УДК 343.3/.7:004.056 (477)

БАТИРГАРЕЄВА В.С., *доктор юридичних наук, с.н.с.,* головний науковий співробітник НДІ інформатики і права НАПрН України.
ORCID: https://orcid.org/0000-0003-3879-2237.

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ЗАСОБАМИ КРИМІНАЛЬНОГО ПРАВА

Анотація. *У статті обґрунтовується необхідність створення чіткої несуперечливої концептуальної моделі кримінально-правового захисту інформаційного простору Української держави та внесення у зв'язку із цим змін та доповнень до чинного Кримінального кодексу України.*

Ключові слова: *інформаційний простір, інформаційна безпека, інформаційні відносини, інформаційні злочини, кібербезпека.*

Summary. *The article substantiates the need to create a clear and consistent conceptual model of criminal legal protection of the information space of the Ukrainian state and to make changes and additions to the current Criminal code of Ukraine in this regard.*

Keywords: *information space, information security, information relations, information crimes, cybersecurity.*

Аннотация. *В статье обосновывается необходимость создания четкой непротиворечивой концептуальной модели уголовно-правовой защиты информационного пространства Украинского государства и внесения в связи с этим изменений и дополнений в действующий Уголовный кодекс Украины.*

Ключевые слова: *информационное пространство, информационная безопасность, информационные отношения, информационные преступления, кибербезопасность.*

Постановка проблеми. Для якомога кращого розуміння феномену глобалізації сучасного світу та його проблем виникає потреба в осмисленні цього світу як єдиної системи комунікативних зв'язків, що стає можливим завдяки стрімкому розвитку й запровадженню інформаційних технологій у життєдіяльність суспільства та переходу останнього в якісно нову фазу свого розвитку – інформаційну. Одними із наочних проявів цього процесу є не лише поступове нівелювання значення фізичних кордонів між державами, які дедалі сприйматимуться не більше, ніж умовністю, даниною часу, а й епоха тотального панування інформаційного простору з усіма негативними та позитивними наслідками, що випливають із цього факту. Перед деякими із негативних аспектів інформаційного простору людина, суспільство та держава виявляються протягом якогось часу ледве чи небеззахисними, адже під впливом інформаційної глобалістики інколи створюються такі загрози переліченим фундаментальним категоріям, які піддаються правовій оцінці "із запізненням", а тому про ніяку своєчасність реагування на них, на жаль, не може йтися, хоча відповідно до ст. 17 Конституції України забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Тому недаремно парною для категорії "інформаційний простір" стає саме категорія "інформаційна безпека", визначень якої на теперішній час безліч. Не вдаючись до дискусії про повноту охоплення подібними визначеннями усіх сенсоутворюючих рис описаного явища, лише зазначимо, що, по-перше, безпека інформаційна від другої половини XX ст. стає одним із найважливіших елементів національної безпеки [1, с. 74], адже вона є невід'ємною частиною, яка

