність загроз “приватності” людини з боку нових винаходів і методів ведення бізнесу (ці загрози є реальними і для України [12]), та необхідності створення спеціального “права на приватність”. Автори розуміли, що технічний прогрес і розвиток технологій в майбутньому внесе корективи у правове регулювання питання “приватності”. Виходячи з посилки щодо актуальності своїх передбачень, вони зазначали, що це право повинно бути гнучким і здатним прилаштовуватись до потреб сьогодення. Наводячи правові аргументи щодо права особи на “приватність”, С. Уоррен і Л. Брандейс, зокрема, зазначали: *“Закони повинні визнавати і захищати право на приватність. Захист права на приватність порівнюється із захистом права інтелектуальної власності”*. Хоча, на наш погляд, персональні дані важко прямо віднести до об’єктів творчості.

Можна також звернути увагу на судову практику США щодо реалізації принципу приватності у сфері персональних даних.

Одним із перших прецедентів, створеним на основі реалізації “права на приватність”, стало рішення Верховного Суду штату Джорджія у справі “Павесіч vs. Нью Ігланд Лайф Іншуранс Ко.” (1905 р.). Задовольняючи позов чоловіка, зображеного без його згоди в рекламному оголошенні, суд визначив об’єкт і мету правового захисту таким чином: *“Той, хто бажає жити життям відносного усамітнення, має право обрати час, місце та способи, у які він буде піддавати себе громадському спостереженню”* [20].

Надалі, у 1928 році, суддя Верховного суду США Л. Брандейс офіційно заявив про наявність в Конституції США *“права бути залишеним у спокої”* [9]. У подальшому за справою “GRISWOLD vs. CONNECTICUT” суддя Верховного суду США Дуглас вивів “право на приватність” з перших п’яти поправок до Конституції США, визнавши, що ці поправки “охороняють різні аспекти недоторканності приватного життя”. Резюмуючи рішення суду він зазначив: *“Ми маємо справу з правом на недоторканність приватного життя, яке старше, ніж Білль про права”* [21].

Вважаємо за важливе підкреслити у вищенаведеному те, що вказані думки та юридичні рішення формувалися у часи, коли слів інформатизація, телекомунікації, Інтернет тощо взагалі не існувало, і мова йшла лише про “приватну недоторканість” у звичайній, не віртуальній, життєдіяльності.

Кожна людина від народження наділена певними біологічними якостями. Завдяки цим якостям і наступній життєдіяльності вона здобуває соціальні якості, які разом з біологічними відображаються у різних відомостях, у тому числі у персональних даних, які супроводжують її все життя і поступово губляться після смерті. Зміст персональних даних містить інформаційний та, що стає дедалі більш характерним для нашого часу, – економічний аспект, який відображає право власності людини на будь-які відомості про себе. Проте нині риторичним залишається питання, *кому саме належить інформація про будь-яку людину*. Персональні дані фізичної особи юридично не є її власністю, з усіма відповідними економічними наслідками. До речі, до недавнього часу поняття “інформаційні ресурси”, “персональні дані” були відсутні, а пов’язані з ними економічна, фінансова, банківська та інші комерційні складові не брались до уваги.

Економічний зміст персональних даних виражається в тому, що зі становленням і функціонуванням внутрішнього ринку, який передбачає рух інформаційних ресурсів, технологій, продукції і послуг, виникає необхідність руху персональних даних за допомогою інформаційно-комп’ютерних технологій і мереж та необхідність у забезпеченні захисту їх соціальної, споживчої та мінової вартості. Тобто захисту соціально-економічних інтересів людини і, тим самим, захисту прав, свобод та безпеки.

Інформація в усьому світі завжди коштувала та коштує грошей. Ринкові відносини передбачають не безоплатну передачу інформації-товару, а взаємовигідний економічний обмін в умовах вільної конкуренції. Персональні дані конкретної людини ототожнюють відповідну про неї інформацію, яка може представляти економічний інтерес і може бути товаром, хочемо ми того чи ні, наприклад, якщо вкладена праця по акумулюванню відомостей у автоматизованих системах, базах даних чи картотеках. Але цей товар не має відповідного юридичного визначення і не підпадає під дію норм інституту інтелектуальної власності повною мірою, тому що персональні дані не є результатом творчості.

Зважаючи на те, що інтереси будь-яких суб’єктів і конкретної людини можуть не збігатися, а її персональні дані можуть використовуватися для задоволення потреб політичної, економічної, фінансової, комерційної та будь-якій іншій діяльності, ці дані повинні мати належні правові, організаційні і технологічні засоби захисту від їх несанкціонованого використання, а також одержати якісно новий статус – статус об’єкта

права власності відповідної фізичної особи. Таке бачення забезпечення прав людини надає додатковий соціально-економічний захист в умовах розвитку економічної інтеграції поширення та поглиблення процесів інформатизації, зростання активності при формуванні інформаційних ресурсів, державних реєстрів та різноманітних баз персональних даних.

З огляду на викладене можна дотримуватися гіпотези про те, що *захист персональних даних об'єктивно ґрунтується на спеціальному та специфічному методі упорядкування суспільних відносин, який передбачає комплексне застосування принципів регулювання права власності на матеріальні об'єкти і права інтелектуальної власності. Тобто, персональні дані можуть бути визначені особливим видом приватної власності, що юридично виступає в умовній формі права власності, монополія на яку обмежується виключно законом.* Важливим у вказаному, як вважаємо, є те, що запропонований підхід може слугувати підґрунтям для упорядкування інформаційних відносин щодо усіх інших видів приватності, що створює передумови **уніфікації різних систем захисту**.

Зазначене, як видається, цілком відповідає положенням статті 11 Конвенції Ради Європи № 108 згідно з якою *“Жодне положення цієї глави (Глава II – Основоволожні принципи захисту даних – від авт.) не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб'єктам даних більший ступінь захисту, ніж передбачений цією Конвенцією”* [22].

Заслуговує на увагу і рішення Конституційного Суду України, що *“інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною”* [23]. Ще раніше у 1997 році Конституційний Суд України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К.Г. Устименка) відніс до *конфіденційної інформації** такі відомості як освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані [24].

Про принципову можливість та правомірність реалізації розглянутих пропозицій у національному законодавстві свідчать і положення статті 22 Конституції України згідно з якою *“права і свободи людини і громадянина, закріплені цією Конституцією, не є вичерпними”*. Також варто враховувати, що у редакції Закону України “Про інформацію” від 23.06.05 р. у статті 54 було визначено, що *інформаційний суверенітет України забезпечується виключним правом власності України на інформаційні ресурси*. Й це право власності здійснюється через права її суб'єктів – громадян, суспільства і держави.

Висновки.

1. З погляду філософії, проблема інформаційної безпеки та приватності у сфері захисту персональних даних – це, насамперед, проблема захисту людини від реальних і потенційних загроз та зловживань “інформаційною владою” у будь-якій сфері життєдіяльності суспільства і держави.

* Примітка. Згідно Державного стандарту України “Технічний захист інформації. Терміни та визначення” від 1997 р. (ДСТУ 3396.2-97): *“конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов”*. Тобто мова йде про триаду повноважень права власності.

2) Фізичні особи об’єктивно мають право власності на свої персональні дані, яке, на відміну від права власності на матеріальні об’єкти, що надане конституцією, має природно-конституційний зміст і має бути закріплене юридично.

3) В умовах активного розвитку процесів інформатизації, захист персональних даних може і повинен бути забезпечений не лише організаційними та технологічними засобами, але і правовими засобами, що ґрунтуються на принципах регулювання суспільних відносин на майно, речі, шляхом створення особливого інституту права власності (приватної власності) людини на свої персональні дані.

Поряд із зазначеним, як видається, потребують теоретико-правового і законодавчого опрацювання такі актуальні питання:

- пошук балансу між забезпеченням права власності людини на її персональні дані та потребою реалізації визначених Конституцією і законами України функцій держави, що здійснюються в інтересах громадян і суспільства;

- законодавче визначення персональних даних, віднесених до *конфіденційної інформації*, впровадження передбачених законодавством механізмів їх захисту та юридичної відповідальності за правопорушення у цій сфері;

- заборона органам, установам, закладам, підприємствам та організаціям *вимагати у громадян право вільного збирання, обробки і передачі третім особам їх персональних даних без письмової згоди та без повідомлення цих осіб про кожну таку дію;*

- закріплення *прав громадян контролювати та відкликати, уточнювати чи видаляти свої персональні дані в будь-яких системах і базах даних (крім державних реєстрів), а також у глобальних комунікаційних мережах.*

В цілому, за нашими оцінками, що потребують подальшого наукового опрацювання, джерелом права власності на персональні дані є природно-конституційне право людини на унікальні, особливі й делікатні відомості, які не лише ототожнюють чи ідентифікують людину, характеризують її особистість, але й містять у собі предмет споживчої та мінової вартості. Виходячи зі світових тенденцій забезпечення прав і свобод людини та беручи до уваги, що право власності – це один із найважливіших інститутів будь-якої системи права, а право людини на персональні дані належить їй від народження і є результатом природно-конституційної даності, виникає необхідність і правомірність у формуванні ***інституту права приватної власності людини на свої персональні дані***, як основної складової загальної системи захисту прав людини. Розглянуті пропозиції, як видається, формують “стрижень” розвитку системи захисту персональних даних (тобто, нові принципи, логіку і перспективи), що потребуватиме подальшого теоретичного опрацювання на предмет законодавчого врегулювання відносин у сфері захисту персональних даних.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254/96. – Ст. 3. – К.: Інформаційно-видавниче агентство “ІВА”, 1996. – 52 с. – С. 3.
2. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481.
3. Защита персональных данных / А. Баранов, В. Брыжко, Ю. Базанов. – К. : Національне агентство з інформатизації при Президентові України, ВАТ КП ОТІ, 1998. – 128 с.
4. Права человека и защита персональных данных / А. Баранов. В. Брыжко, Ю. Базанов. – Харьков : Фолио, 2000. – 280 с.
5. Смирнов С. Приватность / С. Смирнов. – (Межрегиональная группа “Правозащитная сеть”). – М. : “Права человека”, 2002. – 96 с. – С. 9.

6. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. – Режим доступу : [//www.epic.org](http://www.epic.org)
7. Solove D.J. Information privacy law : Textbook / D.J. Solove, M. Rotenberg. – New York : Aspen Publishers, 2003. – Р. 470.
8. Уоррен С., Брандейс Л. Право на приватність // Право США. – № 1-2/2013. – С. 151-152.
9. Яременко О.І. Право на таємницю приватного життя людини в умовах становлення в Україні інформаційного суспільства. – Режим доступу : <http://www.lawyer.org.ua/?w-p&i-10&d-362>
10. Баранов О., Брижко В. Захист персональних даних в сфері Інтернет речей // Інформація і право. – № 2(17)/2016. – С. 75-81.
11. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах // Інформація і право. – № 3(18)/2016. – С. 45-57.
12. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві : зб. матеріалів виступів на наук.-практ. конференції [“Проблеми захисту прав людини в інформаційному суспільстві”], (Київ, 1 липня 2016 р.) / НДПП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ “КПІ” ; упорядн. Фурашев В.М., Петряев С.Ю. – К. : Вид-во “Політехніка”, 2016. – С. 6-8.
13. Мельник К.С. Іноземний та вітчизняний досвід становлення інституту захисту персональних даних // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2(12). – С. 100.
14. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016. – Режим доступу : <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>
15. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль : Закон України від 31.08.16 р. № 0108. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webp_r0c4_1?pf3511=59911
16. The NIST Definition of Cloud Computing. – Recommendations of the National Institute of Standards and Technology. – Special Publication 800-145. – Gaithersburg, MD : National Institute of Standards and Technology, January 2011. – 7 р. – Режим доступу : http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
17. Юридична енциклопедія : в 6 т. / редкол. Ю. С. Шемшученко (голова редкол.) та ін. – К. : Видавництво “Українська енциклопедія, 2001. – Т. 3 : К–М. – С. 520.
18. Бельсон Я. История государства и права США / Я. Бельсон, К. Ливанов. – Л. : Изд. Ленинградского университета, 1982. – 167 с.
19. Кириллов В.И. Логика : учеб. для юридич. вузов и фак. ун-тов / В.И. Кириллов, А.А. Старченко. – [2-е изд., доп.]. – М. : Высш. шк., 1987. – С. 118-121.
20. Рішення Верховного Суду штату Джорджія у справі “Павесіч vs. Нью Ігланд Лайф Іншуранс Ко.” від 1905 р. (Pavesich vs. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905)) // Information privacy law : Textbook / D.J. Solove, M. Rotenberg. – New York : Aspen Publishers, 2003. – 795 р.
21. U.S. Supreme Court “GRISWOLD vs. CONNECTICUT”, 381 U.S. 479 (1965). – Режим доступу : <http://supreme.justia.com/cases/federal/us/381/479/case.html>
22. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data : Amendment to Convention ETS No. 108 allowing the European Communities to accede. – Strasbourg, 28.1.1981. – Режим доступу : <http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm>

23. Рішення Конституційного Суду України від 20.01.12 р. № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. – Режим доступу : <http://zakon1.rada.gov.ua/laws/show/v002p710-12>

24. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К.Г. Устименка) від 30 жовтня 1997 року // Офіційний вісник України. – 1997. – № 46. – С. 126.

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

УДК 004.77:681.3.06

КАЧИНСЬКА К.А., аспірант Інституту телекомунікацій і глобального інформаційного простору НАН України

## ЗАСОБИ ІНТЕРНЕТ-КОМУНІКАЦІЙ ЯК ВАЖЛИВИЙ ІНСТРУМЕНТ МАСОВОЇ МАНІПУЛЯЦІЇ СВІДОМІСТЮ

**Анотація.** У статті проаналізовані найпоширеніші методи маніпулювання свідомістю особи, суспільства та держави та використання з цією метою різних засобів Інтернет-комунікацій. Розглядаються найбільш вживані засоби Інтернет-комунікацій, що в останнє десятиріччя перетворилися на частину не лише культурного, але й інформаційного простору.

**Ключові слова:** інформація, засоби Інтернет-комунікацій, пропаганда, соціальні мережі, сугестивні впливи.

**Аннотация.** В статье проанализированы наиболее распространенные методы манипулирования сознанием личности, общества и государства и использование с этой целью различных способов Интернет-коммуникаций. Рассматриваются различные аспекты использования Интернет-коммуникаций, которые в последнее десятилетие превратились в часть не только культурного, но и информационного пространства.

**Ключевые слова:** информация, способы Интернет-коммуникаций, пропаганда, социальные сети, суггестивные воздействия.

**Summary.** The article analyzes the methods of manipulating human, social and the state conscience and using various Internet Communications for this purpose. It also discusses various aspects of using Internet technologies that have become the part of not only cultural, but also information space in the last decade.

**Keywords:** information, means of the Internet Communications, propaganda, social networks, suggestive influence.

**Постановка проблеми.** Сучасний період розвитку людської спільноти характеризується новим етапом еволюції суспільних процесів, який в умовах світової економічної кризи та зростання масштабів тероризму й антитерористичних заходів спрямований на прагнення розвиненого індустріального суспільства до вдосконалення своїх соціальних структур і систем забезпечення безпеки. Ключовими умовами, що формують систему механізмів запобігання сугестивного впливу на спільноту, є докладний аналіз маніпулятивних технологій, а також класифікація засобів Інтернет-комунікацій<sup>1</sup>, за допомогою яких він здійснюється. Враховуючи наведене вище, без здійснення такого аналізу видається неможливою успішна реалізація основної мети Стратегії кібербезпеки України – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

**Аналіз останніх публікацій.** Значний вклад у дослідження проблем масової маніпуляції свідомістю здійснили такі вчені як Грачев Г., Зинов'єв А., Кара-Мурза С., Расторгуев С. та ін. В Україні дослідженню питань, пов'язаних із Інтернет-комунікацією та кібербезпекою, присвячені роботи Зими І., Литвиненко О., Нагорного А., Почепцова Г., Присяжнюка М., Сенченко М. та ін., про результати робіт яких йдеться, зокрема, у [43].

© Качинська К.А., 2016

<sup>1</sup> Інтернет-комунікація – це такі методи спілкування, за яких інформація передається по каналах Інтернет з використанням нових технологій – передача голосу, відео, документів, миттєвих повідомлень, файлів тощо.

Проте, розвиток новітніх Інтернет-технологій потребує подальшого дослідження засобів та методів сучасного маніпулювання свідомістю та інформаційно-психологічного впливу на особу, суспільство та державу.

**Метою статті** є визначення основних сучасних засобів Інтернет-комунікацій, а також поширених методів маніпулювання свідомістю, за допомогою яких здійснюється суттєвий вплив на особу, суспільство та державу.

**Виклад основного матеріалу.** Аналіз наукових робіт, що стосуються засобів Інтернет-технологій, за допомогою яких здійснюється суттєвий вплив, дав змогу виокремити такі найпоширеніші методи маніпулятивного впливу, як [7; 17; 21; 23; 32; 37; 41]:

- *метод ствердження.* Цей метод полягає у тому, що ЗМІ часто надають перевагу бездоказовим твердженням замість дискусії аргументів, обмежуючи тим самим плюралізм думок і презентуючи тільки одну, вигідну для них. Так символами безсоромної брехні російської пропаганди стали “розп’ятий хлопчик” і відстрілювання снігурів через те, що вони мають забарвлення російського прапора тощо;

- *метод повтору інформації.* Вважається, що через 30 хвилин аудиторія пам’ятає лише 60 відсотків змісту повідомлення. У кінці дня – лише 40, а за тиждень ледве 10 відсотків. В результаті будь-яка проблема зникає сама собою, якщо ЗМІ не будуть її повторювати, розвивати або нагадувати про неї. І навпаки – якщо абсурдне повідомлення повторювати з достатньою частотою, то врешті-решт воно таки закріпиться у масовій свідомості. В новинах подібні повтори – звична практика;

- *метод фокусу на емоції, а не на здоровий глузд.* Це класичний прийом, спрямований на те, щоб заблокувати здатність людини до раціонального аналізу, а зрештою – до критичного мислення взагалі;

- *метод відволікання уваги.* Одним із найбільш ефективних важелів управління суспільством є відволікання уваги від важливих проблем та рішень, які приймаються політичними та економічними елітами. Це досягається через насичення інформаційного простору менш важливими подіями;

- *метод “дезінформація”.* Сила його в тім, що дезінформація викидається зазвичай у момент прийняття якогось важливого рішення, тож коли з’ясується правда, мета дезінформування вже буде досягнута. Як правило, спростування дезінформації у більшості випадків залишається непоміченим і вже не впливає на сформовані за допомогою неправди соціально-психологічні установки;

- *метод “історичних аналогій”* вельми вигідний у багатьох аспектах. По-перше, пропагандист отримує змогу підлеститися до аудиторії, апелюючи до її ерудованості. Цей метод допомагає в конструюванні “історичних” метафор, а також “історичних міфів”, що використовуються в стратегічній перспективі, котрі програмують об’єкт впливу;

- *метод “міфів”.* Для укорінення соціальних міфів технологія маніпулювання передбачає використання багатого арсеналу конкретних методів впливу на свідомість людей. До них відноситься пряме підтасування фактів, замовчування небажаної інформації, поширення брехні і наклепу, а також більш тонкі, рафіновані засоби: напівправа (коли з метою забезпечити довіру аудиторії об’єктивно і докладно висвітлюються конкретні, малозначущі факти і одночасно замовчуються більш важливі або ж подається загально хибна інтерпретація подій);

- *метод закидання брудом.* Цей метод зараховується до числа найгрубіших пропагандистських прийомів, проте частіше від інших використовується в сучасній політично-інформаційній боротьбі. За рахунок підбору таких епітетів і лексики, що дають



предмету розмови жорстко негативну етичну оцінку, образ “клієнта” перетворюється на суцільне “втління зла” і в такому світлі визріває в масовій свідомості;

- *метод використання стереотипів.* Під стереотипом розуміють сприйняття людьми якогось соціального об’єкта у спрощеному схематизованому вигляді. З часом таке уявлення фіксується у свідомості людини і практично вже не піддається перевірці досвідом – заміна імен, або наклеювання ярликів (наприклад, “фашисти”, “червоно-коричневі”, “особи кавказької національності” або “жидобандерівці”);

- *метод створення проблем, а потім пропонування способів їх вирішення.* Створюється проблема, що викликає необхідну владним колам реакцію і дозволяє впровадити рішення, які в іншій ситуації викликали б протест серед населення. Наприклад – криваві теракти, як рушій для прийняття законів, що підсилюють “безпеку”, а по суті діють на обмеження прав звичайних громадян.

