УДК 342.9
DOI https://doi.org/10.32782/1813-338X-2021.4.33

О. О. Кабиш
аспірант
Науково-дослідного інституту публічного права

СТАН ДОСЛІДЖЕННЯ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Актуальність статті полягає в тому, що на тлі розвитку комп'ютерів та цифрової революції в цілому, з'являються окремі особи та групи, що намагаються за допомогою новітніх технічних інструментів порушити права та свободи інших людей шляхом: незаконного заволодіння їх особистими даними; викрадення грошових коштів, які знаходяться на електронних рахунках; втягнення людей у різноманітні шахрайські схеми, наприклад, пов'язані із продажом неіснуючих товарів і таке інше. Мета статті полягає у наданні оцінці стану дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності. У статті здійснено аналіз теоретичних здобутків науковців – представників різних галузей права, які у своїх роботах досліджували різні теоретичні аспекти протидії кіберзлочинності в Україні. Доведено, що чітко сформульованого підходу до розкриття та оцінки правового регулювання взаємодії суб'єктів протидії кіберзлочинності на сьогодні немає. Констатовано необхідність проведення подальшого, більш глибокого та ширшого дослідження у вказаній сфері. Зроблено висновок, що незважаючи на чималу кількість наукових робіт, чітко сформульованого підходу до розкриття та оцінки правового регулювання взаємодії суб'єктів протидії кіберзлочинності на сьогодні немає. Поверхнево вказане питання розглядалось в межах багатьох галузевих наук. Так, представники кримінального права та кримінології акцентують увагу лише на тому, що взаємодія є необхідним організаційним заходом подолання негативного явища кіберзлочинності. В свою чергу представники кримінального процесуального права та криміналістики обмежують свої дослідження виключено рамками існуючих процесуальних механізмів та порядком здійснення відповідних слідчих дій та заходів, вважаючи взаємодію виключно моделлю розвитку процесуальних відносин. Міжнародники переймаються лише світовою співпрацею в сфері боротьби з кіберзлочинами та її юридичним оформленням. Теоретики права розглядають взаємодію у контексті дослідження і розкриття особливостей змісту кіберзлочинності загалом і таке інше. Ні в якому разі не можна применшувати значення згаданих в статті наукових робіт. Проте, відсутність єдиного сформульованого комплексного бачення природи, змісту, особливостей організації, векторів здійснення та інших аспектів правового регулювання взаємодії суб'єктів протидії кіберзлочинності, ускладнює вироблення її нової концепції та визначення напрямів удосконалення.

Ключові слова: *кіберзлочинність, протидія кіберзлочинності, взаємодія, наукові розробки, стан дослідження проблеми.*

Постановка проблеми. Якщо у XX столітті цифрові технології лише почали своє зародження та розповсюдження на всі сфери життєдіяльності людства, то у XXI кожен з нас не може уявити свій день без використання електронного гаджету підключеного до всесвітньої мережі Інтернет. Дана ситуація має дві сторони. З одного боку, технології суттєво полегшують життя суспільства, адже надають більш широкі можливості у процесі віддаленої комунікації різноманітних суб'єктів, соціального управління, автоматизації певних функціональних процесів виробничого характеру і таке інше. Разом із тим, на тлі розвитку комп'ютерів та цифрової революції в цілому, з'являються окремі особи та групи, що намагаються за допомогою новітніх технічних інструментів порушити права та свободи інших людей шляхом: незаконного заволодіння їх особистими даними; викрадення грошових коштів, які знаходяться на електронних рахунках; втягнення людей у різноманітні шахрайські схеми, наприклад, пов'язані

із продажом неіснуючих товарів і таке інше. Все перелічене в сукупності сформувало серйозну проблему кіберзлочинності, яка постійно перебуває у полі зору правоохоронних органів та міжнародної спільноти.

Стан дослідження проблеми. В останні роки проблема кіберзлочинності набуває все більшої актуальності, що обумовлює високий рівень зацікавленості до неї з боку науковців. Так, даному питанню приділяли увагу: Ю.М. Бтурін, С.А. Буяджи, В.Б. Дзюндзюк, І.М. Забара, А.С. Мацко, О.О. Мережко, А.В. Пазюк, В.В. Сабадаш та багато інших. Вказані вище науковці досить ґрунтовно дослідили поняття, зміст, особливості кіберзлочинності, засади та процедури протидії цьому явищу, специфіку міжнародного співробітництва в даній сфері, тощо. Втім, незважаючи на це, поза увагою вчених залишилось багато інших проблемних питань взаємодії суб'єктів протидії кіберзлочинності.