входить до інших складових національної безпеки, таких як економічна, воєнна, політична, екологічна, науково-технологічна тощо, а, по-друге, існування й реалізація багатьох загроз у цій сфері вже на теперішній час кваліфікуються як правопорушення з відповідними правовими наслідками, що тягне їх вчинення. Причому із розвитком інформаційного суспільства відбувається збільшення кількості порушень правових норм, що регулюють інформаційні відносини [2, с. 56]. Свого часу раніше чинний Закон України "Про основи національної безпеки України" від 2003 р. у ст. 7 визначав, що до головних реальних і потенційних загроз національним інтересам і національній безпеці України в інформаційній сфері належать: прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [3][*]. У 2015 р. у нашій державі прийнято Стратегію національної безпеки України, в якій до актуальних загроз саме інформаційній безпеці віднесено: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства (п. 3.6). Що стосується загроз кібербезпеці і безпеці інформаційних ресурсів, то до їх числа належать: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом (п. 3.7) [5]. Не дивлячись на спробу визначитися з основними загрозами розглядуваній сфері, слід відзначити, що стосовно деяких явищ, що мають, безумовно, шкідливий характер, законодавець й досі у роздумі. Висловлене, наприклад, стосується винайдення все нових і нових форм здійснення як масштабного психологічного впливу на населення, що мешкає на певній території (особливо в умовах ведення так званих гібридних війн), так і впливу, мішенню якого стають окремі люди або групи людей (стокерство, мобінг, булінг, хейзинг та ін.). Крім того, конче потрібна реакція держави на випадки навмисного приховування або необґрунтованої відмови посадових осіб від надання відповідної інформації чи надання інформації, що не відповідає дійсності; використання або(та) поширення інформації щодо особистого життя будь-якої особи без її згоди іншою особою, якій така інформація відома внаслідок виконання своїх службових обов'язків тощо. Так само не можна не звернути увагу на те, що через відсутність у чинному законодавстві України відповідальності за систематичне умисне поширення дезінформації наразі назріла потреба в принциповому обговоренні законопроєкту "Про протидію дезінформації", презентованого Міністерством культури, молоді та спорту України. Метою цього документа є захист інформаційного простору України від дезінформації та гібридних загроз із питань, які становлять суспільний інтерес і стосуються національної безпеки, територіальної цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров'я громадян, довкілля тощо [6].

Проблематика розвитку й убезпечення інформаційного простору постійно знаходиться в зоні підвищеної уваги науковців і практиків. Різні аспекти захисту

[*] *Примітка.* У 2018 р. прийнято новий Закон України "Про національну безпеку України", в якому окремо вже не наводиться перелік загроз інформаційній (кібернетичній) безпеці країни (див. [4]).

інформаційного простору України засобами кримінального права, у тому числі у контексті реалізації завдань із захисту національної безпеки, а так само питання створення ефективної системи запобіжних заходів від загроз у зазначеній сфері розроблялися такими вітчизняними вченими, як Д.С. Азаров, П.С. Берзін, М.В. Бутузов, В.Д. Гавловський, М.В. Карчевський, М.О. Кравцова, С.А. Кузьмін, О.М. Литвинов, В.В. Марков, А.І. Марущак, А.А. Музика, В.Г. Пилипчук, О.Е. Радутний, Н.А. Савінова, В.Б. Харченко, В.П. Шеломенцев та ін. Звісно ж, ці розробки ґрунтуються на доробках у галузі інформаційного права та правових засобів регулювання кіберпростору, найбільш значні з яких відображені у працях вітчизняних та зарубіжних вчених (О.А. Баранов, В.Ю. Баскаков, Дж. Голдсміт (J. Goldsmith) і Т. Ву (T. Wu), М.І. Дімчогло, В.М. Желіховський, М.З. Згуровський, Л.П. Коваленко, Б.А. Кормич, Л. Лесссіг (L. Lessig), М. Лібіцкі (M.C. Libicki), В.А. Ліпкан, О.В. Логінов, Е. Лонгуорт (E. Longworth), В. Майер-Шонбергер (V. Mayer-Schunberger), Ю.Є. Максименко, О.А. Мандзюк, П.Є. Матвієнко, Г.М. Писаренко, Л.І. Рудник, В. І. Теремецький, Е. Тоффлер (A. Toffler), М. Цівіц (M. Ziewitz), В.С. Шапіро, О.В. Шепета та ін.

Проте висловлені ідеї у працях згаданих вище учених-правників здебільшого стосуються чи то розв'язання загальнотеоретичних проблем убезпечення інформаційного простору (насамперед кіберпростору) за допомогою правових механізмів цього захисту, чи то захисту інтересів особи, суспільства або держави від окремих видів правопорушень у розглядуваній сфері. Однак, коли триває напружена робота над новим Кримінальним кодексом України, природно виникає запитання про концептуальну модель кримінально-правового захисту інформаційного простору, що братиметься до уваги під час упорядкування норм про кримінальну відповідальність за злочини відповідної спрямованості. Тому є сенс звернутися до аналізу позицій із приводу забезпечення нормального функціонування інформаційного простору засобами, що за своєю природою виявляються *ultima ratio*.