Необхідно зазначити, що наразі для визначення способів маніпулятивного впливу використовуються різні терміни – такі, як “прийом”, “метод”, “техніка”, “технологія”. У той же час, чітких критеріїв їх розподілу не вироблено, їм також властиві певні поєднання. Ми розглядаємо дану сукупність методів маніпулятивного впливу як теоретичну основу, за допомогою якої в майбутньому будуть отримані кількісні оцінки ризику інформаційно-психологічного впливу на особу, суспільство та державу.

Розглянемо деякі засоби Інтернет-комунікацій, які вдало використовуються для маніпулювання свідомістю людини.

### ***1. Електронна пошта.***

Існують численні Інтернет-мережі комунікаційного зв’язку, що працюють за різними міжнародними протоколами. Нині електронна пошта (e-mail) – зручний засіб швидкого й ефективного спілкування великої кількості адресатів. Тому поширення спеціально підібраної інформації (дезінформації) було однією з перших Інтернет-технологій маніпулювання свідомістю, що активно використовується ворогуючими сторонами під час політичних і воєнних конфліктів [23; 32].

Так під час конфлікту в Косово Югославською стороною широко застосовувалося розсилання електронних листів. Змушуючи сумніватися у правильності офіційної пропаганди, поштові скриньки більше 10 тис. користувачів різних агентств новин та урядових чиновників США регулярно заповнювалися посланням з описом результатів бомбардувань і ракетних ударів по цивільних об’єктах, числа жертв серед мирного населення, а також страждань мирних громадян.

Зі свого боку під час військової компанії в Іраку США за допомогою електронної пошти здійснили широкомасштабну операцію: арабською мовою іракським генералам розсилалися послання із закликом не виконувати накази С. Хусейна. В електронних листах також звучав заклик позначати місцезнаходження складів хімічної, біологічної та ядерної зброї, а також містилося звернення до громадян Іраку допомогти запобігти використанню зброї масового ураження.

Нарешті, ймовірний злом російськими спецслужбами електронної пошти Національного комітету демократичної партії – є найсвіжішим прикладом того як Путін застосовує сучасні інформаційні технології як засіб інформаційної війни. Показово, що зв’язки із Wikileaks Кремль розвиває впродовж багатьох років [1].

Одним з небезпечних видів сугестії є розсилка шахраями електронних листів від імені банків та створення підробленої сторінки сайту банку чи іншої установи з метою “витягнути” у користувача пари логін/пароль від його акаунта (фішинг). Це дає можливість зловмисникам, наприклад, перевести всі гроші з банківського рахунку

жертви на власні. Частіше за все, фішинг розрахований на неуважних користувачів, які не звертають уваги на незвичайні назви сайтів, частіше за все з помилками, незвичайний зовнішній вигляд знайомих ресурсів та нехтують основним правилами сучасної кібербезпеки (наприклад, оригінальна адреса відомого в Україні он-лайн-банку – privat24.ua. У той самий час фішингова сторінка може мати тільки одну неправильну літеру або схожу назву та бути витриманою у корпоративних кольорах компанії – priwat24.ua) [35].

Ще одним напрямком використання всесвітньої мережі, зокрема електронної пошти з метою інформаційного протиборства, маніпулювання свідомістю є виведення з ладу або зниження ефективності функціонування структурних елементів мережі. Серед найбільш часто вживаних таких способів є “бомбардування” електронної пошти великою кількістю електронних листів.

Механізмом реалізації даного способу вважається наступне: оскільки відправка великої кількості електронних посилок на одну адресу впродовж короткого періоду часу ускладнює або робить неможливим отримання звичайних листів із загального масиву. Це може призвести до порушення роботи обслуговуючих серверів. Так, під час різного роду конфліктів його сторони регулярно піддають “поштовому бомбардуванню” різні урядові організації.

## ***2. Мережеве теле- та радіомовлення.***

Реалізація методів управління свідомістю людини, особливо з використанням каналів розповсюдження аудіовізуальної інформації, призвела до появи поняття “медіа вірусу”. Особливістю інформаційних вірусів є здатність утворювати фільтри сприйняття, за допомогою яких відбувається відбір інформації, що створює у сприйнятті людиною суттєве викривлення реальності. Завдяки чому одним з найбільш цинічних розповсюджувачів інформаційних вірусів стала Інтернет-реклама.

Д. Рашкофф описав нове середовище перебування людини, котре ще можна завойовувати – медіа простір. Він розглядав медіа вірус як медіа події, що зумовлюють значні соціальні зміни [20].

Прикладом медіа вірусного зараження є використання медіа вірусів в українсько-російському газовому конфлікті. У новинах мережі істина не відшукувалася, а проголошувалася, її змінювали декларації та здогадки: “Українська сторона не проявляє ніякої ініціативи в підписанні контракту на поставку газу на 2009 рік”; “Балога боїться, що лаври перемоги в газовій війні дістануться Тимошенко, а не Ющенко”; “Газпром скаржитися, що Україна вимагає газ безкоштовно, тобто задарма”; “В Америці вирішили, що в газовому конфлікті винна сама Європа” тощо [37].

В Інтернеті разом із порівняно нешкідливими інформаційними вірусами (сленгові вирази тощо) існують вкрай руйнівні (віруси тоталітарних, молодіжних банд, фашистських ідеологій). Такі віруси можуть програмувати свідомість людини на завдання максимальної шкоди людям або самому собі (наприклад, самогубство). Вважається, що революції, війни та інші масові суспільні негаразди є епідеміями, викликаними інформаційними вірусами [36].

Людина, перебуваючи у віртуальному просторі, частково занурюється у стан ілюзорної реальності. Ілюзорна реальність є продуктом зміненої реальності. Вона збіднює особистість, допомагає лише ввести людину в потрібний стан зниженої критичності свідомості, тобто змушує приймати все за “чисту монету”. У крайньому випадку веде до її руйнування. Саме тому методи вербального впливу на її підсвідомість (нейролінгвістичне програмування – НЛП, гіпноз, контроль свідомості) насправді діють і приносять результати.

На веб-сторінках багатьох політичних партій можна спостерігати, що центральне і найважливіше місце займає гучний слоган партії, спрямований на виклик у людини потрібних емоцій [27]. Психолінгвістично грамотно складені слогани завжди в підтексті містять певний концепт, суттєвий для картини світу споживача інформації. Апеляція до цього концепту на підсвідомому рівні закликає до дій, запрограмованих сугесторами.

За твердженням деяких фахівців, Росія в інформаційній війні проти України використовує технології НЛП і різні форми гіпнозу. При цьому вплив на підсвідомість наших громадян здійснюється за допомогою екрану монітору комп'ютера, вводячи їх у стан підвищеної чутливості до зовнішньої сугестії. Однак особливих успіхів кремлівські пропагандисти досягли у зомбуванні власних громадян.

### ***3. Електронні видання.***

Електронне видання – електронний документ, що пройшов редакційно-видавниче опрацювання, має вихідні відомості та призначений для розповсюдження в незмінному вигляді [21].

В залежності від наявності друкованого еквівалента електронні видання розрізняють:

електронний аналог друкованого видання, що в основному відтворює відповідне друковане видання, зберігаючи розташування на сторінці тексту, ілюстрацій, посилань, приміток тощо;

самостійне електронне видання, що не має друкованих аналогів.

Нині Інтернет-видання перетворюються на масові дискусійні портали. Коментарі є своєрідною зброєю інформаційної війни, завданнями якої є відволікання уваги від гострих тем, знищення репутації опонентів через поширення наклепів, компромету, пліток, провокування до конфліктів, порушення душевної рівноваги об'єкту впливу, зниження інтересу користувачів до ресурсу, формування потрібної громадської думки [16].

Ця сфера інформаційного простору слугує не лише джерелом новин, а й емоційним тлом сприйняття поточних подій, оскільки Інтернет-коментарі зазвичай містять надзвичайно сильний почуттєвий компонент [39]. Читаючи їх, людина поринає в інформаційне поле фрагментарних, суперечливих і часто поверхових відомостей.

### ***4. Спеціалізовані мережеві сайти.***

Вперше сучасні інформаційні технології були використані НАТО для підтримки воєнних операцій. За безпосередньої підтримки американських фахівців з комп'ютерних технологій або з їх допомогою були розроблені спеціалізовані сайти. Вони здійснювали потужне інформаційне супроводження всіх дій альянсу. Впродовж лише перших двох тижнів операції в Косово американське інформаційне агентство CNN підготувало понад 30 статей, розміщених потім у всесвітній мережі [22; 33].

Згодом з'явилися нові риси у психологічних операціях Збройних Сил США – широкомасштабне адресне звернення до іракського воєнного керівництва. Вищим офіцерам навіювалася думка про те, що “іракці понесуть величезні втрати, якщо не приєднаються до боротьби проти Саддама або, принаймні, не відмовляться піднімати зброю проти вторгнення”.

Вище наведене свідчить: немає нічого дивного в тому, що між військовими кампаніями Росії в Україні та Сирії є багато спільного [35].

Путін за допомогою ЗМІ й Інтернет застосував хитрощі, обман і брехню, щоб прикрити операції та їхні цілі. Під час переговорів та конференцій із західними дипломатами його представники постійно погоджувалися на мирні плани, у той час як російські наземні сили продовжували артилерійські обстріли та бомбардування.

Для пропаганди своїх ідей, поширення дезінформації, збору коштів на свою підтримку і залучення нових найманців можливості Інтернету активно і цілеспрямовано використовують як сепаратисти, так і терористи різного роду. Для цього на серверах організаціями та приватними особами розміщується безліч сайтів, що містять статті, фото- та відеоматеріали, а також посилання на повідомлення найбільших світових інформаційних агентств, в яких критикуються дія урядів їх опонентів. Часто сайти дублюються різними мовами [10].

Останнім часом для залучення уваги до агресивної сторони, демонстрації своїх можливостей або намірів часто використовують заміну інформаційного змісту сайтів, здійснюючи підміну його сторінок або їх окремих елементів в результаті злому. Часто використовується реєстрація в пошукових системах сайтів протилежного змісту за однаковими ключовими словами, а також підміна посилань на іншу адресу зі спеціально підготовленим наперед текстом.

### **5. Боти.**

Тривалий час Україна перебуває в епіцентрі інформаційної війни, що на разі загострилася до краю. Її основна мета – маніпулювати свідомістю людей і створювати у суспільстві певні настрої. А Інтернет – найзручніший майданчик для того, щоб плодити усілякі чутки, плітки і фейки [3].

Дослідження компанії Incapsula свідчить, що 61,5 % трафіку всіх сайтів тепер генерують боти. Боти посилають чіткі інформаційні блоки в розрахунку на те, що від їх постійного повторювання ці блоки врешті засвоюються [6]. Наслідки цього не можна недооцінювати.

В соціальних мережах можна створювати ботів у великих кількостях, вони потенційно можуть використовуватися для впливу на громадську думку. Вони можуть створювати численні повідомлення, які змінюватимуть сприйняття певних подій людиною.

Майже за два роки війни українці звикли до російської безглуздої пропаганди на кшталт “розіп’ятих хлопчиків” та “вбитих снігурів” і навіть сміються з того. Але боти та тролі в мережі продовжують вигадувати нові й нові історії про Україну та українців.

Нині боти стають все більш досконалими. Вони краще маскуються і більш схожі на людей. Тому завдання їх розпізнавання стає дедалі важчим. Ми навіть не знаємо, яка точність систем у виявленні останніх і найбільш передових ботів [4; 28].

Штучне керування громадською думкою за допомогою цілого батальйону наполегливих ботів називається “астротурфінг” [14].

Наслідки астротурфінгу насправді настільки серйозні, що міністерство оборони США почало фінансувати дослідження програмного забезпечення, що могло би визначати фейкові акаунти в соцмережах.

### **6. Чат.**

Історично чат став першим методом масового спілкування в Інтернеті. Під чатом розуміють специфічну форму спілкування у Web’і, що називається IRC (Internet Relay Chat), чи просто chat (бесіда). За допомогою IRC (трансляція чатів в Інтернеті) можна вести розмову в Інтернеті в режимі реального часу.

Чат відносять до відкритих груп спілкування, де користувач можете спілкуватися в режимі реального часу, використовуючи псевдонім. Чат-групи або чат-кімнати часто називають відповідно до теми або вікової групи учасників. Спілкуванню в чаті характерні своя мова, етикет і культура [8].

Думки, висловлювані в чатах, здебільшого образні і невтішні. “Тінейджерські балачки”, “ескапістський наркотик”, “відчуття тихого божевілья” – ось далеко не найяскравіші визначення. І на перший погляд вони абсолютно справедливі. При першому відвідуванні чату людина спостерігає величезну мішанину різнобарвних реплік різного ступеня пристойності. Очевидно, що сугестія у чаті може легко використовуватися як спосіб відволікання уваги від актуальних проблем. Тобто, практикувати переважно спілкування заради самого спілкування.

Вважається, що люди в мережі поведуться далеко не так як у реальному житті – вони реалізують те, що не можуть реалізувати в реальному житті. Однак, необхідно додати, що при цьому обов’язково відображаються їх знання, набуті в реальному житті. Зазвичай говорять, що при віртуальному спілкуванні долаються численні соціальні бар’єри у вигляді віку, зовнішності, соціального статусу, манер тощо. Безосібність свого часу швидко створила умови для того, щоби чат став чудовою основою для тролінгу – одного із найяскравіших проявів психологічної маніпуляції в Інтернеті [25].

Тролінг – це написання в Інтернет-мережі (на форумах, у групах новин тощо) провокаційних повідомлень з метою викликати флейм, конфлікти між учасниками, беззмістовну розмову, образи тощо. Під флеймом (з англ. flame – вогонь, полум’я) слід розуміти обмін повідомленнями на форумах і в чатах у формі словесної війни, яка нерідко втрачає відношення до первинної причини дискусії [38].

Головною ціллю тролінгу є внесення в суспільство розладу, хаосу. Провокаційні, інколи гумористичного, іронічно-саркастичного характеру повідомлення троля направлені на залучення інших Інтернет-користувачів до безкорисної конфронтації. Чим більше реагує віртуальне суспільство, тим більша можливість тролінгу з боку ініціатора, оскільки увага інших стверджує його впевненість у тому, що його дії досягають поставленої мети – викликати хаос. Такий штучно створений хаос може трансформуватися в одну з двох стадій: стадія втрати контролю і стадія умілого прихованого використання хаосу його творцем з маніпулятивними цілями. При втраті контролю над хаосом може відбутися або його розпалювання, або затухання.

У зв’язку з вищенаведеним, не можуть не викликати занепокоєння плани менеджменту мережі Facebook, що планує запустити функцію секретних чатів, користувачі яких матимуть можливість встановити таймер електронного листування. Як стверджують розробники, такі чати створюються для зручності обговорення делікатних питань і будуть доступні тільки конкретним користувачам.

### **7. Он-лайн-форуми (веб-форуми).**

Он-лайн-форум – один з найпопулярніших видів спілкування в Інтернеті – це спеціальний веб-сайт для проведення дискусій, на якому користувачі обмінюються досвідом та ідеями з певної заданої теми, в тому числі обговоренню певних політичних подій тощо. Бувають форуми, де учасники спілкуються та діляться досвідом із певних вузькоспеціалізованих тем.

Робота форуму полягає у створенні користувачами тем у розділах і можливістю обговорення всередині цих тем. Найпоширеніший поділ веб-форуму: “розділи → теми → повідомлення”. Звичайно повідомлення несуть інформацію “автор – тема – зміст – дата/час”. Повідомлення та всі відповіді на нього утворюють гілку. Кожен учасник форуму (користувач) має свій унікальний пароль та логін, якими він користується для доступу на сторінку форуму. При цьому учасник за своїм бажанням може або

залишатися анонімним, або брати участь в обговореннях під своїм справжнім ім'ям та прізвищем.

Багато в чому завдяки великому обсягу інформації, що циркулює в Інтернеті, і, на перший погляд, уявній простоті, доступності подачі і розуміння інформаційних повідомлень, як і блоги, різноманітні форуми в більшості мають такі ж самі властивості, що роблять їх чудовим майданчиком сугестивного впливу.

Так, на анонімних Інтернет-форумах продавці синтетичних наркотиків, відомих у народі як “солі” і “мікси”, оголошують про відкриття “філій” у великих містах України. Серед міст, де створюють цілі центри з розповсюдження наркотичних засобів, – Харків, Одеса, Запоріжжя, Дніпро, Черкаси, Львів і Житомир. Організатори наркомережі викладають прайси і оголошують набори “мінерів” – тих, хто розкладатиме пакетики з наркотиками по під’їздах тощо.

### **8. Іміджборд.**

Іміджборд – це різновид форуму з обов’язковою (часто відсутньою) реєстрацією, або навіть ідентифікацією особи, та певними особливостями модерації. Він має розділово-тредовий спосіб організацію спілкування.