Саме тому мета статті полягає у тому, щоб надати оцінку стану дослідження проблеми правового регулювання взаємодії суб'єктів протидії кіберзлочинності.

Виклад основного матеріалу. Кіберзлочинність в цілому, як самостійна сфера суспільних відносин та деструктивний соціальний інститут, неодноразово ставала предметом комплексних вчених робіт. Наприклад, В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко, М.Я. Швець, Р.А. Калюжний та П.В. Мельник розглянули проблему кіберзлочинів через призму інформаційного права та механізмів забезпечення безпеки інформації. В роботі науковців наголошується, що масове впровадження нових технічних засобів, на основі яких здійснюється інформатизація у всьому світі, робить прозорими державні кордони і формує нові геополітичні парадигми у розумінні глобальних соці-технічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угрупованнями. Електронно-комунікаційна інфраструктура, як і інші інформаційні ресурси, стає об'єктом міждержавної боротьби за світове лідерство або об'єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносин. На думку вчених, ключове значення у механізмі організації безпеки інформації становить організація законного використання комп'ютерних систем, що попередить користування ними не за цільовим призначенням та порушення за допомогою них існуючих соціальних та політичних засад. Враховуючи викладене вчені пишуть: «Загальний аналіз проблем організовування захисту інформації в автоматизованих комп'ютерних системах дає можливість визначити три агреговані організаційні моделі заходів: 1) організація запобіжних заходів; 2) організація блокування (протидії) реальним загрозам, що реалізуються; 3) організація подолання наслідків загроз, які не вдалося блокувати або запобігти їм». Крім того науковці доводять, що в основі організації захисту інформації та протидії порушенням, знаходиться тісна модель співпраці одночасно представників як публічної влади, так і приватного сектору і, навіть, окремих громадян» [1].

Різноманітні аспекти змісту кіберзлочинності, а також взаємодії суб'єктів протидії цьому негативному явищу розкривались в рамках монографій та дисертацій у царині різних юридичний галузей. Так, Д.С. Азаров присвятив своє кримінально-правове дослідження встановленню сутності злочинів у сфері комп'ютерної інформації. В його монографії досліджуються проблеми кримінальної відповідальності за злочини у сфері комп'ютерної інформації, пов'язані зі ступенем і характером суспільної небезпеки цих посягань та їх міжнародним характером, ознаками складів цих злочинів, а також санкціями, передбаченими за їх вчинення. Узагальнюється зарубіжний та міжнародний досвід кримінально-правової протидії «комп'ютерним» злочинам. Вченим розроблено доктринальна модель системи норм про кримінальну відповідальність за аналізовані злочини, для втілення якої пропонується проект Закону України «Про внесення змін і доповнень до Кримінального кодексу України щодо відповідальності за злочини у сфері комп'ютерної інформації» [2].

З точки зору кримінального процесу та криміналістики протидію кіберзлочинності та взаємодію в рамках даного питання дослідила Л.В. Борисова у дисертації: «Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження». Мета дослідження полягала в тому, щоб на основі сучасних концепцій науки криміналістики розробити тактичні й процесуальні основи криміналістичного дослідження транснаціональних комп'ютерних злочинів. Для досягнення поставленої мети було сформульовано такі взаємопов'язані між собою завдання: 1) розкрити поняття комп'ютерної інформації як предмета правового захисту та визначити криміналістично значущі вихідні дані про транснаціо-

нальні комп'ютерні злочини; 2) визначити зміст поняття «транснаціональний комп'ютерний злочин»; 3) розкрити сутність основних елементів криміналістичної характеристики транснаціональних комп'ютерних злочинів та взаємозв'язків між ними; 4) типізувати слідчі ситуації початкового етапу розслідування транснаціональних комп'ютерних злочинів; 5) розкрити особливості виявлення і закріплення слідів транснаціональних комп'ютерних злочинів; 6) охарактеризувати місце та особливості застосування спеціальних знань у ході розслідування транснаціональних комп'ютерних злочинів; 7) розробити систему рекомендацій, спрямованих на запобігання, протидії та розслідування транснаціональних комп'ютерних злочинів [3, с.9].