Метою статті є: по-перше, аналіз нормативного матеріалу, за допомогою якого виконуються завдання закону про кримінальну відповідальність за правопорушення в інформаційному просторі України на теперішній час; по-друге, вибірковий огляд позицій, що висловлені з приводу захисту зазначеного сегмента життєдіяльності суспільства; по-третє, моделювання можливого підходу до організації правової матерії у сфері захисту інформаційного простору України від кримінально караних правопорушень.

Виклад основного матеріалу. На теперішній час відповідальність за порушення так званих інформаційно-правових норм передбачається у цивільно-правовому, адміністративному та кримінальному законодавстві. Так, за правопорушення в інформаційній сфері лише Кримінальним кодексом України встановлена відповідальність у кількох десятках статей. При цьому особливістю нинішньої моделі захисту інформаційних відносин є те, що відповідні норми містяться у різних розділах Особливої частини законодавства про кримінальну відповідальність. Однак важливо підкреслити, що розглядаючи питання відповідальності за протиправні діяння в інформаційному просторі, а так само криміналізуючи нові суспільно небезпечні діяння у цій сфері, йдеться не лише про кіберпростір як середовище, створюване інформаційними системами, об'єднаними в локальні або глобальні комп'ютерні мережі або реалізованими на окремих комп'ютерах та інших пристроях [7, с. 191], а й про циркуляцію будь-якої інформації, з використанням якої може пов'язуватися вчинення злочину.

Так би мовити, класичними прикладами порушення законодавства в інформаційному просторі є комп'ютерні злочини (розділ XVI Особливої частини КК

України), незаконне розголошення інформації з обмеженим доступом (наприклад, розголошення відомостей, що становлять державну або професійну (службову) таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових або професійних обов'язків (статті 111, 132, 163, 168, 232, 384, 387 та ін. КК України) або, навпаки, приховування чи перекручування певних відомостей (інформації) (статті 220^2, 232^2, 238, 298^1 та ін. КК України)). Також важливе значення інформаційний вплив (інакше кажучи, певні дії в інформаційному просторі) на особу має і під час вчинення багатьох інших злочинів. Так, об'єктивна сторона доведення до самогубства може полягати у шантажі, тобто погрозі розголошення відомостей, які потерпілий бажає зберегти в таємниці [8, с. 53]. Шахрайство, в якому обман потерпілого здійснюється шляхом незаконних операцій з використанням електронно-обчислювальної техніки (так звані комп'ютерні шахрайства), є наочним прикладом того, як "успіх" злочинних дій стає можливим завдяки інформаційному впливу на особу за допомогою інструментів кіберпростору. Як бачимо, низка статей КК України встановлює відповідальність за вчинення певних дій, що можуть мати значення для інформаційних відносин, хоча в диспозиціях таких статей про ці відносини й не згадується. Але тим не менш, повторимося, до орбіти протиправних дій "потрапляє" інформаційний простір, в якому потерпіла особа втрачає впевненість та починає відчувати себе в небезпеці, інколи вчиняючи будь-які дії, що, врешті-решт, завдають шкоду самій цій особі.

Якщо звернутися до Конвенції про кіберзлочинність 2001 р., підготовленої Радою Європи та ратифікованої Україною у 2005 р., із самої назви документа випливає, що правопорушення в інформаційному просторі цією Конвенцією обмежуються лише кіберпростором. Так, нею розрізнюються чотири види кримінальних правопорушень:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані та втручання в систему);

2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами);

3) правопорушення, пов'язані зі змістом (дитяча порнографія);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [9].

Отже, у цілому йдеться про загрози кібербезпеці, метою якої є виключно захист оброблюваних цифрових даних, на відміну від інформаційної безпеки в цілому, що призначена для комплексного захисту інформаційних ресурсів і даних у будь-якій формі.