Оскільки іміджборди є підвидом форумів, то і мережева культура, що формується на їх базі, містить ті ж самі загальні категорії, що й форумна. Розділово-тредова система спілкування формує явища протидії та використання механізму оновлення тредів, причому кількість тредів зазвичай обмежена. У зв’язку з особливостями розмітки, утворюються особливі засоби вираження текстом як то наприклад поетапна конкретизація. Важливу роль у цьому відіграє простота оформлення [24].

Головна причина популярності іміджбордів – безосібне дописування без реєстрації і з мінімальною модерацією. Так, дана концепція надає лише можливості. Але користувачі, використовуючи дані можливості, перетворюють те про що ви прочитали у попередніх розділах, на домівку феєрії та драми.

За рахунок вищенаведених обставин, культура іміджбордів, є надзвичайно насиченою особливостями, що відрізняють її від усіх відомих досі Інтернет-культур. Значна частина цих особливостей полягає у відкиданні будь-яких моральних принципів (незалежно від того, де мешкає член спільноти) та використанні нових засобів соціальної динаміки [10].

До визначення власне іміджбордів увіходить також поняття про орієнтованість на обмін зображеннями. Використання банерів, яскравої навігації, а також динамічної картини відволікає користувачів, поступово переманюючи їхню увагу, що стало нині одним з дієвих видів маніпулювання в Інтернеті.

### **9. Блоги.**

Блог (англ. blog) – це мережевий журнал чи щоденник подій, веб-сайт, головний зміст якого – інформація, що регулярно додається. Це авторський твір, де автор (блогер) висловлює власне ставлення і суб’єктивні думки з приводу певної події. Сукупність усіх блогів в Інтернеті створює блогосферу [30].

Популярність блогосфери зумовлена можливістю використання таких недоступних раніше інструментів як RSS, trackback тощо. Для блогів характерні короткі записи тимчасової значущості. Записи демонструються у зворотньо-хронологічному порядку. Тобто, спочатку ви отримуєте найновіші повідомлення. Крім того він діалогічний за своєю природою і передбачає зворотний зв’язок між аудиторією та автором.

Переважає більшість блогів (99 %) – це веб-сайти, в яких основна значуща частина – текст [9]. Проте блог може існувати у вигляді зображень, звуків або відео без жодного писаного слова, а е-пошта чи RSS (технологія отримання поновлень на своїх улюблених веб-сторінках) дозволяють обійтися без сайту. Теоретично у жанрі блога можна творити навіть в он-лайн: розміщувати повідомлення на дошках оголошень, залишаючи місце для коментарів, або вести стилізовану рубрику в журналі.

У контексті наших досліджень особливий інтерес становлять тематичні блоги. Саме блоги і мікроблоги за рахунок “живого спілкування”, за підтримки функції зворотного зв’язку можуть створювати якісно нове міжособистісне спілкування. Воно дозволяє вільно спілкуватися з будь-якою людиною незалежно від її територіального розташування, національної приналежності, ідеологічних переконань, віросповідання, включаючи людину в глобальний інформаційний простір.

Ключовою схемою для здійснення сугестивного впливу в блогах є: увага – довіра – репутація – вплив [20]. Щоб блог привернув увагу маніпуляторів, він повинен бути популярним у мережевому співтоваристві, викликати довіру, що забезпечує його репутацію в Інтернеті. Тільки в такому разі сугестивний вплив буде продуктивним.

Впродовж останніх років блоги отримали шалену популярність. Це сталося завдяки веб-сервісам, що дозволяють будь-кому без технічних навичок вести власний блог. Мільйони людей почали писати блоги – їхня кількість подвоюється кожні півроку [26].

Маніпулятивний потенціал блогів, що заснований на їхній принциповій настанові на довіру, відкритість і комунікацію, високо оцінили політики, військові, економісти, громадські активісти тощо.

### **10. Смартмоб.**

Смартмоб (англ. smart mob – розумний натовп) – форма соціальної організації, яка самоконструюється завдяки засобам ефективного використання високих технологій.

Це визначення було запропоноване Г. Рейнгольдом, який вважав, що “розумні натовпи” – це результат поширення і розвитку комунікаційних технологій. Смартмоби організовуються за допомогою Інтернету і мобільних телефонів та PDA. Вони можуть проводитися одночасно в декількох місцях для залучення уваги преси та суспільства [9].

У ЗМІ термін “флешмоб” замінив термін “смартмоб”. Флешмоб з англ. flash mob перекладається як “миттєвий натовп” – це наперед спланована масова акція, в якій велика група людей збирається в людному місці, виконує наперед обумовлені дії (сценарій) а потім розходиться. Збір учасників флешмобу здійснюється засобами зв’язку, загалом через Інтернет і участь в ньому є добровільною.

Формування політичних поглядів та переконань серед молоді можливе і за допомогою політ-мобів (соціо-мобів). Це – проведення акцій із соціальним або політичним відтінком. Вони є простим, оперативним і безпечнішим засобом вираження суспільної думки або привертання уваги до певних проблем, ніж мітинги чи демонстрації.

Прикладом політ-мобу можуть бути акції протесту в Білорусії, коли люди демонстративно зав’язали очі та відвернулися від встановленого на площі екрана, по якому трансливався виступ прокурора Білорусі. Щороку мобери проводять всесвітні фестивалі флешмобу: у серпні 2009 – у Харкові, 2010 – у Мінську, 2011 – в Одесі.

Ще одним варіантом флешмобу є флешмоб-туризм. Мобери можуть приїздити в будь-яке місто та брати участь у заходах. Як приклад можемо назвати сайт “Подорожник”, коли можна домовитися з незнайомими людьми стосовно доїзду на автомобілі за півціни або безкоштовно.

Якщо проаналізувати психологічні основи мотивації учасників флешмобів, то вони є різними: розвага, бажання відчувати себе вільними від суспільних стереотипів поведінки, вплинути на оточуючих, самоствердитися, спроба пережити гострі відчуття, відчуття причетності до спільної справи, отримати ефект як від групової психотерапії, емоційна розрядка, пошук нових друзів. Загалом мета досягається коштом “ефекту натовпу”.

### ***11. Комп’ютерні ігри.***

На разі комп’ютерні ігри – не лише галузь комп’ютерної індустрії, що стрімко розвивається та приносить мільйонні прибутки, але й потужний пропагандистський інструмент.

Важлива відмінність від інших інформаційних продуктів полягає в тому, що у випадку комп’ютерних ігор споживач (гравець) не обмежується пасивним споживанням інформації: внаслідок самої природи цього явища запускається психологічний механізм співучасті. Неминуче ототожнення глядача з героєм фільму/книги в комп’ютерній грі набуває активного характеру. Комп’ютерні ігри роблять людину – свого роду учасником жорстоких дій, що можуть тривати нескінченно довго.

Якщо стосовно дітей така ситуація є природною, то стосовно дорослої людини надмірне захоплення грою, перетворення гри на мету існування виглядає якщо не патологією, то явною інфантильністю. Ця інфантильність може бути частиною індивідуальності, а може і являти собою наслідки певного впливу соціуму на особу: штучна інфантилізація, тобто редукція свідомості дорослих людей до рівня підлітка з його максималізмом, чорно-білою картиною світу, підвищеною емоційністю може бути різновидом політичної маніпуляції масами [37].

Ігри-бойовики (головне завдання – знищити ворогів) можуть ґрунтуватися на різних сюжетах, як фантастичних (дія розгортається у вигаданій реальності), так і пов’язаних з реальними подіями, політичними, соціальними, географічними реаліями. Прикладом останніх можуть слугувати політичні комп’ютерні ігри і військові комп’ютерні ігри, що виступають як засіб формування стереотипів.

Політичною комп’ютерною грою ми можемо назвати ту гру, сюжет якої заснований на використанні реальних образів і подій політичного простору. Прикладом такої гри може бути комп’ютерна гра “Утеча Жакіянова”. Сюжет гри оснований на реальних подіях березня 2002 року, коли співголова політичного руху “Демократичний вибір Казахстану” Жакіянов був змушений переховуватися від переслідування місцевих спецслужб і поліції [42].

Сюжет військової комп’ютерної гри може бути заснований як на реальних війнах і бойових діях, так і на гіпотетичних військових, на умовних чи фантастичних конфліктах. За часовими параметрами політичні і військові комп’ютерні гри можна поділити на:

- 1) засновані на історичному матеріалі (наприклад, ігри, що пропонують змінити хід Другої світової війни, чи гра, що вийшла до 41-ї річниці вбивства президента Джона Ф. Кеннеді в США;
- 2) що використовують сучасні події;
- 3) футурологічні – події відбуваються в майбутньому.

Варто зазначити, що сюжети політичних і військових стратегічних ігор часто перетинаються: наприклад, результатом розвитку політичної кризи у грі (як і в реальному житті) часто є військовий конфлікт та етнічне насильство. Так гравець сірійської комп’ютерної гри “Під ясенем” може відчувати себе учасником інтифади:



палестинським юнаком, що бореться проти ізраїльських вояків. Гра користується величезною популярністю в арабському світі і вже викликала критику Ізраїлю.

Політизовані комп'ютерні ігри стають частиною й українського політичного простору. У свій час у російських, українських і білоруських Інтернет-магазинах з'явилася комп'ютерна гра “Операція “Галичина”, створена компанією “NeoGame”. Творці гри пропонують гравцеві перетілитися у командира загону російського спецназу, що допомагає підкорити центральну частину Західної України, що збунтувалася після перемоги проросійського президента. Представники українського політикуму й експерти виявилися одностайними в оцінці гри: її сюжет не є випадковим, за ним стоять певні політичні сили, а цілі виходять за межі простої розважальності.

В останнє десятиліття комп'ютерні ігри перетворилися на частину не лише культурного, але й інформаційного простору. За рахунок широкого охоплення аудиторії, вони активно формують певні стереотипи у свідомості людини. Насамперед це стосується дитячої та підліткової аудиторій, наслідком чого є проникнення у глибші шари психіки, засвоєння стереотипів у ранньому віці (а також охоплення тих сегментів, що не цікавляться політикою). Про це свідчать постійно повторювані спроби різних держав узяти під контроль ринок комп'ютерних ігор.

### ***12. Електронна психотропна зброя.***

Дія психотропної (психофізичної) зброї заснована передусім на використанні дистанційного впливу на людину з метою корекції її поведінки та фізіологічних функцій. Процес змінювання свідомості полягає в програмуванні поведінки людини на підсвідомому рівні [7; 29].

Засоби для змінювання свідомості особистості є різновидом психотропної зброї [31; 41]. Одним з них є “комп'ютерні віруси” – спеціальні програми, що здатні до самопоширення без відома користувача та всупереч його бажанню. Вони заражають програмне забезпечення у спосіб уведення свого об'єктного коду до коду зараженої програми. Вже винайдений вірус (“вірус ббб”) , що згубно впливає на психофізичний стан користувача комп'ютером.

### ***13. Соціальні мережі.***

Сервіси, створені для швидкого міжособистісного спілкування, нині дедалі більше стають небезпечним інструментом маніпуляції масовою свідомістю. Соціальні мережі Фейсбук, ВКонтакте, Однокласники тощо об'єднують в неформальне спілкування мільйони людей, дають можливість створювати спільноти, визначити оформлення особистих сторінок, вести переписку, як особисту, так і публічну.

Популяризація соціальних мереж в Інтернеті доповнює їх політичну та інші види активності. За допомогою даних мереж можливе застосування різноманітних технологій маніпулювання свідомістю: пропаганди, реклами, піару, перекручування інформації, дезінформації й її замовчування тощо [11; 15].

Так, найбільш легкий за формою спілкування канал комунікації – Твітер створює користувачеві труднощі: подача інформації дрібними порціями не дозволяє користувачеві ефективно її використовувати й осмислювати. Як наслідок, вирвані з потоку різноспрямованої інформації повідомлення втрачають свою актуальність і значимість. Іншим маніпулятивними прийомами є одночасна подача суперечливої інформації, викидання лише частини інформації, що змушує індивіда думати в потрібному для себе руслі, агресивний дискурс подачі інформації. Як наслідок наведених вище явищ, у людини спрацьовує психологічний бар'єр: поверхневий

аналіз інформації, відсутність мотивації, протестність і зниження рівня підтримки влади [19; 34].

Очевидно, що нині соціальні мережі стали складним інструментом маніпулювання [2; 13; 33]. Цей інструмент за допомогою використання новітніх технік передачі інформації дозволяє впливати на настрої окремих груп суспільства, активізувати ті чи інші події.

Вони стали майданчиком для різних опитувань та оцінок рейтингів. Маніпуляція використовується як у формуванні питань, підташовці дат опитування, так і в поширенні результатів. Тому не дивно, що нині соціальні мережі витіснили за популярністю персональні сайти, форуми та чати.

Усі ці засоби Інтернет-комунікацій стали важливим інструментом масової маніпуляції свідомістю [12; 33].

### **Висновки.**

Здійснений аналіз найпоширеніших методів маніпулювання свідомістю особи, суспільства та держави дав змогу підтвердити, що в умовах формування глобального інформаційного простору і розвитку інформаційного суспільства усі сфери життєдіяльності особи, суспільства, держави та міжнародної спільноти безпосередньо пов'язані з засобами маніпулювання свідомістю за допомогою сучасних Інтернет-комунікацій. За рахунок широкого охоплення аудиторії засоби Інтернет-комунікацій продовжують активно використовуватися для застосування методів маніпулятивного впливу, формування певних стереотипів у свідомості людини. Тому виявлення медіа-вірусів, методів вербального та сутєстивного впливу на підсвідомість людини, грубих пропагандистських прийомів потребують перегляду базових причин війн і революцій, тероризму, фанатизму та одержимості, а також ролі релігій, ідеологій, преси, радіо та телебачення.

### **Використана література**

1. Апанасик В. WikiLeaks. Избранные материалы / В. Апанасик. – М. : Альпина нон фикшн, 2011. – 280 с.
2. Ассанж Дж. Шифропанки. Свобода и будущее Интернета / Дж. Ассанж. – М. : Азбука Бизнес, 2014. – 240 с.
3. Баранюк К. Приємний співрозмовник чи інтернет-бот? – Режим доступу : [http://www.bbc.com/ukrainian/vert\\_fut/2015/08/150818\\_vert\\_fut\\_how\\_online\\_bots\\_are\\_tricking\\_you\\_vp](http://www.bbc.com/ukrainian/vert_fut/2015/08/150818_vert_fut_how_online_bots_are_tricking_you_vp)
4. Баррат Дж. Последнее изобретение человечества. Искусственный интеллект и конец эры Homo sapiens / Дж. Баррат. – М. : Альпина нон фикшн, 2015. – 304 с.
5. Барроуз М. Будущее : расшифровано. Каким будет мир в 2030 году / М. Барроуз. – М. : Манн, Иванов и Фарбер, 2015. – 352 с.
6. Батогов А. Более половины мирового Интернет-трафика генерируют боты. – Режим доступу : <http://hi-news.ru/research-development/bolee-poloviny-mirovogo-internet-trafika-generiruyut-boty.html>
7. Вайншенк С. Законы влияния. Как побудить людей делать то, что вам нужно / С. Вайншенк. – М. : Изд-во : Манн, Иванов и Фербер, 2014. – 272 с.
8. Вострецова В.О. Спілкування в чатах як один із видів електронного спілкування. – Режим доступу : [http://www.rusnauka.com/PNR\\_2006/Philologia/7\\_vostrecova.doc.htm](http://www.rusnauka.com/PNR_2006/Philologia/7_vostrecova.doc.htm)
9. Гавришак Л. Новітні інформаційні технології як засіб розвінчування сучасної подвійної суспільної моралі. – Режим доступу : [http://ddpu.drohobych.net/filos\\_gum/wp-content/uploads/2016/04/2013\\_7.pdf](http://ddpu.drohobych.net/filos_gum/wp-content/uploads/2016/04/2013_7.pdf)
10. Галицький І.В. Екстремізм в соціальних мережах : організаційно-правові заходи протидії / Альманах міжнародного права. – 2014. – Вип. 4. – С. 74-83.