Цікавою є праця С.А. Буяджи, який розглянув правове регулювання боротьби з кіберзлочинністю у теоретико-правовому аспекті. Його робота націлювалась на розробку концептуального розуміння специфіки генезису та тенденцій розвитку і механізму правового регулювання боротьби із кіберзлочинністю. Для досягнення зазначеної мети вчений поставив такі задачі: 1) визначити правову природу боротьби із кіберзлочинністю; 2) дослідити генезис правового регулювання боротьби із кіберзлочинністю; 3) охарактеризувати структуру механізму правового регулювання боротьби з кіберзлочинністю; 4) розкрити та конкретизувати досвід міжнародно-правового регулювання боротьби з кіберзлочинністю; 5) з'ясувати специфіку національного правового регулювання боротьби з кіберзлочинністю; 6) виокремити тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні; 7) виділити особливості правового регулювання боротьби з кіберзлочинністю у зарубіжних країнах. Окрім цього, в дисертації науковець детально проаналізував особливості міжнародного співробітництва в сфері боротьби з кіберзлочинністю, визначивши, що остання здійснюється в наступних напрямках: 1) прийняття міжнародно-правових механізмів регулювання та взаємодії правоохоронних органів у питаннях боротьби із кіберзлочинністю; 2) гармонізація національних законодавств із міжнародним законодавством; 3) безпосередня співпраця, як офіційна, так і неофіційна; 4) узгодження повноважень при здійсненні боротьби із кіберзлочинністю [4].

Варто наголосити, що переважна більшість наукових опрацювань питання взаємодії суб'єктів протидії кіберзлочинності та правового регулювання даної проблеми, проводились у форматі наукових статей. Багато подібних робіт написано теоретиками міжнародного права. Так, А.В. Войціховський відмічає: широке використання сучасних інформаційних технологій у державних і недержавних структурах, а також у суспільстві в цілому висуває вирішення проблем інформаційної безпеки в число основних. Окрім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Актуальність даної теми праці вказаного науковця обумовлена саме тим, що зростання інформаційних технологій зумовлює не тільки прогресивні зміни в економіці, але й негативні тенденції розвитку злочинного світу, появу нових форм і видів злочинних посягань. Це виявляється в тім, що зловмисники активно використовують у своїй злочинній діяльності новітні комп'ютерні засоби і нові інформаційні технології. Розповсюдження комп'ютерних вірусів і дитячої порнографії, шахрайство з пластиковими платіжними картками, розкрадання грошових коштів з банківських рахунків, комп'ютерний тероризм – це далеко не повний перелік злочинів, сукупність яких отримала широковживану назву «кіберзлочинність». Метою його статті стало комплексне вивчення проблем, пов'язаних із міжнародною співпрацею правоохоронних органів у боротьбі з кіберзлочинністю і на базі цього розроблення пропозицій щодо підвищення ефективності протистояння даним злочинам [5, с.107].

В.В. Марковим досліджено особливості злочинів у сфері інформаційно-телекомунікаційних технологій, звертається увага на основні проблеми щодо їх виявлення, розкриття та розслідування. Висвітлено напрямки міжнародної взаємодії у сфері протидії кіберзлочинності, що базуються на міжнародних нормативно-правових актах. Наголошено на необхідності вивчення досвіду зарубіжних країн щодо організації діяльності підрозділів боротьби з кіберзлочинністю. Проаналізовано досвід діяльності поліції Канади в цьому напрямку. Виділено рівні взаємодії оперативних нашої держави з метою оперативного документування злочинів у сфері інформаційно-телекомунікаційних технологій та види їх співробітництва з правоохоронними органами інших держав. В статті науковця зауважено, що удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуван-

ням національних особливостей на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн [6].

У статті М.Ю. Якимчук розглянуто основні аспекти правового регулювання кіберзлочинності в національному праві через призму міжнародного. Наголошено, що у сучасному світі країни розробляють нові методи боротьби з такими злочинами. Зазначено: «США сформувала так звані «NIST Cyber security Framework» – стандарти з безпеки, які дозволяють виявляти, реагувати і навіть запобігати кіберзлочинам, а також Акт про повідомлення щодо порушення правил безпеки «Notice of Security Breach Act», згідно з яким компанії мають право вільно вибрати для себе спосіб забезпечення приватності своїх систем; Європейський Союз прийняв Директиву щодо мережевої та інформаційної безпеки «NIS Directive on security of network and information systems», що визначив важливе значення надійності й безпеки мережевих та інформаційних систем для економічної та суспільної діяльності; Україна створила підрозділ «CERT-UA», який у межах своїх повноважень проводить аналіз та накопичення даних про кіберінциденти, веде державний їх реєстр» [7].