Засновуючись на наведеній класифікації конвенційних правопорушень, О.В. Юрченко та О.Д. Дудченко наводять своєрідний атлас злочинів у сфері кібернетичної безпеки, одночасно доповнюючи перелік тих злочинів, що не віднесені Конвенцією до виокремлених груп правопорушень. Так, до групи злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем ними віднесено незаконний доступ (хакерство, злам шифру, інформаційний шпіонаж, перехоплення даних, спотворення інформації та систем). Група злочинів, пов'язаних із контекстом, може бути представлена такими діяннями, як виготовлення еротичних або порнографічних матеріалів, дитячої порнографії, расизм, агресивні висловлювання, релігійні злочини, наклеп і фальшива інформація. У свою чергу, до злочинів, пов'язаних із правом власності в інформаційній сфері, слід віднести злочини проти авторських прав, торгівельних знаків, незаконні азартні ігри, спам і пов'язані з ним загрози. До злочинів, пов'язаних із комп'ютерами, дослідниками віднесено шахрайство і

комп'ютерне шахрайство, підробка з використанням комп'ютера, крадіжка ідентичності, неправильне використання пристроїв. Окремо наводиться група так званих комбінованих злочинів, до яких належать, наприклад, кібертероризм, інформаційна війна, відмивання грошей із використанням комп'ютерних технологій, фітинг [10].

Як бачимо, чимало злочинів, зокрема так званої загальнокримінальної спрямованості й тих, що пов'язані з інформаційним впливом або поряд з іншим посягають і на інформаційний простір тріади "особа-суспільство-держава", все одно залишаються поза межами цього своєрідного атласу, оскільки до уваги беруться лише діяння в кіберпросторі. До того ж перелічується чимало таких діянь, правова природа яких ще не має чіткого визначення (наприклад, фальшива інформація, інформаційна війна) або які на теперішній час не криміналізовані, хоча колись піддавалися захисту заходами кримінально-правового впливу (наприклад, наклеп). Водночас звернемо увагу на той факт, що запропонований підхід все ж таки можна визначити як спробу надання більш-менш систематизованого переліку діянь, що володіють ознакою суспільної небезпечності, посягаючи на інформаційний простір держави, суспільства та особи як такий.

У розвиток думки про суспільно небезпечні діяння, що реально існують, але ще не криміналізовані, окремо слід зупинитися на обговоренні ідеї про розробку і прийняття Закону України "Про протидію дезінформації", представленого, як вже зазначалося, Міністерством культури, молоді та спорту України. Уявляється, що на теперішній час протидія дезінформації – одна з ключових проблем убезпечення національного інформаційного простору від загроз в умовах ведення так званої гібридної війни проти нашої держави, низького рівня медіаграмотності українців та неможливості ідентифікувати особу, яка масово розповсюджує ту чи іншу дезінформацію. Так, на сьогодні чинним законодавством України не передбачено можливості звернення до правоохоронних органів і суду з приводу поширення дезінформації за відсутності особи, чиї права безпосередньо порушено. Не вдаючись до аналізу ідей, які запропоновано покласти в основу проєкту розглядуваного нормативного акта стосовно правових форм та організаційно-технічних методів ідентифікації осіб, що є поширювачами інформації, у тому числі й неправдивої, лише підкреслимо, що в чинному законодавстві України сьогодні відсутня відповідальність за масове поширення дезінформації в інформаційному просторі. Тому, враховуючи велику шкоду, що сягає рівня соціальної шкідливості або навіть суспільної небезпечності та може завдаватися такими діями одразу державі, суспільству та необмеженому колу осіб, є сенс встановлення, по-перше, адміністративної відповідальності за розповсюдження дезінформації, порушення правил спростування, надання відповіді та вимог прозорості, а по-друге, кримінальної відповідальності за систематичне умисне масове розповсюдження завідомо недостовірних повідомлень про факти, події або явища, що становить загрозу національній безпеці, громадській безпеці, територіальній цілісності, суверенітету, обороноздатності України, праву українського народу на самовизначення, життя та здоров'я громадян, стану довкілля у період відсутності повного контролю України за державним кордоном України. При цьому кваліфікуючими або особливо кваліфікуючими ознаками перелічених кримінально караних дій пропонується визнати їх вчинення з використанням комп'ютерних програм, призначених для автоматичного масового розповсюдження інформації (ботів), або спеціально організованої системи (групи) облікових записів, або користувачів інформаційних послуг, або засобів умисного фальшування (підробки) джерел інформації, а так само фінансування подібних