11. Гвоздик О. Соціальні мережі – вільний обмін думками чи маніпулювання свідомістю? – Режим доступу : <http://xpress.sumy.ua/article/society/5700>
12. Грачев Г. Манипулирование личностью : организация, способы и технологии информационно-психологического воздействия / Г. Грачев, И. Мельник. – М. : Алгоритм, 2002. – 228 с.
13. Грингард С. История вещей. Будущее уже здесь / С. Грингард. – М. : Альпина Паблишер, 2016. – 188 с.
14. Данько Ю.А. Астротурфінг як інструмент віртуальної маніпуляції та політичної пропаганди в умовах інформаційної доби // Сучасне суспільство : політичні науки, соціологічні науки, культурологічні науки. – 2015. – Вип. 2 (1). – С. 38-49.
15. Довгань О.Д. Соціальні мережі як чинник впливу на інформаційну безпеку // Правова інформатика. – № 2(46)/2015. – С. 25-31.
16. Журавльов А. Інтернет-спільноти у новій хвилі інформаційних війн. – Режим доступу : <http://www.vidkryti-ochi.org.ua/2009/01/blog-post.html>
17. Кара-Мурза С.Г. Манипуляция сознанием / С.Г. Кара-Мурза. – М. : Изд-во: Эксмо, 2005. – 832 с.
18. Карр М. Великий переход. Революция облачных технологий / М. Карр. – М. : Манн, Иванов и Фарбер, 2013. – 272 с.
19. Ким Э. Ничего личного. Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные для собственной выгоды / Э. Ким. – М. : Альпина Паблишер, 2016. – 224 с.
20. Компанцева Л. Ф. Принципи сугестивної лінгвістики в інтернетній комунікації // Філологічні науки. – 2013. – Кн. 3. – С. 13-20.
21. Левин Р.В. Механизмы манипуляции : защита от чужого влияния / Р.В. Левин. – М. : Изд-во : Диалектика-Вильямс, 2016. – 432 с.
22. Лисичкин В.А. Третья мировая (информационно-психологическая) война / В.А. Лисичкин, Л. А. Шелепин. – М. : Инс-т социально-психологических исследований АСН, 2000. – 304 с.
23. Литвиненко О.В. Впливи та операції. Теоретико-аналітичні нариси / О.В. Литвиненко. – К. : НІСД, 2003. – 240 с.
24. Матвеев А. Технологии манипулирования в сети Интернет. – Режим доступу : <http://www.enabling.ru/php/content.php?id=2488>
25. Могилко С. В. Тролінг як спосіб психологічної маніпуляції в інтернеті. – Режим доступу : <http://s-journal.cdu.edu.ua/base/2008/v4/v4pp57-60.pdf>
26. Морозов Е. Интернет как иллюзия. Обратная сторона сети / Е. Морозов. – М. : Изд-во: АСТ, 2014. – 528 с.
27. Нагорний А.І. Сучасні методики маніпулювання суспільномасовою свідомістю та їх застосування в політичних технологіях. – Режим доступу : <http://www.ukr-socium.org.ua/Arhiv/Stati/4.2008/Pages%20from%20167-174.pdf>
28. Паливода Н. Інтернет-трилер “Бот”, або не вірте коментарям. – Режим доступу : [http://mymedia.org.ua/articles/infowars/nternet-triler\\_bot\\_abo\\_ne\\_v\\_rte\\_komentaryam.html](http://mymedia.org.ua/articles/infowars/nternet-triler_bot_abo_ne_v_rte_komentaryam.html)
29. Перцефф Д. Гиперболоид смерти. Психотронное оружие в действии / Д. Перцефф. – СПб. : Изд-во “Вектор”, 2008. – 184 с.
30. Попов А. Блоги. Новая сфера влияния / А. Попов. – М. : Изд-во: Манн, Иванов и Фарбер, 2008. – 336 с.
31. Почепцов Г.Г. Психологические войны / Г.Г. Почепцов. – М. : “Рефл-бук”, – К. : “Ваклер” – 2002. – 528 с.
32. Прибутко П.С. Інформаційні впливи : роль у суспільстві та сучасних воєнних конфліктах / П.С. Прибутко, І.Б. Лук’янець. – К. : ПАЛИВОДА, 2007. – 252 с.
33. Присяжнюк М.М. Сучасні інформаційні технології у сфері безпеки та оборони. – Режим доступу : [http://kobzar1814.blogspot.com/2011/04/blog-post\\_29.html](http://kobzar1814.blogspot.com/2011/04/blog-post_29.html)

34. Прокофьев В.Ф. Опасно! Объект атаки – психика и сознание человека. – Режим доступу : <http://mystic-news.com/articles/82-opasno-obekt-ataki-psihika-i-soznanie-cheloveka.html>
35. Социальная инженерия или манипуляции сознанием. – Режим доступу : <http://zillya.ua/ru/sotsialnaya-inzheneriya-ili-manipulyatsii-soznaniem>
36. Стасула Н. Електронні засоби виявлення вербальної маніпуляції в ЗМІ. – Режим доступу : <http://ena.lp.edu.ua:8080/bitstream/ntb/10663/1/13.pdf>
37. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева, Є.Д. Скулиш, О.Д. Бойко, В.В. Остроухов] ; за заг. ред. Є.Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2010. – 248 с.
38. Филлипс У. Тролло. Нельзя просто так взять и выпустить книгу про троллинг / У. Филлипс. – М. : Альпина Паблишер, 2015. – 300 с.
39. Фіялка С. Інтернет-коментарі в системі масової комунікації / Вісник Книжкової палати. – 2015. – № 9. – С. 47-48.
40. Форд М. Технологии, которые изменят мир / М. Форд. – М. : Манн, Иванов и Фарбер, 2014. – 277 с.
41. Чалдини Р. Психология влияния / Р. Чалдини. – СПб. : Питер, 2002. – 288 с.
42. Шерман О. Комп'ютерні ігри як засіб впровадження політичних стереотипів. – Режим доступу : [http://vlp.com.ua./files/31\\_34.pdf](http://vlp.com.ua./files/31_34.pdf)
43. е-боротьба в інформаційних війнах та інформаційне право : монографія / Брижко В.М. [та ін.] ; за ред. члена-кореспондента АПрН України, доктора економічних наук, професора М. Швеця. – К. : НДЦПІ АПрН України, 2007 р. – 239 с.

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

УДК 343.2

СЕМЕНЮК О.Г., кандидат юридичних наук,
заступник начальника Управління Служби безпеки України

ДЕРЖАВНА ТАЄМНИЦЯ ЯК ПРЕДМЕТ ЗЛОЧИНУ

Анотація. У статті проведено аналіз наукових поглядів щодо поняття предмета злочину, на підставі чого запропоновано власне визначення цієї дефініції; визначено характерні ознаки державної таємниці як предмета злочину; аргументовано позицію щодо необхідності декриміналізації ст. 422 КК України у зв'язку з відсутністю предмета цього злочину.

Ключові слова: предмет злочину у сфері охорони державної таємниці, судова експертиза, державний експерт з питань таємниць, компетентність державного експерта, військова таємниця.

Аннотация. В статье проведен анализ научных взглядов на понятие предмета преступления, на основании чего предложено собственное определение этой дефиниции; определены характерные признаки государственной тайны как предмета преступления; аргументирована позиция необходимости декриминализации ст. 422 УК Украины в связи с отсутствием предмета этого преступления.

Ключевые слова: предмет преступления в сфере охраны государственной тайны, судебная экспертиза, государственный эксперт по вопросам тайны, компетентность государственного эксперта, военная тайна.

Summary. The article analyzes the concept of scientific views on the subject of crime, whereby author proposes own definition of this concept; characteristic features of state secrets as a subject of crime are determined; position on the need for decriminalization of Art 422 of Criminal Code of Ukraine in the absence of the object of the crime is substantiated.

Keywords: subject of crime in the area of state secrets, forensics, state expert on secrets, competence of state expert, military secret.

Постановка проблеми. Проблема предмета злочину у кримінальному праві є однією з найбільш суперечливих і маловивчених. Спеціального дослідження предмета злочину до останнього часу не проводилося. Деякі положення про предмет злочину розглядалися, головним чином, у зв'язку з відмежуванням його від об'єкта злочину.

Між тим, значення предмета злочину як самостійної ознаки складу злочину та його роль у механізмі заподіяння шкоди охоронюваним кримінально-правовими засобами сферам життєдіяльності людей, у виявленні об'єкта злочину та кваліфікації діяння має важливе самостійне теоретичне і практичне значення.

Істотною властивістю державної таємниці, як предмета злочину, є обов'язкова наявність її специфічних ознак, без встановлення яких не може бути вирішено питання про притягнення особи до кримінальної відповідальності за вчинення злочинів у сфері охорони державної таємниці, кваліфікацію цих діянь та призначення покарання.

Аналіз публікацій. Дослідженням предмета злочину займалися М. Бікмурзін, А. Герцензон, А. Кістяківський, М. Коржанський, А. Круглевський, Є. Лащук, О. Мазуренко, А. Музика, Б. Нікіфоров, А. Піонтковський, О. Радутний, Н. Розенфельд, Н. Таганцев, В. Тацій, В. Філімонов, Є. Фесенко та інші науковці. Проте питання щодо предмета злочину у сфері охорони державної таємниці залишилися за межами їх наукових робіт.

Метою статті є аналіз наукових поглядів щодо поняття предмета злочину та пошук власного визначення цієї дефініції; визначення характерних ознак державної таємниці як предмета злочину.

Виклад основного матеріалу. Упродовж багатьох років у наукових колах не вщухають дискусії щодо предмета злочину, його місця у складі суспільно небезпечного діяння.

У дореволюційний період учені вважали, що предмет злочину належить до об'єкта злочину, а в деяких випадках прирівнюється до останнього [1, с. 182; 2, с. 141; 3, с. 7]. Зокрема А. Кістяківський зазначав, що “об'єктом злочину називається предмет, на який спрямовано або щодо якого вчинено злочин” [4, с. 280]. Б. Нікіфоров стверджував, що предмет є складовою об'єкта посягання, тому пропонував не виділяти його як окрему ознаку і взагалі зняти проблему самостійного дослідження предмета злочину [5, с. 130, 132].

Водночас на необхідності розмежування понять об'єкта та предмета злочину ще на початку ХХ століття наголошував А. Круглевський, пояснюючи це співпадіння ототожненням таких різних понять, як об'єкт захисту та об'єкт дії злочину [6, с. 13-14]. У кримінально-правовій літературі останніх років висловлено обґрунтовану думку про те, що наведене співвідношення “об'єкта захисту” й “об'єкта дії” інтерпретується саме як співвідношення об'єкта і предмета злочину в їхньому сучасному розумінні [7, с. 13]. Взаємозв'язок об'єкта і предмета посягання, на думку А. Музики та Є. Лашука, полягає у встановленні їх співвідношення на рівні предмета суспільних відносин, що охороняються кримінальним законом [8, с. 106].

Деякі науковці відносять предмет злочину до ознак об'єктивної сторони складу злочину [9, с. 76; 10, с. 160], а В. Філімонов вважає, що предмет злочину є складовою об'єкта злочину та водночас – його об'єктивної сторони [11, с. 35]. Проте, як справедливо стверджує В. Тацій, об'єктивна сторона як елемент складу злочину має власну структуру, свої, властиві їй системоутворювальні ознаки. Тому включення до її складу додаткових ознак навряд чи виправдано. У зв'язку з цим, немає потреби змінювати це уявлення про місце предмета у складі злочину, тим більше, що предмет злочину здебільшого пов'язаний безпосередньо з об'єктом злочину [12, с. 56].

У сучасній кримінально-правовій доктрині найпоширенішою є точка зору, яку ми повністю поділяємо, що предмет злочину належить до факультативних ознак складу суспільно небезпечного діяння [13, с. 100; 14, с. 310; 14, с. 104]. Зокрема, розглядаючи питання про місце предмета в конкретному складі злочину, В. Тацій зазначає: “Вважається, що предмет злочину не може претендувати на роль самостійної ознаки складу злочину. Таке рішення викликано тим, що склад злочину являє собою сукупність його обов'язкових елементів (об'єкта, об'єктивної сторони, суб'єктивної сторони і суб'єкта злочину). Відсутність хоча б одного з цих елементів виключає склад злочину і, отже, кримінальну відповідальність. Предмет же злочину, як уже зазначалося, є не обов'язковим, а факультативним стосовно загального поняття складу злочину” [15, с. 96].

Предмет злочину в науковій літературі визначається по-різному. Так, на думку В. Тація “предметом злочину слід вважати будь-які речі матеріального світу, з певними властивостями яких закон про кримінальну відповідальність пов'язує наявність у діяннях особи конкретного складу злочину... Оскільки предметом злочину може виступати лише певна річ, то предмет є завжди речовою (матеріальною) ознакою” [16, с. 93].

Таку ж позицію щодо матеріальності предмета злочину займає Є. Фесенко. Він зазначає, що “предметом злочину є речі матеріального світу, діючи на які, особа посягає на блага, що належать суб'єктам суспільних відносин” [17, с. 131], а також “матеріалізовані утворення, безпосередньо діючи (впливаючи) на які шляхом їх вилучення, створення, знищення, зміни їх вигляду або правового режиму тощо винна особа посягає на охоронювані законом цінності” [18, с. 77]. Але ці визначення не

охоплюють усі можливі форми існування державної таємниці, яка, крім текстового або графічного відображення на матеріальному носії інформації (документі), може циркулювати на вербальному рівні, тобто шляхом речового обміну секретною інформацією, а також існувати у вигляді фізичного поля, в якому відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

З огляду на ці властивості державної таємниці більш точно розкриває зміст поняття предмету злочину О. Радутний, який, досліджуючи проблемні питання кримінальної відповідальності за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю, дійшов висновку, що предметом злочину слід визнавати “речі або інші явища об’єктивного світу (інформація, енергія тощо), з певними властивостями яких кримінальний закон пов’язує наявність у діянні особи складу конкретного злочину” [19, с. 10].

Відхід від класичного підходу матеріальності предмета злочину та розуміння необхідності його більш широкого сприйняття, дозволив Н. Розельфельд розширити це поняття та доповнити його такою ознакою, як “віртуальність”. Зокрема, за її визначенням предмет злочину визначався як “речі або інші явища об’єктивного світу, як матеріальні, так і віртуальні, із певним впливом на які кримінальний закон пов’язує наявність у діянні особи складу конкретного злочину” [20, с. 59-60]. У подальшому Н. Розельфельд у співавторстві з О. Мазуренко дещо переглянула зміст зазначеного поняття, внаслідок чого віртуальний предмет злочину був ними визначений як такий, що не має зовнішнього представлення, але може набути такого за допомогою спеціальних методів і засобів [21, с. 82].

До таких віртуальних предметів злочину, крім інформації, Н. Савінова (Н. Розельфельд) також пропонує відносити інформаційно-комунікаційні технології та свідомість, оскільки останні “випадають” із кола кримінально-правової охорони, навіть за наявності кримінально-правового забезпечення цих інституцій на нормативному рівні. Визнання наявності й розвитку в державі інформаційного суспільства саме по собі вимагає визнання основних ресурсів такого суспільства предметами, а відсутність у них матеріальної ознаки потребує визнання їх предметами віртуальними [22, с. 231].

На підставі викладеного предмет злочину можна визначити як *матеріальні та віртуальні предмети об’єктивного світу (які людина може сприймати органами чуття чи фіксувати спеціальними технічними засобами), діючи на які, суб’єкт посягає на об’єкт злочину та з певними властивостями яких закон про кримінальну відповідальність пов’язує наявність у діяннях особи конкретного складу злочину*.

Предметом досліджуваних нами злочинів являються відомості, що становлять державну таємницю, а також їхні матеріальні носії, тобто матеріальні об’єкти, у тому числі фізичні поля, в яких секретна інформація відображена у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо. Таким чином, предметом злочинів у сфері охорони державної таємниці може бути як усна інформація, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України, так і її матеріальні носії. Для втрати документів, що містять державну таємницю (ст. 329 КК України) та втрати документів або матеріалів, що містять відомості військового характеру, які становлять державну таємницю (ч. 2 ст. 422 КК України) – лише матеріальні носії секретної інформації.

Відповідно до ст. 10 Закону України “Про державну таємницю” (далі – Закон) віднесення інформації до державної таємниці здійснюється шляхом опублікування

мотивованих рішень державних експертів з питань таємниць у Зводі відомостей, що становлять державну таємницю (далі – ЗВДТ). Крім цього, згідно зі ст. 12 Закону, на підставі та в межах ЗВДТ з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов’язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов’язаних із державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю (стаття 12 Закону) [23].

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі ЗВДТ чи розгорнутих переліків відомостей, що становлять державну таємницю, відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації. Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка в ньому міститься, згідно із ЗВДТ – “особливої важливості”, “цілком таємно”, “таємно”. Реквізити кожного матеріального носія секретної інформації складаються із грифа секретності, номера примірника, статті ЗВДТ, на підставі якої здійснюється засекречування, найменування посади та підпису особи, яка надала гриф секретності. Якщо зазначені реквізити неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони повинні бути зазначені у супровідних документах (стаття 15 Закону) [23]. Матеріальний носій інформації, відповідно до пункту 154 Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та визнання такими, затвердженого постановою Кабінету Міністрів України від 18.12.13 р. № 939 (далі – Порядок), вважається засекреченим із моменту його створення та надання відповідного грифа секретності до прийняття уповноваженою особою рішення про його розсекречування [24].

Формулюючи ознаки складу злочину, законодавець створює модель злочину певного виду. При кваліфікації злочину виявляються найсуттєвіші риси конкретного суспільно небезпечного діяння шляхом співставлення його з інформаційною моделлю, закріпленою у диспозиції статті особливої частини КК України. Наявність чи відсутність у діяннях особи конкретного складу злочину з’ясовується на підставі дослідження і встановлення визначених законодавцем властивостей предмета злочину [17, с. 132].

Такими властивостями державної таємниці, як предмета злочину, є потенційна можливість завдання шкоди національній безпеці України у разі її несанкціонованого витоку. При цьому немає значення, яка саме секретна інформація у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки чи охорони правопорядку буде розголошена або будуть втрачені її матеріальні носії. Будь-який вид секретної інформації (сфера обігу) або її зміст має однакове значення для кримінальної відповідальності.

Отже визначальним критерієм при вирішенні питання про наявність чи відсутність в інформації, яка стала надбанням сторонніх осіб внаслідок її розголошення, протиправного заволодіння або втрати її матеріальних носіїв, відомостей, що становлять державну таємницю, є не наявність визначених законодавством реквізитів секретного документу, а саме наявність у таких відомостей властивостей завдати шкоду національній безпеці України.

Державна таємниця є конститутивною (обов’язковою) ознакою складу злочинів, що розглядаються, найважливішою складовою, яка має вирішальне значення як при кваліфікації злочинів, так і при розмежуванні подібних правопорушень. Водночас, закріплена на даний час у Кримінальному процесуальному кодексі України (далі – КПК України) процедура встановлення наявності чи відсутності у певних відомостях, що стали предметом злочину, державної таємниці, викликає численні зауваження щодо можливості винесення об’єктивних, достовірних та науково обґрунтованих висновків із цього питання та, як наслідок, винесення обґрунтованих судових рішень при розгляді таких кримінальних справ.

Це пов’язано з тим, що, відповідно до вимог частини першої статті 518 КПК України, підготовка висновку щодо завданої національній безпеці України шкоди в разі розголошення секретної інформації чи втрати її матеріальних носіїв здійснюється державними експертами з питань таємниць [25]. Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць, затверджено Указом Президента України від 01.12.09 р. № 987/2009 [26]. Переважно – це керівники міністерств, центральних органів виконавчої влади та їхні заступники (всього 164 особи).

Виходячи з положень діючого законодавства, всі ці високопосадовці *a priori* вважаються носіями наукових, технічних або інших спеціальних знань у сфері охорони державної таємниці. Проте, як засвідчила практика, визначальним критерієм при призначенні осіб на такі посади є наявність у них не стільки фахових, як управлінських здібностей та навичок, активна громадянська позиція або партійна приналежність. Окремі посади, на які покладено функції державних експертів з питань таємниць, є політичними за своєю сутністю. Отже, у більшості державних експертів з питань таємниць відсутні необхідні спеціальні знання у сфері охорони державної таємниці, досвід та навички, необхідні для проведення експертизи у зазначеній сфері, чим порушується такий важливий принцип судово-експертної діяльності, як компетентність експерта.

Слід зазначити, що для забезпечення діяльності державного експерта з питань таємниць та сприяння виконанню покладених на нього функцій у сфері охорони державної таємниці за його рішенням, відповідно до положень пункту 121 Порядку [24], можуть утворюватися експертні комісії при державному експерті з питань таємниць, до завдань яких, крім іншого, належить підготовка пропозицій щодо наявності чи відсутності у матеріальних носіях інформації відомостей, що становлять державну таємницю.

У таких випадках державний експерт з питань таємниць затверджує проект висновку, підготовлений цією комісією. Однак, під час проведення судової експертизи члени комісії, на відміну від державних експертів, не попереджаються про завідомо неправдивий висновок та відмову без поважних причин від виконання покладених на них обов’язків. Тому при проведенні експертизи в рамках кримінального провадження передбачена Порядком процедура надання висновку та відповідей на поставлені експерту питання суперечить КПК України, оскільки експерт, відповідно до частини 3 статті 101 КПК України, дає висновок від свого імені та несе за нього персональну відповідальність [25].