Висновки. Отже, спираючись на проведений у статті аналіз можемо стверджувати, що, незважаючи на чималу кількість наукових робіт, чітко сформульованого підходу до розкриття та оцінки правового регулювання взаємодії суб'єктів протидії кіберзлочинності на сьогодні немає. Поверхнево вказане питання розглядалось в межах багатьох галузевих наук. Так, представники кримінального права та кримінології акцентують увагу лише на тому, що взаємодія є необхідним організаційним заходом подолання негативного явища кіберзлочинності. В свою чергу представники кримінального процесуального права та криміналістики обмежують свої дослідження виключено рамками існуючих процесуальних механізмів та порядком здійснення відповідних слідчих дій та заходів, вважаючи взаємодію виключно моделлю розвитку процесуальних відносин. Міжнародники переймаються лише світовою співпрацею в сфері боротьби з кіберзлочинами та її юридичним оформленням. Теоретики права розглядають взаємодію у контексті дослідження і розкриття особливостей змісту кіберзлочинності загалом і таке інше. Ні в якому разі не можна применшувати значення згаданих в статті наукових робіт. Проте, відсутність єдиного сформульованого комплексного бачення природи, змісту, особливостей організації, векторів здійснення та інших аспектів правового регулювання взаємодії суб'єктів протидії кіберзлочинності, ускладнює вироблення її нової концепції та визначення напрямів удосконалення.

Список використаної літератури:

1. Основи інформаційного права України: Навч. посіб. В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін.; За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. К.: Знання, 2004. 274 с.
2. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): монографія. Київ: Атіка, 2007. 304 с.
3. Борисова Л.В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження: дисертація. Київ: Київський національний університет внутрішніх справ. 2007. 217 с.
4. Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект: дисертація. Київ: ПВНЗ Університет Короля Данила. 2018. 203 с.
5. Войциховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека 2011. №4(41). С.107-112.
6. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. Право і безпека. 2015. №2(57). С.107-113.
7. Якимчук М.Ю. Особливості правового регулювання протидії кіберзлочинності в Україні: порівняльно-правовий аспект. Нове українське право. 2021. Вип.4. С.182-186.

Kabysh O. O. The state of research on the problem of legal regulation of the interaction of actors in the fight against cybercrime

The relevance of the article lies in the fact that against the background of the development of computers and the digital revolution in general, there are individuals and groups that try to use the latest technical tools to violate the rights and freedoms of other people by: illegally taking possession of their personal data; theft of funds that are in electronic accounts; involving people in various fraudulent schemes, for example, related to the sale of non-existent goods and so on. The purpose of the article is to provide an assessment of the state of research on the problem of legal regulation of the interaction of actors in the fight against cybercrime. The article analyzes the theoretical achievements of scientists - representatives of various branches of law, who in their works investigated various theoretical aspects of countering cybercrime in Ukraine. It has been

proven that there is currently no clearly formulated approach to the disclosure and assessment of legal regulation of the interaction of cybercrime combating entities. The need for further, more in-depth and broader research in the specified area was established. It was concluded that despite a considerable number of scientific works, there is currently no clearly formulated approach to the disclosure and evaluation of the legal regulation of the interaction of actors in the fight against cybercrime. The superficially indicated question was considered within the limits of many branches of science. Thus, representatives of criminal law and criminology emphasize only that interaction is a necessary organizational measure to overcome the negative phenomenon of cybercrime. In turn, representatives of criminal procedural law and criminology limit their research exclusively to the framework of existing procedural mechanisms and the order of implementation of relevant investigative actions and measures, considering interaction exclusively as a model of the development of procedural relations. Internationalists are concerned only with global cooperation in the field of combating cybercrime and its legal implementation. Legal theorists consider the interaction in the context of research and disclosure of the specifics of the content of cybercrime in general and so on. In no case should one belittle the significance of the scientific works mentioned in the article. However, the lack of a single formulated comprehensive vision of the nature, content, features of the organization, vectors of implementation and other aspects of legal regulation of the interaction of subjects in the fight against cybercrime complicates the development of its new concept and the determination of improvement directions.

Key words: *cybercrime, combating cybercrime, interaction, scientific developments, the state of problem research.*