дій, вчинення їх повторно або організованою групою осіб, або якщо вони призвели до тяжких наслідків чи спричинили матеріальну шкоду у великому розмірі [11].

Надавши, але не вичерпавши доволі розлогу палітру правопорушень, що становлять безпосередню загрозу інформаційному простору, звернемося й до спроб розв'язати проблему створення оптимальної моделі захисту інформаційного простору за допомогою важелів кримінального права, що мали місце деякий час тому в національній площині. Так, ще наприкінці 2011 р. до Верховної Ради України було внесено проєкт Закону України "Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки" № 9575, що мав за мету вдосконалити систему юридичної відповідальності за правопорушення в сфері інформаційної безпеки. У цьому документі пропонувалося вилучити з КК України ст. 132 (Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби), ст. 145 (Незаконне розголошення лікарської таємниці), ст. 159 (Порушення таємниці голосування), ст. 163 (Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер), ст. 168 (Розголошення таємниці усиновлення (удочеріння)), ст. 182 (Порушення недоторканності приватного життя), ст. 231 (Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю), ст. 232 (Розголошення комерційної або банківської таємниці), ст. 328 (Розголошення державної таємниці), ст. 330 (Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни), ст. 376^1 (Незаконне втручання в роботу автоматизованої системи документообігу суду), ст. 381 (Розголошення відомостей про заходи безпеки щодо особи, взятої під захист), положення ст. 158 (Надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців) щодо втручання або інших несанкціонованих дій з базою даних та положення ст. 209^1 (Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму) у частині розголошення в будь-якому вигляді інформації, яка відповідно до закону надається спеціально уповноваженому центральному органу виконавчої влади зі спеціальним статусом із питань фінансового моніторингу, особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю, ст. 387 (Розголошення даних оперативно-розшукової діяльності, досудового розслідування), ч. 1 ст. 422 (Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості). Натомість, запропоновано узагальнити та включити вилучені статті й склади злочинів до розділу XVI Особливої частини КК України, при цьому замінивши назву розділу "Злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" на "Злочини у сфері інформаційної безпеки" [12].

На наш погляд, висловлена раніше позиція має рацію. Адже сфера інформаційної безпеки у широкому смислі слова виступає самостійним, дуже помітним об'єктом кримінально-правового захисту, який в умовах сьогодення потребує підвищеної уваги з огляду на необхідність забезпечення інформаційних відносин надійним захистом відповідного рівня та якості. Так, лише у 2019 р. за розділом XVI КК України зареєстровано 2088 злочинів. У свою чергу, за цей рік зафіксовано 210 випадків

порушення недоторканності приватного життя (ст. 182 КК України), що пов'язано зі збиранням, зберіганням, поширенням конфіденційної інформації про особу без її згоди або розголосом відомостей про особисту чи сімейну таємницю.