Крім цього, унормований пунктом 120 Порядку розподіл сфер повноважень державних експертів з питань таємниць закріплює за кожним експертом монопольне право виносити рішення лише в конкретній сфері інформаційних відносин, яка не перетинається з іншими експертами, що унеможливорює процесуальний порядок вибору експерта.

Таке монопольне право виносити остаточні висновки з питань, що належать до виключної компетенції цих експертів, призводить до того, що в окремих випадках виникає необхідність проведення експертизи про витік секретної інформації, що стався

через протиправні дії особи, яка є підлеглою державного експерта з питань таємниць. За таких обставин у експерта виникає зацікавленість у результатах цього дослідження, адже, відповідно до вимог статті 5 Закону України “Про державну таємницю”, забезпечення охорони державної таємниці в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов’язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій [23]. Тому, якщо державний експерт дійде до висновку, що дії його підлеглого призвели до витоку секретної інформації, відповідальність за це порушення, а саме за невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці (пункт 6 частини першої статті 212-2 Кодексу України про адміністративні правопорушення [27]), покладається також на керівника підприємства, установи, організації, тобто державного експерта з питань таємниць. Більше того, у випадку витоку секретної інформації з вини державного експерта з питань таємниць, проведення експертизи на предмет наявності у цих відомостях державної таємниці має бути доручено цій же посадовій особі, що фактично унеможлиблює її притягнення до кримінальної відповідальності за такий злочин.

Існуюча на даний час система розмежування сфер повноважень державних експертів з питань таємниць призводить до порушення принципу верифікованості (перевіряння) експертного дослідження, відповідно до якого процедура судово-експертного дослідження, обґрунтованість його проміжних результатів та остаточні висновки можуть бути піддані всебічній оцінці та перевірці як слідчим, так і іншими учасниками процесу.

Процесуальна сторона перевірки висновків експерта полягає в тому, що особа, яка призначила експертизу, здійснює їх логіко-процесуальну оцінку. За потреби висновки експерта перевіряються шляхом інших слідчих та процесуальних дій. У гносеологічному аспекті перевірка полягає в тому, що наукова обґрунтованість експертного дослідження піддається спеціальній оцінці компетентною особою, що залучається ініціатором експертизи [28, с. 33].

Процес дослідження істини у кримінальному процесі має бути істинним, забезпечувати отримання достовірних даних, а отже, ретельно контрольованим на всіх стадіях, перевіреним та добре вивченим. В усякому разі, як зазначає В. Тertiшник, мають бути відомі механізми формування тих чи інших висновків або інформаційних результатів, досліджені всі варіанти дії використаного методу, залежно від різних змінюваних умов його застосування [29, с. 346].

Якщо висновки експерта будуть визнані необґрунтованими, то засобом перевірки проведеної експертизи є нове дослідження у процесуальній формі повторної експертизи. Проте, коли виникають сумніви щодо достовірності висновків державного експерта з питань таємниць, провести повторну експертизу неможливо. Це пов’язано з тим, що сфери повноважень державних експертів з питань таємниць не перетинаються між собою, тобто їм належить монополне право виносити остаточні висновки з питань, що належать до їхньої компетенції. Крім цього, єдина база якісних і кількісних критеріїв, які дозволять визначити та перевірити обґрунтованість висновків експерта щодо наявності чи відсутності у предметі дослідження державної таємниці, відсутня, а можливість перегляду або оскарження таких рішень законодавством не передбачена.

Сьогодні “Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для внесення відомостей до державної таємниці та ступеня їх секретності”, які затверджено наказом Державного комітету України з питань державних секретів та технічного захисту інформації від 09.02.98 р. № 23, є єдиним

нормативним актом, який встановлює порядок оцінювання інформації на предмет наявності в ній відомостей, що становлять державну таємницю. Проте, як свідчить практика, ці рекомендації не знаходять свого застосування.

На тлі відсутності єдиного підходу до оцінювання можливої наявності та можливого обсягу шкоди національній безпеці України внаслідок несанкціонованого витоку інформації, що підлягає експертизі на предмет наявності в ній державної таємниці, є абсолютно виправданою критична позиція правозахисників щодо необґрунтованості більшості висновків державних експертів з питань таємниць та недостатності правової формалізації окремих видів державних інформаційних ресурсів.

Окремо необхідно зупинитися на питанні щодо предмета злочину, передбаченого ст. 422 Кримінальним кодексом України (далі – КК України). Відповідно до назви цієї статті та її диспозиції предметом цього злочину є відомості військового характеру, що становлять державну таємницю, або документи чи матеріали, що містять такі відомості.

До прийняття КК України 2001 року, ця стаття носила назву “Розголошення військової таємниці або втрата документів, що містять військову таємницю”. Вперше вона з’явилася у Положенні про військові злочини (1927 р.) [30], а потім відтворена у Кримінальному кодексі УСРР (1927 р.) у вигляді ст. 206²⁵ [31] та у Кримінальному Кодексі УРСР (1961 р.) у вигляді ст. 253 [32].

Військовою таємницею охоплювалися: а) секретні відомостей про збройні сили і обороноздатність Союзу РСР, що спеціально охороняються; б) документи, що містять відомості, які віднесені до державної таємниці; в) військові відомості, які не підлягають оголошенню, але не становлять державної таємниці. Таким чином, військову таємницю складали відомості військового характеру, що становили державну та службову таємницю.

Інститут військової таємниці існував одночасно з інститутом державної таємниці, проте, на відміну від останнього, перелік відомостей військового характеру не визначався жодним нормативним актом та був, за визначенням І. Слободянюка, тим самим “інструментом”, за допомогою якого партійно-радянський державний апарат середнього та нижчого рівнів, а також органи військового управління обмежували доступ громадян та засобів масової інформації до тих відомостей, розголос яких міг завдати шкоди інтересам обороноздатності та військової безпеки держави. Цьому сприяла спрощена процедура встановлення обмежувальної відмітки “Для службового користування” на будь-якому офіційному документі [33, с. 39].

Військова таємниця використовувалася переважно для захисту інформації з обмеженим доступом так званого проміжного характеру, тобто відомостей із грифом обмеження доступу “таємно”, які не відносилися до державної таємниці, та документів “Для службового користування”, які формувалися органами військового управління, військових частин, підрозділів, військових навчальних закладів та підприємств Міністерства оборони. При цьому система організації захисту військової таємниці була ідентичною до захисту державної таємниці: однакове діловодство, вимоги до технічних засобів виготовлення цих документів, порядок надання допуску та доступу до цих відомостей.

У випадку розголошення відомостей або втрати їх матеріальних носіїв необхідний був висновок компетентного органу військового управління щодо наявності або відсутності у цих відомостях державної або військової таємниці [34 с. 118]. Як правило, такі висновки робили керівники режимно-секретних підрозділів (т.зв. “восьме” управління).

Із прийняттям у 1994 році Закону України “Про державну таємницю” гриф обмеження доступу “таємно” став використовуватися у якості реквізиту документів, що містили відомості, віднесені до державної таємниці. Крім цього, цей Закон у статті 6 закріпив норму, згідно з якою до державної таємниці у порядку, встановленому цим

Законом, може бути віднесена інформація: у сфері оборони, у сфері економіки, у сфері зовнішніх відносин та у сфері державної безпеки і охорони правопорядку [35]. При цьому таке поняття, як відомості військового характеру, що становлять державну таємницю, цим та жодним іншим нормативним актом у сфері охорони державної таємниці не передбачене, а отже, не має жодного юридичного змісту.

Незважаючи на те, що новий КК України (2001 р.) відійшов від традиційної назви зазначеної статті й відмовився від поняття “військова таємниця”, виключивши із диспозиції статті відповідальність за розголошення військових відомостей, які не підлягають оголошенню, але не становлять державної таємниці, ми можемо стверджувати, що ст. 422 КК України в існуючій на даний час редакції встановлює кримінальну відповідальність за діяння, які не можуть бути вчинені у зв’язку із відсутністю предмета цього злочину. З урахуванням наведених аргументів, зазначена стаття, на наше переконання, має бути декриміналізована, оскільки у випадку розголошення відомостей у сфері оборони, що становлять державну таємницю, або втрати матеріальних носіїв такої інформації, відповідальність настає за статтями 328 або 329 КК України.

Висновки.

Закріплена у КПК України процедура призначення експертиз у кримінальному провадженні, яке містить державну таємницю, не забезпечує дотримання більшості принципів судово-експертної діяльності. Тому норма, викладена у частині першій ст. 518 КПК України про проведення експертизи у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації виключно посадовою особою, на яку покладено виконання функцій державного експерта з питань таємниць, має бути скасована.

Компетентність державного експерта з питань таємниць має визначатися не займаною посадою, а забезпечуватися системою підготовки та атестацією на право самостійного проведення судової експертизи. Атестація цих експертів повинна проводитися експертно-кваліфікаційною комісією, яка перевірятиме їх професійний рівень та спроможність проводити експертні дослідження відповідно до сучасних наукових методичних досягнень судової експертології.

Наявність єдиної методики оцінювання можливої шкоди внаслідок несанкціонованого витоку інформації, що підлягає експертизі на предмет наявності чи відсутності в ній державної таємниці, зробить процес оцінювання інформації зрозумілим і прозорим як для самих експертів, так і для інших учасників кримінального провадження під час перевірки обґрунтованості їхніх висновків.

Використана література

1. Таганцев Н.С. Курс русского уголовного права : часть общая. / Н.С. Таганцев . – Кн. 1. – СПб., 1874. – 284 с.
2. Пионтковский А.А. Учение о преступлении по советскому уголовному праву / А.А. Пионтковский : курс советского уголовного права : общая часть. – М. : Ин-т государства и права Акад. наук СССР, 1961. – 666 с.
3. Герцензон А.А. Квалификация преступлений / А.А. Герцензон. – М. : Изд-во ВЮА КА, 1947. – 26 с.
4. Кистяковский А.Ф. Элементарный учебник общего уголовного права с подробным изложением начал русского уголовного законодательства : часть общая / А.Ф. Кистяковский. – [3-е изд., печ. без перемен со 2-го]. – К. : Ф.А. Иогансон, 1891. – 892 с.

5. Никифоров Б.С. Объект преступления по советскому уголовному праву / Б.С. Никифоров. – М. : Госюриздат, 1960. – 232 с.
6. Круглевский А.Н. Имущественные преступления / А.Н. Круглевский. – М., 1915. – 212 с.
7. Новоселов Г.П. Учение об объекте преступления : методологические аспекты / Г.П. Новоселов. – М. : НОРМА, 2001. – 208 с.
8. Музика А.А., Лащук Є.В. Про загальне поняття предмета злочину. // Вісник Асоціації кримінального права України. – 2014. – № 1(2). – С. 103-118.
9. Михайленко П.П. Уголовное право Украины : общая часть / П.П. Михайленко. – К., 1995. – 431 с.
10. Бикмурзин М.П. Предмет преступления : теоретико-правовой анализ : монография / М.П. Бикмурзин. – М. : Юрлитинформ, 2006. – 184 с.
11. Филимонов В.Д. Охранительная функция уголовного права / В.Д. Филимонов. – СПб. : Юридический центр Пресс, 2003. – 198 с.
12. Тацкий В.Я. Объект и предмет преступления в советском уголовном праве / В.Я. Тацкий. – Х. : Выща шк., 1988. – 196 с.
13. Кримінальне право України : загальна частина : [підруч.] ; за ред. проф. В.В. Сташиса, В.Я. Тація. – [4-те вид., переробл. і допов.]. – Х. : Право, 2010. – 456 с.
14. Наумов А.В. Российское уголовное право : общая часть : курс лекцій / А.В. Наумов. – [2-е изд., перераб. и доп.]. – М. : БЕК, 1996. – 560 с.
15. Матишевський П.С. Кримінальне право України : загальна частина : підруч. для студ. юрид. вузів і ф-тів / П.С. Матишевський. – К. : А.С.К., 2001. – 352 с.
16. Кримінальне право України : загальна частина : підруч. для студентів юрид. спец. вищ. закладів освіти / [М.І. Бажанов, Ю.В. Баулін, В.І. Борисов та ін.] ; за ред. професорів М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – К.-Харків : Юрінком Інтер – Право, 2003. – 416 с.
17. Кримінальне право України : загальна частина : підруч. для студентів юрид. вузів і ф-тів. / [Г.В. Андрусів, П.П. Андрушко, В.В. Бенківський та ін.] ; за ред. П.С. Матишевського та ін. – К. : Юрінком Інтер, 1999. – 512 с.
18. Фесенко Є. Цінності як об’єкт злочину // Право України. – 1999. – № 6. – С. 75-78.
19. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.08 / Нац. юрид. академія. – Харків, 2002. – 21 с.
20. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.08 / Інститут держави і права НАН України ім. В.М. Корецького, 2003. – 222 с.
21. Мазуренко О., Розенфельд Н. Комп’ютерна інформація, як предмет злочинів, передбачених Розділом XVI КК України // Право України. – 2004. – № 6. – С. 80-83.
22. Савінова Н.А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні : теоретичні та практичні аспекти : монографія / Н.А. Савінова. – К. : ТОВ “ДСК”, 2011. – 342 с.
23. Про державну таємницю : Закон України від 21.01.94 р. // Відомості Верховної Ради України (ВВР). – 1994. – № 16. – Ст. 93.
24. Про затвердження Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України. (Для службового користування) : Постанова Кабінету Міністрів України від 18.12.13 р. № 939.
25. Кримінальний процесуальний кодекс України : Закон України // Відомості Верховної Ради України (ВВР). – 2013. – № 9-10. – № 11-12. – № 13. – Ст. 88.
26. Про перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць : Указ Президента України від 01.12.09 р. № 987/2009. – Режим доступу : http://kodeksy.com.ua/norm_akt/source-Президент/type-Указ/987-01.12.2009.htm

27. Кодекс України про адміністративні правопорушення : Закон Української РСР // Відомості Верховної Ради Української РСР. – 1984. – Додаток до № 51. – Ст.1122.

28. Щербаковский М.Г. Судебные экспертизы : назначение, производство, использование : учебно-практическое пособие / М.Г. Щербаковский. – Харьков : Эспада, 2005. – 544 с.

29. Тертишник В.М. Науково-практичний коментар до Кримінально-процесуального кодексу України / В.М. Тертишник. – К. : А.С.К., 2005. – 1056 с. – (Нормативні документи та коментарі).

30. Положение о воинских преступлениях : Постановление ЦИК и СНК СССР от 27 июля 1927 г. // Собрание Законов и Распоряжений Рабоче-Крестьянского Правительства СССР. – 1927. – № 50. – Ст. 505.

31. О введении в действие Уголовного Кодекса УССР ; в ред. 1927 года : Постановление ВЦИК от 8 июня 1927 г. // Собрание Узаконений и Распоряжений Рабоче-Крестьянского Правительства Украины. – 1927. – № 26-27. – Ст. 131.

32. Кримінальний кодекс Української РСР : Закон Української РСР. – К. : Держ. вид-во політ. л-ри УРСР, 1961. – 135 с.

33. Слободанюк И.А. Развитие уголовного законодательства об ответственности военнослужащих за посягательства на режим сохранности государственной и военной тайны : монография в авторской редакции / И.А. Слободанюк. – М. : Военный университет, 2005. – 182 с.

34. Комментарий Закона об уголовной ответственности за воинские преступления ; под ред. А.Г. Горного. – М.: Юрид. лит., 1981. – 152 с.

35. Про державну таємницю : Закон України від 21.01.94 р. // Відомості Верховної Ради України (ВВР). –1994. – № 16. – Ст. 93.

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

УДК 342.5:002.6

**БЄЛЄВЦЕВА В.В.**, доктор юридичних наук, старший науковий співробітник,  
завідувач сектору інформаційного правопорядку  
НДІ інформатики і права НАПрН України

## **УДОСКОНАЛЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ОБІГУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ**

**Анотація.** Розглянуто окремі аспекти міжнародного співробітництва щодо протидії правопорушенням у сфері комп'ютерної інформації. Наведені підходи до удосконалення національного законодавства з питань відповідальності за правопорушення у сфері комп'ютерної інформації, а також напрями міжнародної співпраці щодо протидії кіберправопорушенням.

**Ключові слова:** інформація, комп'ютерна інформація, кіберправопорушення, відповідальність, протиправні дії у сфері комп'ютерної інформації.

**Аннотация.** Рассмотрены отдельные аспекты международного сотрудничества в области противодействия правонарушениям в сфере компьютерной информации. Приведены подходы к усовершенствованию национального законодательства по вопросам ответственности за правонарушение в сфере компьютерной информации, а также направления международного сотрудничества в области противодействия киберправонарушениям.

**Ключевые слова:** информация, компьютерная информация, киберправонарушения, ответственность, противоправные действия в сфере компьютерной информации.

**Summary.** The article considers some aspects of international cooperation in area of counteraction to offences in the field of computer information. In conclusions the author of the article brings approach of improvement to the national legislation regarding responsibility for offence in the field of computer information, and also directions of international cooperation in area of counteraction to cyber offences.

**Keywords:** information, computer information, cyber offences, responsibility, illegal actions in the field of computer information.

**Постановка проблеми.** Сучасний розвиток держави та суспільства стає більш залежним від використання та роботи комп'ютерних систем для автоматичної обробки інформації. Особливої актуальності проблеми удосконалення правового регулювання комп'ютерної інформації набувають у зв'язку з інтенсивним процесом модернізації комп'ютерних систем, що призводить до появи нових можливостей вчинення правопорушень в інформаційній сфері.

В усьому світі комп'ютерні технології та мережа Інтернет досить швидко входять до повсякденного життя. За оцінкою незалежних експертів кількість користувачів Інтернет в Україні на кінець 2015 року складає не менш 58 %. За матеріалами Кабінету Міністрів України, біля 17 % користувачів мережі Інтернет здійснили купівлю-продаж через мережу Інтернет, а більш третини українців користувачів соціальних мереж здійснили придбання в он-лайн-режимі за допомогою соціальних мереж. Не дивлячись на те, що переважна більшість операцій в мережі Інтернет здійснюються із законними цілями, усесвітня мережа дедалі частіше використовується для запровадження шахрайських схем.

У 2014 році Управління по боротьбі з кіберзлочинністю МВС України зареєструвало 4800 злочинів у сфері ІТ, у 2015 році – 6025 [1].

У таких державах, як США, Великобританія, Японія, Канада, Німеччина державні уряди усвідомили характер загрози від комп'ютерних правопорушень, і створили більш менш ефективну систему законодавства і правоохоронних органів для боротьби з ними. Боротьба з такого роду правопорушеннями базується на розумінні необхідності тісної взаємодії і співпраці на усіх рівнях державної влади і приватного сектора економіки [2].