Повертаючись до структури КК України, зробимо висновок, що у чинному Кодексі з усього масиву злочинних діянь проти інформаційних відносин відповідного простору до Розділу XVI включені тільки ті з них, що пов'язані зі сферою кіберпростору (комп'ютерної інформації). Однак, на наш погляд, розмірковуючи над оптимальною моделлю захисту засобами кримінального права чисельних інформаційних відносин, що виникають й існують у суспільстві, треба виходити, по-перше, з акумуляції норм, що здійснюють захист усіх суб'єктів, яким може завдаватися шкода (особа, суспільство та держава) переважною більшістю відповідних злочинів, в одному розділі КК України, а, по-друге, доцільно вести мову не про захист інформаційних відносин у вузькому їх розумінні, а про захист інформаційного простору, під яким розуміється "інформаційне середовище, в якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання поширення, охорони та захисту інформації, інформаційних продуктів та інформаційних ресурсів" [7, с. 166]. Тобто йдеться про такий простір, що покликаний забезпечувати нормальну й безпечну інформаційну взаємодію між окремими особами, суспільством і державою у різних комбінаціях.

Таким чином, з урахуванням викладеної вище інформації та виходячи з наведеного розуміння інформаційного простору, вважаємо за доцільне здійснити оптимізацію кримінально-правового забезпечення охорони інформаційної безпеки України, насамперед змінивши назву розділу XVI Особливої частини КК України на таку: "Злочини проти інформаційної безпеки особи, суспільства, держави". При цьому до єдиного розділу кодексу слід віднести, по-перше, всі так звані комп'ютерні злочини, що містяться у теперішньому розділі XVI Особливої частини КК України (статті 361, 361^1, 361^2, 362, 363, 363^1), та злочини, пов'язані із внесенням неправдивих відомостей або будь-яким втручанням у роботу баз даних державних реєстрів (ст. 158 КК України (Надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців) у частині умисного внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованих дій з інформацією, що міститься в базі даних Державного реєстру виборців, чи іншого несанкціонованого втручання в роботу бази даних Державного реєстру виборців; ст. 376^1 (Незаконне втручання в роботу автоматизованої системи документообігу суду).

По-друге, до цього ж самого Розділу логічно перемістити склади злочинів, що на теперішній час містяться в інших розділах КК України, але стосуються однієї специфічної площини протиправної діяльності, а саме протиправних діянь щодо комерційної, банківської та різних видів професійної таємниці, а так само діянь щодо таємниці волевиявлення. З огляду на поняття комерційної таємниці, що наводиться у ст. 505 Цивільного кодексу України, та банківської таємниці, про яку йдеться у ст. 60 Закону України "Про банки і банківську діяльність", до запропонованого розділу необхідно віднести склади злочинів, передбачені статтями 231 (Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю), 232 (Розголошення комерційної або банківської таємниці), 232^1 (Незаконне використання інсайдерської інформації). Близькою до цієї групи злочинів є й приховування інформації про діяльність емітента (ст. 232^2).

Що стосується професійної таємниці, під якою розуміється інформація з обмеженим доступом, яка стала відомою або доступною представнику певної професії у зв'язку з виконанням професійних або поряд з ними службових чи процесуальних обов'язків, незаконне розголошення або використання якої завдає шкоди інформаційній безпеці особи, суспільства чи держави [13, с. 6], то до цього розділу доцільно перемістити такі склади злочинів, що передбачені статтями 132 (Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби), 145 (Незаконне розголошення лікарської таємниці), 168 (у частині розголошення таємниці усиновлення (удочеріння) службовою особою або працівником медичного закладу, яким відомості про усиновлення (удочеріння) стали відомі по службі чи по роботі), 209^1 (Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму (у частині розголошення інформації з питань фінансового моніторингу особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю), 330 (Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни), 381 (Розголошення відомостей про заходи безпеки щодо особи, взятої під захист), 387 (Розголошення даних оперативно-розшукової діяльності, досудового розслідування). У свою чергу, порушення таємниці волевиявлення особи може полягати у здійсненні дій, передбачених ст. 159 (Порушення таємниці голосування).

По-третє, логічним так само уявляється включення до розділу "Злочини проти інформаційної безпеки особи, суспільства, держави" складів злочинів, пов'язаних із порушенням державної таємниці, а саме: статті 328 (Розголошення державної таємниці), 329 (Втрата документів, що містять державну таємницю), 422 (Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості). Об'єктом перелічених злочинів виступають суспільні відносини з охорони державної таємниці в різних сферах діяльності держави, що можна охарактеризувати як відносини інформаційної безпеки [8, с. 689].

По-четверте, злочинами, що фактично порушують право особи на власну інформаційну безпеку приватного життя, положення про яку чітко сформульовані у статтях 31 і 32 Конституції України, слід вважати порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163) та порушення недоторканності приватного життя (ст. 182). Отже, ці склади кримінально караних правопорушень так само доцільно перемістити до єдиного розділу КК України, про який йдеться.

По-п'яте, вважати злочинами, що, у тому числі, порушують порядок циркуляції певної інформації й у такий спосіб посягають на упорядкованість інформаційного простору, пов'язаного з належною реалізацією та правовим забезпеченням авторського права й права на інтелектуальну власність, доцільно й діяння, передбачені статтями 176 (Порушення авторського права і суміжних прав) і 177 (Порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію).

По-шосте, велику шкоду суспільним відносинам у сфері інформаційного простору завдають злочини, пов'язані з пропагандою, у тому числі в засобах масової інформації, культу насильства і жорстокості, расової, національної чи релігійної нетерпимості та дискримінації (ст. 300), а так само з поширенням порнографії (ст. 301). Наприклад, лише у 2019 р. за ст. 301 КК в Україні було зареєстровано 1012 злочинів. Ці діяння, посягаючи

на засади суспільної моральності в сфері духовного й культурного життя, безумовно, зачіпають і безпеку сфери інформаційного простору, завдаючи учасникам (суб'єктам) цієї сфери неабиякої шкоди. Включення цієї групи злочинів до єдиного розділу під назвою "Злочини проти інформаційної безпеки особи, суспільства, держави", напевно, викликатиме чимало заперечень. Однак як робочу гіпотезу варіант з їх віднесенням до знов створеного розділу, на нашу думку, не слід беззаперечно відкидати.

По-сьоме, у порядку *de lege ferenda* до єдиного Розділу "Злочини проти інформаційної безпеки особи, суспільства, держави" слід внести злочин або злочини, пов'язані з поширенням дезінформації (звісно ж, якщо буде прийнятий Закон України "Про протидію дезінформації").

Що стосується техніки об'єднання перелічених кримінально караних правопорушень в єдиному розділі Кодексу, то це можна зробити шляхом виключення відповідних статей із тих розділів, в яких вони знаходяться зараз, та присвоєння їм нової нумерації в тому "базовому" розділі, до якого планується їх перенести. У майбутньому ж Кримінальному кодексі, робота над яким активно триває у цей час, висловлена пропозиція у технічному плані не викликатиме жодних перешкод, оскільки всім статтям буде присвоєна нова нумерація. Єдине, на що треба звернути у майбутньому увагу: чи будуть ті або інші правопорушення віднесені до злочинів або до кримінальних проступків. Від цього залежатиме їх знаходження чи то в Кримінальному кодексі України, чи то у Кодексі про кримінальні правопорушення України.

Інформаційна безпека особи, суспільства та держави так само може потерпати ще від цілої низки злочинів. Йдеться принаймні про злочини, передбачені статтями 109 (Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади), 110 (Посягання на територіальну цілісність і недоторканність України), 111 (Державна зрада) та 114 (Шпигунство) КК України. На теперішній час перелічені злочини охоплюються розділом I Особливої частини КК України, що має назву "Злочини проти основ національної безпеки України". На наш погляд, ці склади злочинів потребують особливого виокремлення в самостійному розділі законодавства про кримінальну відповідальність, адже вони посягають на ті, так би мовити, фундаментальні суспільні відносини, що забезпечують існування й розвиток України як суверенної, незалежної, демократичної, соціальної й правової держави на сучасній політичній карті світу.

Висновки.