Глибоке дослідження проблем комп'ютерних технологій неможливе без залучення фахівців різних галузей знань – кібернетики, математики, інформатики, радіотехніки, електроніки, зв'язку тощо. Найважче фахівцям юридичної науки, оскільки необхідно як дати своєчасну і належну правову оцінку існуючим правопорушенням у сфері комп'ютерної інформації, так і підготувати норми закону до появи нових форм комп'ютерних правопорушень. Одночасно важливо не тільки професійно сформулювати закон, але і розробити механізм його реалізації.

За час дії статей Кодексу України про адміністративні правопорушення (далі – КУпАП) та Кримінального кодексу України (далі – КК України) правопорушення у сфері комп'ютерної інформації як в теорії, так і в практиці їх застосування виявилися істотні суперечності, причинами яких, є: недоліки правової конструкції норм про правопорушення у сфері комп'ютерної інформації, невірне уявлення правоохоронних органів про значення і роль досліджуваних норм у забезпеченні захисту та охорони суспільних стосунків, помилки у теоретичному і практичному тлумаченні деяких правових термінів і положень ст. 188<sup>39</sup>; 212<sup>2</sup> – 212<sup>6</sup> КУпАП та ст. 361-363<sup>1</sup> КК України.

**Метою статті** є визначення напрямів оновлення законодавства України з питань відповідальності за правопорушення у сфері обігу комп'ютерної інформації.

**Виклад основного матеріалу.** Захист інформації, що знаходиться в обігу в інформаційних системах та інформаційно-телекомунікаційних мережах, від несанкціонованого доступу, використання, розголошення, поширення, зміни або знищення інформації здійснюється в державі з метою забезпечення: цілісності і достовірності інформації (недопущення неправомірної зміни або знищення інформації); охорони конфіденційності інформації, доступ до якої обмежений законом або відповідно до закону; реалізації права на інформацію (гарантованого доступу до інформації, у випадках, коли такий доступ має бути забезпечений).

Слід зауважити, що основні поняття в законодавстві з питань обігу комп'ютерної інформації були сформульовані досить давно. За цей час науково-технічний прогрес не зупинявся, тому сьогодні з'являються нові терміни та категорії, які вимагають прийняття принципово нових законів. Наприклад, такий феномен як “спам”, що оцінюється у законодавстві багатьох держав як правопорушення у мережі Інтернет, в українському законодавстві не має належного регулювання.

Практика реалізації положень національного законодавства з досліджуваної проблематики свідчить про те, що наявні проблеми протидії правопорушенням у сфері обігу комп'ютерної інформації обумовлені недосконалістю правових норм, суперечністю їх тлумачення, відсутністю науково-методичних рекомендацій та офіційних управлінських роз'яснень щодо кваліфікації цих діянь, наприклад, постанов Верховного Суду України, а також ратифікованих міжнародних угод з питань ефективної спільної боротьби з даними видами правопорушень.

В українському законодавстві відсутній чіткий понятійний апарат, що стосується інформації та інформаційного обміну. Це дає, у свою чергу, можливість маніпулювати поняттями та уникати відповідальності. Якщо розглядати детальніше нормативно-правові акти України, то можна наявно побачити розбіжність в поняттях і відсутність



чітких визначень, особливо в наукових поняттях і технічних термінах у нормативно-правових актах, Держстандартах, технічній літературі тощо.

Державне регулювання у сфері захисту комп’ютерної інформації здійснюється шляхом встановлення вимог щодо захисту самої інформації, щодо власників інформації, користувачів інформації та власників інформаційних систем, користувачів інформаційно-телекомунікаційних мереж, а також відповідальності за несанкціонований доступ до конфіденційної інформації або за інші види правопорушень у сфері захисту інформації і права на інформацію.

З метою ефективної протидії несанкціонованому доступу до комп’ютерної інформації зусиль лише на національному рівні недостатньо. Необхідна розробка, стандартизація та уніфікація законодавства та програмних засобів, що дозволять визначити місцезнаходження та встановити особу, яка протиправно використовує комп’ютерну інформацію засобами комп’ютерних мереж та глобальних телекомунікаційних систем, відповідно до досвіду держав, що підписали Європейську конвенцію про кіберзлочинність [3].

Важливим документом у досліджуваній сфері є прийнята 15 березня 2016 року Стратегія кібербезпеки України [4]. Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Основу національної системи кібербезпеки України становитимуть Міністерство оборони України, Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Також слід акцентувати увагу на вирішенні організаційних проблем виявлення та ідентифікації осіб, які вчиняють протиправні дії у сфері комп’ютерної інформації на міжнародному рівні за допомогою оперативно-розшукових заходів. При цьому, з метою визнання судовими інстанціями різних держав у якості доказів документів передбачити методи фіксації, збору та передачі їх, можливості точного визначення географічного місцезнаходження вузлів мережі Інтернет для того, щоб правоохоронні органи змогли визначити країну походження й тим самим країну процесуальної юрисдикції, у тому числі використовуючи так звану “комп’ютерну розвідку”. З метою впровадження вищевикладених пропозицій видається необхідним доробити існуючі законодавчі акти, а також прийняти нові.

З урахуванням швидкого розвитку глобальних комп’ютерних мереж особливу роль могла б зіграти міжнародна інтегрована база даних кіберправопорушників, в якій фіксувалися б особи, схильні до вчинення протиправних дій у сфері комп’ютерної інформації, характеристика вчинених правопорушень тощо. При цьому необхідно розробити та запровадити закриті канали доступу до комп’ютерної мережі між підрозділами кіберполіції різних держав для повсякденного та екстреного зв’язку. Можливо, міжнародні угоди повинні включати деякі процесуальні санкції.

У зв’язку з цим необхідно розробити комплекс пропозицій до удосконалення правового регулювання протидії кіберправопорушенням. Отже, вважаємо за доцільне навести наші думки з цього приводу.

Використовуваний в українському законодавстві термін “правопорушення у сфері комп’ютерної інформації” певною мірою відповідає змісту Розділу XVI КК України. У світлі необхідних змін і розширення переліку складів даного виду правопорушень, уявляється правильнішим використання терміну “кіберправопорушення” для позначення будь-яких правопорушень, здійснених з використанням комп’ютера. Дане формулювання також відповідає традиційним уявленням про об’єкт посягання, як сферу соціальних відносин, і виводить з чисто технічної в суспільну площину.

Далі, на законодавчому рівні необхідно закріпити поняття комп'ютерної інформації, використовуване в законодавстві України (наприклад, комп'ютерна інформація – це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватись, змінюватись чи використовуватись за допомогою АЕОМ.

Також слід змінити поняття інформації, закріплене в українському законодавстві. При цьому можливо застосування підходу, використовуваного в міжнародно-правових актах, коли не дається чітке визначення інформації, але перераховується, що для цілей даного акту включається в поняття інформації. Такий підхід спрощує роботу правозастосовчих органів і робить ефективнішою реалізацію положень нормативно-правових актів. Разом з тим, такий підхід не знімає необхідності розроблення загального і прийняттого визначення інформації.

### **Висновки.**

Пропозиції з удосконалення законодавства щодо відповідальності за правопорушення у сфері обігу комп'ютерної інформації можуть бути зведені до наступного:

- у число ознак об'єктивної сторони деяких складів КУпАП та КК України слід включити використання комп'ютерної техніки. Таким чином, включення використання комп'ютерної техніки в число ознак об'єктивної сторони відповідало б і вимогам практики (такі зміни полегшили б кваліфікацію діянь), і підвищеної суспільної небезпеки подібних правопорушень. Як приклад, можна навести склад шахрайства, здійсненого з використанням комп'ютера (у японському законодавстві існує окремий склад комп'ютерного шахрайства), розкрадання, здійсненого шляхом використання комп'ютерної техніки; незаконне отримання інформації, що складає комерційну або банківську таємницю, шляхом перехоплення в засобах зв'язку, незаконного проникнення в комп'ютерну систему або мережу; порушення правил поведінки з інформацією (документами, комп'ютерною інформацією), що містить державну таємницю;

- вважаємо за необхідне внесення змін до статей КУпАП та КК України, що встановлюють юридичну відповідальність за ухилення від сплати податків і зборів. Зокрема, слід виділити таку ознаку об'єктивної сторони правопорушень, як ухилення від сплати податків у сфері електронної торгівлі. Підвищена суспільна небезпека даного правопорушення визначається його високою латентністю і зростаючими обігами електронної комерції, оскільки обіг електронної торгівлі в Україні постійно зростає. Офіційна статистика відсутня, проте, на думку експертів, електронні продажі будуть надзвичайно швидко зростати і стануть сегментом ринку, що динамічно розвивається. Правопорушення, пов'язані з ухиленням від сплати податків, з одного боку не відносяться до комп'ютерних правопорушень у вузькому сенсі, а з іншого – вони безпосередньо пов'язані з такою сферою як кіберпростір, комп'ютерні мережі і здійснюються з використанням комп'ютера;

- необхідно доповнити розділ XVI КК України статтями, що передбачають відповідальність за кібератаки на сайти в Інтернеті, за виробництво, продаж, придбання для використання комп'ютерних паролів, кодів доступу або інших даних, за допомогою яких можна отримати доступ до комп'ютерної системи з метою використання їх для вчинення протиправних дій. Слід криміналізувати й дії з виготовлення та збуту спеціальних засобів для неправомірного доступу до комп'ютерної системи або мережі;

– слід передбачити такі заходи з профілактики комп’ютерних правопорушень, як повідомлення приватних компаній про загрозу електронних атак і рекомендації щодо встановлення відповідного програмного забезпечення із захисту від комп’ютерних правопорушень;

– слід також встановити систему податкових пільг для тих підприємств, які вкладають кошти у розробку систем захисту інформації. Очевидно, що в результаті втрат приватних компаній від комп’ютерних правопорушень, шкоди зазнає й держава у цілому. Це виражається в недоотриманих податках, паралізації банківської діяльності тощо.

Підводячи підсумок слід зазначити, що аналіз міжнародно-правового регулювання комп’ютерних правопорушень дозволяє зробити висновок про відсутність належного та ефективного нормативно-правового регулювання комп’ютерних правопорушень і про гостру необхідність його розробки. Специфіка і тенденції розвитку законодавства з питань протидії комп’ютерним правопорушенням вимагають найпильнішої уваги учених різних спеціальностей. Піднімаючи питання забезпечення безпеки комп’ютерної інформації, хотілось привернути увагу до даної проблеми і стимулювати подальше обговорення цієї тематики.

### Використана література

1. В Україні зростає кількість кіберзлочинів / “Економічна правда” від 28.03.16 р. – Режим доступу : <http://www.epravda.com.ua/news/2016/03/28/587044>
2. Информационные технологии : учебник ; под ред. В.В. Трофимова. – М. : Издательство Юрайт ; ИД Юрайт, 2011. – 624 с.
3. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824-IV // Відомості Верхововної Ради України (ВВР). – 2006. – № 5-6. – Ст. 71.
4. Про рішення Ради національної безпеки і оборони України від 27.01.2016 р. “Про Стратегію кібербезпеки України” : Указ Президента України від 15.03.16 р. № 96/206 // Офіційний вісник України. – 2016. – № 23. – С. 69.

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

Інформація в інших галузях права

УДК 343.544+343.545:340.13+007.51:316.324.8

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”

**КОРУПЦІЯ – ІНФОРМАЦІЙНИЙ ОБРАЗ ВОРОГА
У КРИМІНАЛЬНОМУ ПРАВІ УКРАЇНИ**

Анотація. В статті досліджується феномен корупції з точки зору образу ворога, який є зручним для відволікання уваги суспільства від рішучої боротьби з іншими суспільно небезпечними явищами (викрадання коштів з бюджетів різних рівнів або програм по боротьбі з корупцією, необґрунтоване завищення тарифів на комунальні послуги, що веде до зубожіння населення, відмова у доступі до правосуддя, свідомо протидія з боку правоохоронних органів реалізації права на необхідну оборону тощо), розглянуто різновиди корупції – “римського” та “візантійського” типу.

Ключові слова: корупція, образ ворога, законодавча діяльність, інформаційне забезпечення, кримінально-правова охорона, “римський” тип корупції, “візантійський” тип корупції, права людини.

Аннотация. В статье рассматривается феномен коррупции с точки зрения образа врага, который является удобным для отвлечения внимания общества от борьбы с другими общественно опасными явлениями (хищения средств из бюджетов различных уровней или программ по борьбе с коррупцией, необоснованное завышение тарифов на коммунальные услуги, что приводит к обнищанию населения, отказ в доступе к правосудию, сознательное противодействие со стороны правоохранительных органов реализации права на необходимую оборону и т.п.), рассмотрены разновидности коррупции – “римского” и “византийского” типа.

Ключевые слова: коррупция, образ врага, законодательная деятельность, информационное обеспечение, уголовно-правовая охрана, “римский” тип коррупции, “византийский” тип коррупции, права человека.

Summary. The article deals with the phenomenon of corruption in terms of the image of the enemy, which is convenient to divert public attention from the fight against other social hazards (theft of funds from the budgets of various levels or anti-corruption programs, unjustified overstatement of tariffs for communal services, which leads to the impoverishment of population, denial of access to justice, conscious opposition of law enforcement services to the right to self-defense, etc.), considers types of corruption, like the “Roman” and “Byzantine” types.

Keywords: corruption, the image of the enemy, legislation, information provision, criminal legal protection, “Roman” type of corruption, “Byzantine” type of corruption, human rights.

Постановка проблеми. На сьогодні корупції та її різноманітним проявам оголошено непримириму боротьбу. Розробці понять, засобів та ефективних методів приділяється підвищена увага як на законодавчому рівні, так і в науковій літературі.

Аналіз останніх досліджень. Значний теоретичний внесок з питання розв’язання проблеми подолання корупції належить таким вченим, як П.П. Андрушко, Л.В. Багрій-Шахматов, Ю.В. Баулін, В.І. Борисов, В.М. Гаращук, П.Т. Гега, С.В. Гізимчук, В.О. Глушков, В.В. Голіна, Ю.В. Гродецький, І.М. Даньшин, А.П. Закалюк, В.С. Зеленецький,

О.Г. Кальман, М.І. Камлик, В.М. Киричко, С.М. Клімова, В.А. Клименко, В.П. Коваленко, М.Й. Коржанський, Р.Л. Максимович, Г.А. Матусовський, М.І. Мельник, В.О. Навроцький, В.Я. Настюк, І.С. Нуруллаєв, С.Г. Омельченко, А.В. Савченко, Т.І. Слущка, Є.Л. Стрельцов, В.Я. Тацій, В.І. Тютюгін, М.І. Хавронюк, Ф.В. Шиманський, О.М. Юрченко та ін.

Метою статті є дослідження стану боротьби з корупцією під кутом зору образу ворога, що пропонується суспільству, визначення витоків цього явища, напрацювання ефективних засобів запобігання та протидії.

Виклад основного матеріалу. Затверджена та діє Державна програма щодо реалізації засад державної антикорупційної політики в Україні (Антикорупційної стратегії) на 2015 – 2017 роки, затв. постановою Кабінету Міністрів України від 29 квітня 2015 р. № 265, що визначає пріоритети державної антикорупційної політики до 2018 року, реалізація яких створить основу для подальших реформ у цій сфері, зокрема дасть змогу усунути одну з основних причин незадовільного стану справ у сфері антикорупційної політики в Україні, якою є фрагментарність і недосконалість законодавчої та інституційної антикорупційної інфраструктури [12].

В сфері боротьби з корупцією задіяні значні людські, матеріальні та фінансові ресурси. Так, Європейський Союз виділяє понад 16 мільйонів євро на підтримку українських державних антикорупційних органів, про що, за повідомленням УНІАН, 16 вересня 2016 року заявив єврокомісар з питань розширення та європейської політики сусідства Йоганнес Ган [5]. Підтримка охоплюватиме консультації, навчання та зміцнення потенціалу; матеріальна допомога буде надходити у вигляді ІТ-обладнання та програмного забезпечення. Програму впроваджуватиме Данське агентство з міжнародного розвитку (DANIDA), яке має великий досвід в управлінні проектами в сфері належного врядування в Україні та за кордоном. До складу DANIDA буде залучено інші країни-члени, зокрема з Центральної та Східної Європи. Це допоможе, зокрема, скористатися їх багатим досвідом і знанням у цій галузі. Загальний бюджет програми – 16,34 млн. євро. З цієї суми внесок Євросоюзу становить 15 млн. євро, решта – кошти Данії [6].

Корупційним злочином, на думку В.М. Киричко, слід визнавати лише таке передбачене Кримінальним кодексом України (далі – КК України) суспільно небезпечне діяння, що містить не тільки ознаки відповідного складу злочину, а й ознаки корупції, передбачені ст. 1 Закону України від 7 квітня 2011 року № 3206-VI “Про засади запобігання і протидії корупції” [8, с. 26] (який був чинним на той момент; сьогодні замість вказаного нормативного акту діє Закон України “Про запобігання корупції” від 14 жовтня 2014 р. № 1700- VII [13]).

Згідно до положень ст. 1 Закону України “Про запобігання корупції” від 14 жовтня 2014 р. № 1700-VII корупційним правопорушенням визнається діяння, що містить ознаки корупції, вчинене особою, зазначеною у ч. 1 ст. 3 цього Закону, за яке законом встановлено кримінальну, дисциплінарну та/або цивільно-правову відповідальність, а корупцією, з свого боку, є використання особою, зазначеною у ч. 1 ст. 3 цього Закону, 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, зазначеній у частині першій статті 3 цього Закону, 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.

Втім, Є.Л. Стрельцов [15, с. 65-70] зазначає, що є помітною тенденція зміни філологічного (граматичного) тлумачення поняття корупції, починає переважати її розуміння від лат. *corrumpere* (“розтлівати”) як розкладання, розбещеності тощо, а не як підкупу, продажності, що мало місце раніше. В основних міжнародно-правових документах та національному законодавстві виділяються різновиди корупції за наступними критеріями: 1) за статусом суб’єктів; 2) за періодичністю діянь, що вчиняються; 3) за рівнями корупції. Корупційні вчинки мають різний предмет протиправної згоди, в тому числі: а) майно (як у натуральній, так і грошових формах); б) інформацію; в) рішення органів влади, судові рішення, рішення інших правоохоронних органів тощо. Крім того, до корупційних почали відносити діяння, які порушують встановлений порядок здійснення фінансових операцій (фінансової діяльності) або так званий фінансовий правопорядок, яким визначається здійснення різних видів господарської діяльності. Як свідчить міжнародний досвід, основна увага при розслідуванні та правовій оцінці фінансових шахрайств (зловживань), до переліку яких включена і корупція, приділяється не лише, а можливо і не стільки соціальним ознакам суб’єкта (його публічності, виконанню відповідних функцій держави або місцевого самоврядування), скільки виду (видам) соціальної роботи, яку він здійснює, виконуючи свою професійну діяльність (наприклад, надання публічних послуг).

Між тим, попри значний обсяг наукових досліджень, активність та гучні заяви з боку державних посадовців, насправді відсутні будь-які вагомі результати, а стан боротьби з корупцією продовжує залишатися незадовільним.

Так, на думку Ю.А. Пономаренко [11, с. 145], достатньо розбалансованими є законодавчі приписи про боротьбу з корупційними злочинами, і під ідеєю посилення боротьби з ними, навпаки, відбулася декриміналізація багатьох діянь. Так, необґрунтовано декриміналізовано перевищення влади, вчинене службовою особою, яка не є працівником правоохоронних органів (ст. 365 КК України). У результаті цього суди та органи досудового розслідування вимушені або не притягувати до відповідальності осіб, які вчиняють діяння істотної суспільної небезпечності, або ж неправомірно “підганяти” кваліфікацію вчиненого під зловживання владою або службовим становищем (ст. 364 КК України), хоча між перевищенням та зловживанням, як відомо, є сутнісна відмінність. Крім того, звужене визначення істотної шкоди та тяжких наслідків злочинів в сфері службової діяльності (пункти 3 і 4 примітки до ст. 364 КК України) викликало неможливість кримінально-правового реагування на ті випадки зловживання владою, перевищення влади або службової недбалості, що спричинили не матеріальну, а, наприклад, фізичну шкоду чи порушили конституційні права і свободи людини, чи підірвали авторитет і довіру до органів влади.

Н.А. Савінова пояснює такий стан речей “ефектом плато” (plateau effect)¹, в якому перебуває вітчизняна кримінально-правова доктрина, та за якого остання не розвиває кримінальне право з необхідним для звичайної людини й очікуваним суспільством коефіцієнтом корисності [14, с. 122]. При цьому звернуто увагу на доволі слушне питання: чому доктрина кримінального права не акцентує такої ж уваги на масовості і значній суспільній небезпечності інших кримінальних правопорушень (суддівські злочини, злочинні побори в школах, порушення прав пацієнтів, перевищення влади працівниками правоохоронних органів тощо), необхідності боротися з ними і забезпечувати належне кримінально-правове поводження із жертвами таких масових

¹ Ефект плато (plateau effect) – ефект “плоскогір’я”, “застрявання” на етапі розвитку, коли без надзусиль або змін підходів подальший рух “вгору” неможливий (див.: [2] та [3]).

діянь. Пояснення вбачається у наступному: “...тренди вигадування нового загального “ворога”, на кшталт тотальної боротьби з корупцією, за наявності переважно політичної, але не кримінально-правової складової, урешті-решт, призводитимуть до оскарження відповідних справ у ЄСПЛ і відповідно відшкодування з бюджету країни (а це наші кошти – зарплати, пенсії, стипендії). Безумовно, боротьба з корупцією має проводитися, але розумно, продумано і головне – з користю для суспільства, а не на шкоду йому” [14, с. 124].

Цей “образ ворога” у вигляді корупційних правопорушень є доволі привабливим для можновладців звичайної формації, які бажають звітуватися, але не мають справжнього наміру долати чи винищувати розглядуване явище.

Взагалі, під “образом ворога” розуміють [9] цілісне уявлення про опонента (явище), що інтегрує перекручені та ілюзорні риси, яке починає формуватися в ході латентного періоду конфлікту в результаті сприйняття, детермінованого негативними оцінками. Поки немає протидії, поки погрози не реалізовано, образ ворога носить опосередкований характер. У процесі ескалації образ ворога проявляється все більш виразно й поступово витісняє об’єктивний образ.

Про те, що образ ворога (у розглядуваному випадку – корупційні правопорушення та їх суб’єкти) стає домінуючим в інформаційній моделі конфліктної ситуації, свідчать: 1) недовіра (все, що виходить від ворога, або погано, або, якщо це розумно, то переслідує нечесні цілі); 2) покладання провини на ворога (корупція є відповідальною за всі проблеми у державі і суспільстві); 3) негативне очікування (все, що робить корупціонер, він робить з єдиною метою – завдати нам шкоди); 4) ототожнення зі злом (корупційні відносини втілюють протилежне тому, що я є і до чого прагну, корупціонер прагне знищити те, чим я дорожу, і тому повинен бути сам знищений); 5) виставлення “нульової суми” (все, що вигідно корупціонеру, шкодить нам, і навпаки); 6) деіндивідуалізація (той, хто належить до групи корупціонерів, автоматично є нашим ворогом); 7) відмова в співчутті (ми не маємо нічого спільного з нашим ворогом, ніяка інформація не зможе спонукати нас виявляти до нього гуманні почуття, керуватися етичними критеріями стосовно ворога нерозсудливо; зокрема, корупціонер не може бути звільнений, як всі інші правопорушники за аналогічних умов, від кримінальної відповідальності на підставі положень ст. 45 КК України у зв’язку з дійовим каяттям тощо).

Закріпленню образу ворога сприяють штучне фокусування надмірної уваги, зростання негативних емоцій, очікування деструктивних дій іншої сторони, негативні стереотипи і установки, значимість об’єкта конфлікту для особистості (групи), тривалість конфлікту, зовнішні очікування тощо.

Але об’єктивно слід визнати, що корупція є не більш суспільно небезпечною, ніж викрадання коштів з бюджетів різних рівнів або з програм по боротьбі з корупцією, необґрунтоване завищення тарифів на комунальні послуги, що веде до зубожіння населення, відмова у доступі до правосуддя (заперечення судами всіх ланок можливості оскаржити рішення про обрання запобіжного заходу у вигляді тримання під вартою, якщо воно прийняте (продовжено) не в межах досудового розслідування, а під час розгляду кримінальної справи по суті вже судом), свідомо протидія з боку правоохоронних органів реалізації права на необхідну оборону тощо.

Крім того, справжнє ставлення у суспільстві до проблеми корупції є вельми неоднозначним. Складність справи полягає у захворюванні вітчизняного суспільства саме на другий різновид корупції, яким запропоновано [1] відповідно найменування

“римський тип” (сплатити за те, щоб отримати надмірне або заборонене) та “візантійський тип” (сплатити за те, щоб отримати належне, гарантоване законами).

Але ж корупція існує повсюди. Скандали щодо її першого, тобто – римського, різновиду періодично спалахують у всіх благополучних країнах Європи та Америки. Тому є зрозумілим їх презирство та обурення в адресу суб’єктів міжнародного права, на території яких не подолано корупцію другого, візантійського типу (Україна, Камерун, Іран, Непал, Нікарагуа, Парагвай тощо).

Але не слід забувати, що в останніх корупція виступає своєрідним соціальним клапаном, який дозволяє ледве дотягнутися до мінімального рівня забезпечення і реалізації прав людини, що тільки на папері проголошені міжнародними та місцевими нормативними актами в якості найвищих цінностей держави і суспільства.

Як слушно зауважує О.О. Житний, “...якщо з якихось причин публічна влада не використовує для цього свого виключного повноваження на застосування кримінально-правового примусу або не здатна ефективно реалізувати його, суспільство звертається до засобів “квазіправосуддя” (влаштовуються самосуди над злочинцями, поширюється практика посередництва представників організованих злочинних угруповань у вирішенні майнових, господарських суперечок тощо), що лише сприяє подальшій конфліктогенності соціуму” [7, с. 83]. Те ж саме стосується і підґрунтя корупції.

Висновки та пропозиції.

Для ефективного подолання розглядуваних негативних явищ вбачається необхідним: 1) припинити традиційне оковамилювання європейської спільноти удаваними досягненнями; 2) зняти законодавче навантаження з проблеми корупції; 3) почати реальне знищення підґрунтя корупції “візантійського” типу шляхом забезпечення реальної можливості реалізації прав і свобод громадян.

Щодо першого напрямку, вважаємо, що не слід соромитися власного вітчизняного надбання, в тому числі в правовій сфері, є всі необхідні підстави рішуче і мотивовано відмовляти в імплементації запозичених положень, які є руйнівними для національної системи права.

Адже, як вірно зазначає Ю.А. Пономаренко [11, с. 143], виконання наших міжнародних зобов’язань, що впливають, наприклад, зі ст. 18 Кримінальної конвенції про боротьбу з корупцією (1999 р.), не зобов’язує державу до категоричних й неприйнятних дій, зокрема, до встановлення саме кримінальної відповідальності чи заходів кримінально-правового характеру стосовно юридичних осіб за вчинення від їх імені чи в їх інтересах корупційних правопорушень. Останні, як всі ми пам’ятаємо, були введені у сферу вітчизняного кримінально-правового законодавства навіть не через прагнення удосконалення, а з метою поліпшення візового режиму відносно Євросоюзу (Загальну частину КК України було доповнено розділом XIV-1 “Заходи кримінально-правового характеру щодо юридичних осіб” на підставі положень Закону України “Про внесення змін до деяких законодавчих актів України (щодо виконання Плану дій щодо лібералізації Європейським Союзом візового режиму для України стосовно відповідальності юридичних осіб)” від 23 травня 2013 р. № 314-VII).

Навпаки, міжнародними документами, зокрема, положеннями п. 5 Декларації 13-го Конгресу ООН по запобіганню злочинності та кримінальному правосуддю (Доха (Катар), 12 – 19 квітня 2015 р.) підкреслюється повага до суверенітету та внутрішнього законодавства – “...уважая при этом в полной мере принципы суверенитета и территориальной целостности государств и признавая ответственность государств-членов за обеспечение уважения человеческого достоинства, всех прав человека и основных свобод для всех, в частности для тех людей, которые испытывают воздействие

преступности, и тех людей, которые могут вступать в контакт с системой уголовного правосудия, в том числе уязвимых членов общества, независимо от их статуса, которые могут подвергаться самым разным и изощренным формам дискриминации, а также за предупреждение и противодействие преступлениям, мотивированным нетерпимостью или дискриминацией любого рода...” [4].

З приводу другого напрямку вбачається можливим внести зміни до ст. 45 (“Звільнення від кримінальної відповідальності у зв’язку з дійовим каяттям”) КК України шляхом виключення тексту “...крім корупційних злочинів...” та примітки² до неї, адже можливість звільнення особи, яка після вчинення злочину щиро покалася, активно сприяла розкриттю злочину і повністю відшкодувала завдані нею збитки або усунула заподіяну шкоду, повинна мати місце для будь-якого злочину невеликої тяжкості або необережного злочину середньої тяжкості, що вчинений вперше, *без будь-яких винятків*, що пов’язані з його тією чи іншою спрямованістю (корупційною, військовою, проти правосуддя тощо).

Як слушно зауважує О.М. Подільчак [10, с. 204], сумнівними є спроби запобігання корупції шляхом встановлення більш жорстоких покарань та правил, коли, на відміну від корупціонерів, більш асоціальні злочинці можуть скористатися багатьма можливостями пом’якшення свого становища (ст. ст. 47, 48, 81, 82 КК України).

Так само слід вчинити і з Розділом XIV-1 “Заходи кримінально-правового характеру щодо юридичних осіб” Загальної частини КК України, а саме – визнати його таким, що не відповідає загальним положенням і принципам вітчизняної правової доктрини, і скасувати у найближчий термін.

Стосовно реалізації третього напрямку, зокрема, в сфері кримінального права та практики його застосування, слушним буде рекомендувати представникам судової влади нарешті визначитися з власною громадянською позицією та не ухилятися від винесення виправдувальних вироків у всіх випадках, коли для цього є підстави відповідно до ч. 1 ст. 373 КПК України; забезпечувати доступ до правосуддя, в тому числі шляхом усунення перешкод для оскарження рішення про обрання запобіжного заходу у вигляді тримання під вартою, якщо воно прийняте (продовжено) не в межах досудового розслідування, а під час розгляду кримінальної справи по суті вже судом в порядку положень ст. ст. 315, 331 КПК України, які доповнити наступним текстом “оскарження рішень щодо про обрання, зміни або скасування запобіжного заходу здійснюється в порядку, передбаченому ст. ст. 309, 310 КПК України”; нарешті, усунути протидію з боку правоохоронних органів застосуванню інституту необхідної оборони (ст. 36 КК України), який тільки в законодавчій площині проголошений вельми зразково заохочувально і прогресивно, а на практиці перебуває у сфері нездійснених мрій законослухняних громадян тощо.

Перспективи подальших досліджень. Зазначені кроки сприятимуть подоланню корупції більше, ніж культивування її як образу ворогу в кримінальному праві України. Порушені 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.

² Примітка до ст. 45 КК України: Корупційними злочинами відповідно до цього Кодексу вважаються злочини, передбачені статтями 191, 262, 308, 312, 313, 320, 357, 410, у випадку їх вчинення шляхом зловживання службовим становищем, а також злочини, передбачені статтями 210, 354, 364, 364-1, 365-2, 368-369-2 цього Кодексу.

Використана література

1. Gorky Look. Сорта “того-самого”, або Каррумба! (парт оне). Коррумба, або Дай сюда, иди отсюда (парт тво). – Режим доступу : <http://gorky-look.livejournal.com/71734.html>
2. Fontanilla K. Overcoming the Exercise Plateau Effect. – Режим доступу : <http://sacng.com/ng/blog/2010/10/overcoming-the-exercise-plateau-effect>
3. Sullivan B., Herbert H. Thompson. What is the Plateau Effect? – Режим доступу : http://www.huffingtonpost.com/bob-sullivan/what-is-the-plateau-effec_b_3160082.html
4. Декларация Тринадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию. – Режим доступу : <https://documents-dds-ny.un.org/doc/UNDOC/LTD/V15/021/22/PDF/V1502122.pdf?OpenElement>
5. ЄС виділяє 16 мільйонів євро на боротьбу з корупцією в Україні / Економічна правда. – Режим доступу : <http://www.epravda.com.ua/news/2016/09/16/605743>
6. ЄС і Данія виділили €16 млн на боротьбу з корупцією в Україні. – Режим доступу : http://ukr.lb.ua/news/2016/09/15/345242_ies_i_daniya_vidilili_16 mln_borotbu.html
7. Житний О.О. Кримінальне право України та забезпечення миру (засоби і можливості) : 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. 80-83.
8. Киричко В.М. Кримінальна відповідальність за корупцію / В.М. Киричко. – Х. : Право, 2013. – 424 с.
9. Образ врага. Ескалація конфлікту / [Смельяненко Л. М., Петюх В. М., Торгова Л.В., Гриненко А.М.]. – (Конфліктологія : навч. посіб.). – К.: КНЕУ, 2003. – 315 с. – Режим доступу : buklib.net/books/24696
10. Подільчак О.М. Формування правосвідомості особи через реалізацію соціальної функції кримінального права : 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. 201-204.
11. Пономаренко Ю.А. Деякі перспективи розвитку кримінально-правової політики України на основі Доської Декларації 2015 року : 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. 142-146.
12. Про затвердження Державної програми щодо реалізації засад державної антикорупційної політики в Україні (Антикорупційної стратегії) на 2015 – 2017 роки : Постанова Кабінету Міністрів України від 29.04.15 р. № 265. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/265-2015-p>
13. Про запобігання корупції : Закон України від 14.10.14 р. № 1700-VII. – Режим доступу : <http://zakon3.rada.gov.ua/laws/show/1700-18/page>
14. Савінова Н.А. Эффект плато (plateau effect) у парадигмі вітчизняної кримінально-правової доктрини : 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. 119-124.
15. Стрельцов Є.Л. Еволюція у розумінні корупції: зміна акцентів : 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. 65-70.

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

УДК 399.187:338.242+ 681

**ЛЕОНОВ Б.Д.**, доктор юридичних наук, старший науковий співробітник,  
провідний науковий співробітник Українського науково-дослідного  
інституту спеціальної техніки та судових експертиз СБУ,  
**ЄВТУШЕНКО Є.В.**, провідний спеціаліст Українського науково-дослідного інституту  
спеціальної техніки та судових експертиз СБУ

## ПУБЛІЧНІ ЗАКУПІВЛІ В ЕЛЕКТРОННІЙ СИСТЕМІ “PROZORRO” ЗА СТАНДАРТАМИ ЄС

**Анотація.** У статті висвітлено організацію і проблеми, що виникають у відомствах, підприємствах та установах бюджетної сфери власності під час проведення публічних закупівель в системі електронних закупівель “ProZorro” за участю іноземних виробників, а також шляхи вирішення цих проблем.

**Ключові слова:** “ProZorro”, публічні закупівлі, система електронних закупівель, іноземні виробники, зовнішньоекономічна діяльність.

**Аннотация.** В статье освещены организация и проблемы, возникающие в ведомствах, предприятиях и учреждениях бюджетной собственности во время проведения публичных закупок в системе электронных закупок “ProZorro” при участии иностранных производителей, а также пути решения этих проблем.

**Ключевые слова:** “ProZorro”, публичные закупки, система электронных закупок, иностранный производитель, внешнеэкономическая деятельность.

**Summary.** The article is indicating issues of organization and the problems arising in the departments, enterprises and institutions of public sector property during public procurement using e-procurement system “ProZorro” with foreign manufacturers, as well as solutions for those problems.

**Keywords:** “ProZorro”, public procurement, e-procurement system, foreign manufacturers, foreign economic activity.

**Постановка проблеми.** Ринки державних закупівель Європейського союзу та України вкрай цікаві для бізнесу. Однак, через ряд обмежень європейський бізнес практично не бере участі в державних закупівлях України, у той же час, український бізнес фактично не має можливості прямої участі в державних закупівлях ЄС. Тому наступним напрямом розвитку державних закупівель є інтеграція з аналогічними системами ЄС. У сегменті технічного регулювання Україна за планом імплементації регламентів, гармонізованих з ЄС, до кінця 2016 року повинна підписати перші договори про взаємне визнання системи оцінки якості між Україною та Європою. Це означатиме, що українські підприємства зможуть без додаткової сертифікації поставляти свою продукцію в Європу, а європейські компанії у зворотному напрямку ввозити свої товари. Таким чином, проведення реформи державних закупівель зі створення на ринку України конкурентного середовища між резидентами та нерезидентами є актуальним питанням.

Побудова нової системи державних закупівель “ProZorro” розпочалась з вирішення питання по спрощення доступу бізнесу та іноземних компаній-виробників до тендерів (допорогової закупівлі) для збільшення конкуренції та прозорості. Підтримкою реформи займалися міжнародні організації Western NIS Enterprise Fund, USA ID, Європейський банк реконструкції та розвитку, Британський департамент міжнародного розвитку та

Федеральне міністерство економічного співробітництва та розвитку Німеччини. Головні розробники електронної системи “ProZorro” (Нефьодов М.Є., Стародубцев О.Є., Находа О.І.; Шимків Д.А., Нестуля В.О.) у своїх дослідженнях [1] висвітлюють спільну роботу з європейськими експертами у проєкті “Гармонізація системи державних закупівель в Україні зі стандартами ЄС” в контексті підготовки законопроекту “Про публічні закупівлі”.