Теоретичне дослідження питань захисту інформаційного простору Української держави дозволяє стверджувати, що особливістю нинішньої моделі захисту інформаційних відносин засобами кримінального права є те, що відповідні норми містяться в різних розділах Особливої частини КК України. Принаймні можна виділити сім блоків правопорушень (з урахуванням злочинів проти основ національної безпеки України), що так чи інакше безпосередньо можуть завдавати шкоду цій сфері життєдіяльності суспільства. У цьому вбачається деяка штучність законодавчого підходу до захисту єдиного інформаційного простору та виникнення джерела нескінченної дискусії про первинність захисту відповідними нормами чи то кіберпростору, чи то простору, яким, окрім кіберпростору, охоплюються ще й інші площини інформаційного комунікування різноманітних суб'єктів (соціальних інституцій та їх представників, окремих осіб, великих колективів або навіть народів).

Ефективна модель захисту інформаційних відносин, що існують у суспільстві, засобами кримінального права, передбачає насамперед акумуляцію норм, що

здійснюють захист всіх суб'єктів, яким може завдаватися шкода (особа, суспільство та держава) переважною більшістю відповідних злочинів, в єдиному розділі КК України.

Водночас має йтися не про захист інформаційних відносин у вузькому їх розумінні, а про захист саме інформаційного простору як специфічного середовища, яке пов'язане з протіканням різноманітних інформаційних процесів із приводу створення, обігу інформації та захисту як самої інформації у будь-якій з її форм, інформаційних продуктів і послуг, так й інструментів її циркуляції у суспільстві. Такий хід міркувань зумовлює створення об'єднаної "платформи" захисту відповідних суспільних відносин у вигляді єдиного розділу Особливої частини КК України.

Використана література

1. Тарасюк А.В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право.* № 4(31)/2019. С. 73-82.

2. Писаренко Г.М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2016. Вип. 36. Т. 2. С. 55-58.

3. Про основи національної безпеки України: Закон України від 19.06.03 р. № 964-IV. *Відомості Верховної Ради України.* 2003. № 39. Ст. 351.

4. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241.

5. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287/2015. *Офіційний вісник Президента України*. 2015 р. № 13. Ст. 874.

6. Міністр культури презентував законопроект про протидію дезінформації. URL: https://www.sud.ua/ru/news/publication/159088-ministr-kulturi-prezentuvav-zakonoproyekt-pro-protidiyu-dezinformatsiyi (дата звернення 18.02.2020).

7. Попова Т.В., Ліпкан В.А. Стратегічні комунікації (словник); за ред. В.А. Ліпкана. Київ: ФОПС. Ліпкан, 2016. 416 с.

8. Кримінальний кодекс України: науково-практичний коментар. Особлива частина. У 2 т. Т. 2. 5-те вид., доп.; за ред. В.Я. Тація, В.П. Пшонки, В.І. Борисова, В.І. Тютюгіна. Ю.В. Баулін. Харків: Право, 2013. 1040 с.

9. Про кіберзлочинність: Конвенція Ради Європи від 23 листопада 2001 року. ETS № 185. *Офіційний вісник України.* 2007. № 65. Ст. 2535.

10. Юрченко А.В., Дудченко А.Д. Security Management for Business. Тема № 10 (2015).pdf. – (Презентація). URL: http://www.myshared.ru/slide/980543 (дата звернення 22.02.2020).

11. Про протидію дезінформації. – (Презентація законопроекту). URL: https://www.mkms.gov. ua/files/InformPolityka.pdf (дата звернення 18.02.2020).

12. Пояснювальна записка до проекту Закону України "Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки". URL: http://www.search.ligazakon.ua/l_doc2.nsf/link1/GF7DZ00A.html (дата звернення 06.02.2020).

13. Резнікова Г.І. Криміналістична характеристика злочинів щодо розголошення професійних таємниць: автореф. дис. …канд. юрид. наук: 12.00.09. – (Нац. юрид. ун-т імені Ярослава Мудрого). Харків, 2015. 20 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~