**Метою статті** є вдосконалення організаційно-правових засад проведення електронних процедур закупівель із участю у торгах іноземних компаній-виробників для економії бюджетних коштів, створення на ринку України конкурентного середовища та спрощення податкового та митного законодавства.

**Виклад основного матеріалу.** У лютому 2015 року пілотний проєкт системи електронних державних закупівель “ProZorro” повинен був зробити закупівлі відкритими, прозорими і доступними для всіх форм учасників, у тому числі спростити механізм доступу учасників-нерезидентів у публічних процедурах.

Електронна система закупівлі може проводити допорогові і надпорогові процедури закупівлі. Закупівлі товарів та послуг на суму до 200 тис. грн, а робіт – до 1,5 млн. грн., вважаються допороговими, які регламентуються тільки внутрішнім регламентом роботи системи, технічними обмеженнями та вимогами замовника. Все, що вище цієї суми, переходить у розряд надпорогові закупівлі, які регулюються умовами Закону України “Про публічні закупівлі” від 25.12.15 р. № 922-VIII [2]. Надпорогові закупівлі мають такі процедури: відкриті торги, які вважаються єдиною конкурентною процедурою, переговорну процедуру закупівлі і конкурентний діалог.

Відповідно до цього Закону з 1 квітня 2016 року до системи були підключені близько 500 державних підприємств та всі центральні органи виконавчої влади, які почали проводити закупівлі виключно за допомогою системи “ProZorro”, а починаючи з 1 серпня, до системи “ProZorro” приєдналися усі державні підприємства, установи, організацій та їх об’єднання.

Законом передбачено, що вітчизняні та іноземні учасники всіх форм власності та організаційно-правових форм беруть участь у процедурах закупівель на рівних умовах. Замовники забезпечують вільний доступ усіх учасників до інформації про закупівлю, передбаченої цим Законом. Замовник не може встановлювати дискримінаційні вимоги до учасників.

Замовник застосовує одну з процедур закупівель (відкриті торги, конкурентний діалог або переговорну процедуру закупівлі) для визначення учасника-переможця. До початку оголошення процедури закупівлі замовник готує тендерну документацію в якій визначає порядок оформлення тендерної пропозиції, надання документального підтвердження за кваліфікаційними критеріям і вимогами, а також проєкт договору для поставки (виконання) товару (послуг). Основні умови щодо змісту тендерної документації викладені у статті 22 Закону [2].

Модель електронної системи закупівель побудована на централізації всіх закупівель, які відбуваються на авторизованих електронних майданчиках, при цьому результати проведених процедур закупівель відображаються на єдиній електронній платформі “ProZorro”.

З появою системи “ProZorro” кожен громадянин може побачити укладені договори, а також і допорогові закупівлі. До цього державні установи укладали прямі договори, які ніде не оприлюднювалися. Авторизовані електронні майданчики дозволяють отримати будь-кому інформацію у вільному доступі щодо початку і проведеної закупівлі, результати аукціону, які пропозиції прийняті та відхилені (з обґрунтуванням),

інформацію про переможця закупівлі та інші дані. Також завдяки модулю бізнес-аналітики “<http://bi.prozorro.org>” можна відслідковувати результати тендерів за замовниками, постачальниками, а також в розрізі регіонів.

Розміщення інформації в електронній системі закупівель здійснюється замовником шляхом її внесення та заповнення в електронному вигляді через автоматизоване робоче місце замовника. Оприлюднення інформації на веб-порталі здійснюється електронною системою закупівель.

Замовник для отримання доступу до автоматизованого робочого місця безоплатно проходить реєстрацію на авторизованому електронному майданчику або веб-порталі шляхом здійснення одного із способів ідентифікації/авторизації відповідно до постанови Кабінету Міністрів України від 24.02.16 р. № 166 “Про затвердження Порядку функціонування електронної системи закупівель та проведення авторизації електронних майданчиків” [3].

Розкриття тендерних пропозицій з інформацією та документами, що підтверджують відповідність учасника кваліфікаційним критеріям, та інформацією і документами, що містять технічний опис предмета закупівлі, здійснюється автоматично електронною системою закупівель відразу після закінчення електронного аукціону. Перед початком електронного аукціону автоматично розкривається інформація про ціни тендерних пропозицій.

Оцінка тендерних пропозицій проводиться автоматично електронною системою закупівель на основі критеріїв і методики оцінки, зазначених замовником у тендерній документації, та шляхом застосування електронного аукціону.

Замовник приймає рішення про намір укласти договір про закупівлю з переможцем процедури закупівлі, який надав найбільш економічно вигідну пропозицію, у зв’язку з цим тендерна пропозиція, запропонована нерезидентом (іноземна компанія-виробник) може розглядатися як економічно вигідна.

Суб’єкт зовнішньоекономічної діяльності (замовник) має право укладати будь-які види зовнішньоекономічних договорів (контрактів), крім тих, що обмежено вимогами чинного законодавства України.

Договір (контракт) укладається суб’єктом зовнішньоекономічної діяльності або його представником за типовою формою, що встановлено Положенням про форму зовнішньоекономічних договорів (контрактів), затвердженим наказом Мінекономрозвитку України від 06.09.01 р. № 201.

Відповідно до Закону України “Про зовнішньоекономічну діяльність” повноваження представника на укладення зовнішньоекономічного договору (контракту) може впливати з доручення, статутних документів, договорів та інших підстав, які не суперечать цьому Закону [5].

У більшості випадків виробник-нерезидент вимагає попередню оплату для реєстрації замовлення та подальшого виготовлення (виконання) товару (послуг). Чинне законодавство дозволяє розпорядникам та одержувачам бюджетних коштів у договорах про закупівлю товарів, робіт і послуг за бюджетні кошти передбачати (відповідно до рішення головного розпорядника бюджетних коштів) попередню оплату товарів, робіт і послуг на строк не більше 3 (трьох) місяців, у нерезидентів України, якщо вони не виробляються (не надаються) в Україні. При цьому постановою Кабінету Міністрів України від 23.04.14 р. № 117 “Про здійснення попередньої оплати товарів, робіт і послуг, що закуповуються за бюджетні кошти” передбачено попередню оплату не більше одного року [6].

Вимоги щодо Типових платіжних умов зовнішньоекономічних договорів (контрактів) викладено у постанові Кабінету Міністрів України та Національного банку України від 21.06.95 р. № 444 “Про типові платіжні умови зовнішньоекономічних договорів (контрактів) і типові форми захисних застережень до зовнішньоекономічних договорів (контрактів), які передбачають розрахунки в іноземній валюті”. Ця постанова містить рекомендації при проведенні розрахунків за зовнішньоекономічними договорами (контрактами) застосовувати документарне інкасо або документарний акредитив [7].

Документарне інкасо – форма розрахунків, за якою банк інкасує суму, яку має заплатити покупець продавцю проти надання відповідних документів. Банк виконує функції агента за грошовими розрахунками між експортером та імпортером. Він надає імпортеру, за вказівкою експортера/банку, документи про відвантаження товару/послуг, та інкасує проти цих документів належну суму, або отримує акцептований вексель.

При розрахунках у формі інкасо відповідальність банків обмежується переданням і оформленням документів проти оплати чи акцептування векселя.

На відміну від документарного акредитива, де банки несуть зобов’язання здійснити платіж, при розрахунках у формі інкасо вони не зобов’язані платити самі, якщо покупець не виконує, чи не в змозі виконати свої зобов’язання щодо оплати.

Документарний акредитив – це безвідкличне зобов’язання банку-емітента здійснити платіж проти належного представлення бенефіціаром (експортером, продавцем) документів.

Оскільки при виконанні зобов’язань з інкасо при відвантаженні чи наданні послуг оплата постачальнику не гарантується, доцільно використовувати документарне інкасо тільки у таких випадках:

- продавець (експортер) і покупець (імпортер) довіряють один одному;
- бажання платити і кредитоспроможність покупця не викликають сумніву;
- політична, економічна і правова атмосфера в країні імпортера є стабільною;
- міжнародні платіжні операції країни імпортера не обмежуються.

Основним нормативним актом, що регулює порядок проведення розрахунків у іноземній валюті між резидентами та нерезидентами України є Закон України “Про порядок здійснення розрахунків в іноземній валюті” [8].

Стаття 2 цього Закону визначає, що імпортні операції резидентів, які здійснюються на умовах відстрочення поставки (фактичного проведення попередньої оплати), у разі, якщо таке відстрочення перевищує 180 календарних днів з моменту здійснення авансового платежу або виставлення векселя на користь постачальника продукції (робіт, послуг), що імпортується, потребують висновку центрального органу виконавчої влади, що реалізує державну політику у сфері економічного розвитку [8].

Одночасно при застосуванні розрахунків щодо імпортних операцій резидентів у формі документарного акредитиву строк починає діяти з моменту здійснення уповноваженим банком платежу на користь нерезидента.

Порушення резидентами строків у 180 календарних днів або інших, що встановлені НБУ, тягне за собою фінансову відповідальність (штрафні санкції – пеня) за кожний день прострочення у розмірі 0,3 % суми неоподаткованої виручки (вартості недопоставленого товару) в іноземній валюті, перерахованої у грошову одиницю України за валютним курсом НБУ на день виникнення заборгованості. Загальний розмір нарахованої пені не може перевищувати суми неоподаткованої виручки (вартості недопоставленого товару).

Висновок стосовно віднесення операцій резидента до поставки складних технічних виробів і товарів спеціального призначення, та продовження встановлених строків (далі – Висновок) видається Мінекономрозвитку.

Про видачу висновку Мінекономрозвитку резидент інформує протягом п'яти робочих днів з дати його видачі Національний банк та Державну фіскальну службу.

Постанова Національного банку України від 30.12.03 р. № 597 “Про переказування коштів у національній та іноземній валюті на користь нерезидентів за деякими операціями” забороняє уповноваженим банкам здійснювати авансові платежі (попередню оплату) в іноземній валюті за імпортом товару за зовнішньоекономічним договором (контрактом), загальна вартість якого перевищує 50 000 доларів США (або еквівалент цієї суми в іншій іноземній валюті за офіційним курсом гривні до іноземних валют, установленим НБУ на день укладення договору), якщо НБУ повідомлено уповноважений банк про не підтвердження можливості здійснення цих платежів. Підтверджені платежі виконуються не раніше четвертого операційного дня з дня подання уповноваженим банком інформації про ці платежі в реєстрі [9].

Уповноважені банки для погодження з НБУ зазначених платежів зобов'язані формувати відповідний реєстр, який подається до НБУ засобами електронної пошти разом з копіями документів (у сканованому вигляді), які є підставою для здійснення цих операцій.

Відповідно до постанови Національного банку України від 30.12.03 р. № 597 “Про переказування коштів у національній та іноземній валюті на користь нерезидентів за деякими операціями” пакет документів, що подається до НБУ для підтвердження можливості як купівлі, так і перерахування іноземної валюти, має також містити довідку Державної фіскальної служби України про відсутність у резидента заборгованості з податків, зборів, платежів та в передбачених постановою Правління НБУ, випадках – відповідний акт цінової експертизи (погодження) [10].

Не потребує включення до реєстру для подання до НБУ інформація про переказ коштів, що здійснюється виключно за рахунок іноземної валюти, купленої з дотриманням вимог підпункту 2 постанови НБУ [9].

Одночасно з умовами придбання/перерахування валютних коштів за зовнішньоекономічними контрактами НБУ встановлює вимоги щодо граничних термінів використання/оплати або продажу придбаних для потреб клієнта-резидента валютних коштів. Клієнт-резидент зобов'язаний використати придбану іноземну валюту, що куплена у встановленому порядку через суб'єкта ринку, не пізніше ніж за 10 робочих днів після дня її зарахування на його поточний рахунок на потреби, зазначені в заяві про купівлю іноземної валюти (за умови, якщо придбання валюти не проводилось для покриття акредитива) [11].

У разі невиконання клієнтами-резидентами зазначених вимог вони зобов'язані відповідно до законодавства продати протягом 5 робочих днів куплену іноземну валюту. При цьому позитивна курсова різниця, що може виникнути за такою операцією, щокварталу перераховується до Державного бюджету України, а збільшена курсова різниця відноситься до негативного результату господарської діяльності резидента [8].

### **Висновки.**

За результатами аналізу законодавчих актів у сфері публічних закупівель необхідно констатувати відсутність законних підстав та відповідно технічних можливостей для електронних переговорів в системі “ProZorro” у разі застосування переговорної процедури закупівлі або конкурентного діалогу за участю іноземних компаній-виробників. Під час виконання зовнішньоекономічного контракту виникає

низка ризиків, які пов’язані з дотриманням умов нерезидента у разі придбання високоточного та аналітичного обладнання, що потребує запрошення фахівця постачальника для проведення пусконаладжувальних робіт та навчання персоналу, а витрати на проїзд фахівця-виробника сплачуватимуться за рахунок замовника. Перегляд ціни після визначення переможця у бік збільшення або зменшення за умовами контракту можливий на розсуд постачальника-нерезидента без повідомлення замовника. При цьому постачальник-нерезидент залишає за собою право розпочати процес поставки до закінчення строку дії контракту.

Оскільки витрати щодо розмитнення товару та отримання різних дозвільних документів здійснюються за рахунок коштів, не запланованих річним планом закупівель для сплати цих платежів, оплата проводиться на підставі різних документів та за різними кодами економічної класифікації видатків бюджету, які також не передбачені кошторисними призначеннями та потребують перерозподілу. Зазначене може призвести до збільшення витрат коштів державного бюджету, що вважатиметься економічно не обґрунтованим.

Враховуючи викладене, вважаємо, що подальша модернізація української системи державних закупівель сприятиме:

поліпшенню умов для конкуренції на ринку державних контрактів в Україні за результатами підвищення рівня законності, відкритості та неупередженості процесу укладення контрактів;

забезпеченню кращого співвідношення ціни та якості при виборі переможця тендеру на державні закупівлі;

удосконаленню системи управління державними фінансами, у тому числі зменшенню надмірного витрачання державних коштів;

зміцненню позиції України на міжнародному рівні завдяки виконанню міжнародних зобов’язань (особливо перед міжнародними торговими партнерами, донорами та кредиторами);

підвищенню конкурентоспроможності і експортного потенціалу українських підприємств на міжнародних ринках, як результат відповідності сучасним вимогам щодо державних контрактів.

### Використана література

1. Система “ProZorro” готова до повного переведення держзакупівель в електронний формат. – Режим доступу: <http://www.bugalter.com.ua/zakupivli-za-derzhkoshty>
2. Про публічні закупівлі : Закон України від 25.12.15 р. № 922-VIII. – Режим доступу : <http://www.zakon.rada.gov.ua>
3. Про затвердження Порядку функціонування електронної системи закупівель та проведення авторизації електронних майданчиків: постанова Кабінету Міністрів України від 24.02.16 р. № 166. – Режим доступу : <http://www.zakon.rada.gov.ua>
4. Про затвердження Положення про форму зовнішньоекономічних договорів (контрактів): наказ Міністерства економіки та з питань європейської інтеграції України (Міністерство економічного розвитку і торгівлі України) від 06.09.01 р. № 201. – Режим доступу : <http://www.zakon.rada.gov.ua>
5. Про зовнішньоекономічну діяльність: Закон України від 16.04.91 р. № 959-XII. – Режим доступу : <http://www.zakon.rada.gov.ua>
6. Про здійснення попередньої оплати товарів, робіт і послуг, що закуповуються за бюджетні кошти: постанова Кабінету Міністрів України від 23.04.14 р. №117. – Режим доступу : <http://www.zakon.rada.gov.ua>



7. Про типові платіжні умови зовнішньоекономічних договорів (контрактів) і типові форми захисних застережень до зовнішньоекономічних договорів (контрактів), які передбачають розрахунки в іноземній валюті: постанова Кабінету Міністрів України та Національного банку України від 21.06.95 р. № 444. – Режим доступу : <http://www.zakon.rada.gov.ua>

8. Про порядок здійснення розрахунків в іноземній валюті: Закон України від 23.09.94 р. № 185/94. – Режим доступу : <http://zakon.rada.gov.ua>

9. Про особливості здійснення деяких видів валютних операцій : постанова Національного банку України від 23.02.15 р. № 124. – Режим доступу : <http://www.zakon.rada.gov.ua>

10. Про переказування коштів у національній та іноземній валюті на користь нерезидентів за деякими операціями: постанова Національного банку України від 30.12.03 р. № 597. – Режим доступу : <http://www.zakon.rada.gov.ua>

11. Про затвердження нормативно-правових актів Національного банку України : постанова Національного банку України від 10.08.05 р. №281. – Режим доступу : <http://www.zakon.rada.gov.ua>

12. Про затвердження Порядку продовження строків розрахунків за зовнішньоекономічними операціями : постанова Кабінету Міністрів України від 29.12.07 р. № 1409. – Режим доступу : <http://www.zakon.rada.gov.ua>

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

До відома авторів

“ІНФОРМАЦІЯ І ПРАВО” – 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 інформаційного права, інформаційної і національної безпеки, правової інформатики та інформації в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має бути спрямований на вирішення визначених автором наукових завдань згідно з такими напрямками досліджень:

- Інформаційне право.
- Правова інформатика.
- Інформаційна і національна безпека.
- Інформація в інших галузях права.

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:
 - постановка проблеми (загальна характеристика) та аналіз досліджень (публікацій), в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття;
 - формування мети (постановка завдання) статті;
 - виклад основного матеріалу – вирішення завдання та обґрунтування результатів.
- Висновки, пропозиції за результатами розв’язання проблеми.
- Перспективи щодо подальших досліджень.
- Використана література (згідно з наказом ВАК України від 26.01.08 р. № 63).
- Підпис, адреса (e-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 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

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

№ 4(19)

2016

| | |
|--|---|
| Засновники журналу: | <ul style="list-style-type: none">- 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”. |
| Видавець: | © Науково-дослідний інститут інформатики і права Національної академії правових наук України. |
| Адреса редакції: | 01032, м. Київ, вул. Саксаганського, 110-В.
НДІ інформатики і права НАПрН України.
Тел.: 234-94-56; e-mail: bvm777@ ukr.net |
| Веб-сторінки журналу у мережі Інтернет: | //www.ippi.org.ua – (НДІ інформатики і права НАПрН України);
//www.nbuv.gov.ua – (Нац. бібліотека України ім. В.І. Вернадського). |