points of interaction and third-party suppliers and buyers, it can be difficult to monitor whether all parties are following proper cybersecurity protocols. Therefore, in today's business environment, cyber security is becoming an integral part of supply chain management. This involves a thorough analysis of potential risks created by external suppliers, buyers and other market participants, logistics and transportation, with further preventive measures to reduce them. Any supply chain is only as strong as its weakest link. Therefore, cyber security measures are mainly aimed at identifying vulnerabilities and eliminating cyber threats in the weakest links of the supply chain.

The article deals with the essence of supply chain management and analyzes the role of cyber security in the management system. It is noted, that in modern conditions, cyber security is becoming an element of supply chain management. The main types of risks and cyber threats in supply chains are analyzed, in particular the issue of security of third-party suppliers. Measures to eliminate cyber risks and to increase cyber security in supply chain management are proposed. By taking a proactive approach and implementing strong cybersecurity measures, companies can reduce the risk of cyberattacks and ensure the security of their supply chain.

Keywords: *supply chains, cyber security, information flows, counterparties, cyber threats.*

УДК 342
DOI: 10.31733/2078-3566-2022-6-542-547

Влада ЛІТОШКО©
викладач

Каріне МКРТЧЯН©
викладач

ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ОСНОВ СПІВПРАЦІ ДЕРЖАВ З ПРОТИДІЇ ПРАВОПОРУШЕННЯМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

Правопорушення у сфері інформаційних технологій становлять реальну загрозу суспільним відносинам на внутрішньодержавному рівні та міжнародному правопорядку. Проблема протидії правопорушенням у сфері інформаційних технологій неодноразово розглядалася в документах регіональних міжнародних організацій. Оскільки кожен регіональний правовий режим є унікальним і має свої особливості, у статті розглядаються можливі наслідки такої регіоналізації. На основі проведеного дослідження зроблено висновок, що регіоналізація міжнародно-правової взаємодії у боротьбі забезпечення кібербезпеки має свої позитивні і негативні сторони та призвела до ситуації, яка частково може бути пояснена транснаціональним характером правопорушень у цій сфері.

Ключові слова**:** *протидія правопорушенням, міжнародна співпраця, правопорушення у сфері інформаційних технологій, інформаційна безпека, кібербезпека*.

© В. Літошко, 2022
ORCID iD: https://orcid.org/0000-0001-5712-6841
Vlada_lit@ukr.net

© К. Мкртчян, 2022
ORCID iD: https://orcid.org/0000-0002-6554-3917
karina19_7777@ukr.net

Постановка проблеми. Незважаючи на значущість співпраці із протидії правопорушенням у сфері інформаційних технологій, нині державам не вдалося виробити узгоджені підходи та укласти відповідний міжнародний договір під егідою Організації Об'єднаних Націй. Регіональне міжнародно-правове регулювання, у свою чергу, характеризується фрагментарністю і розрізненістю. Зазначене знижує ефективність міждержавної взаємодії та актуалізує необхідність аналізу міжнародно-правових засад протидії правопорушенням у сфері інформаційних технологій.

Вказане зумовлює необхідність дослідження теоретико-правових аспектів сучасного стану міжнародно-правового співробітництва з протидії правопорушенням у сфері інформаційних технологій та перспективних напрямів розвитку багаторівневої взаємодії держав із забезпечення кібербезпеки. Міжнародне співробітництво з протидії правопорушенням у сфері інформаційних технологій є актуальним для України, що активно виступає за зміцнення міждержавної взаємодії в цій галузі.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Окремі аспекти кібербезпеки все частіше актуалізуються у дослідженнях українських науковців. Теоретичним основам протидії правопорушенням у сфері інформаційних технологій у сучасному світі приділили увагу С. Гнатюк, В. Ліпкан, І. Сопілко, О. Довгань. Аналіз положень законодавства у сфері інформації та кібербезпеки з погляду кримінального права та адміністративного права знайшов відображення у роботах І. Дороніна, І. Діордіца. Вчені Н. Ткачук, М. Гуцалюк, та К. Галінська присвятили свої публікації питанню кібербезпеки як стратегії національного інформаційного правопорядку. Однак, констатуючи значний науковий внесок учених, зазначимо, що в умовах стрімкого розвитку громадянського суспільства, правової держави та технологій, окремі аспекти цієї теми потребують уваги.

Метою статті є дослідження теоретико-правових аспектів сучасного стану міжнародно-правового співробітництва із протидії правопорушенням у сфері інформаційних технологій та перспективних напрямів розвитку багаторівневої взаємодії держав із забезпечення кібербезпеки.

Виклад основного матеріалу. Правопорушення у сфері інформаційних технологій (Далі – ІТ) є однією з найбільш швидко зростаючих та руйнівних загроз. Зокрема, нагальною є гармонізація законодавства, як матеріального та процесуального, а також налагодження взаємної між державами у цій сфері.

Розвиток ІТ у сучасному сіті є настільки стрімким, що уряди держав часто не встигають адаптувати національне законодавство до всіх змін. Крім того, учені акцентують на тому, що правопорушення у сфері ІТ мають тенденцію до транснаціонального характеру і тому потребують підтримання всебічної міжнародно-правої співпраці для його припинення [1].

Проте, незважаючи на те що держави та міжурядові організації визнають транснаціональний характер досліджуваних правопорушень, є полеміка щодо необхідності укладання відповідного договору універсального характеру. Так, різні підходи до встановлення протиправності поведінки в кіберпросторі можуть перешкодити ефективному співробітництву компетентних органів і, як наслідок, протидії деліктам у сфері ІТ [2, 3].

До міжнародно-правових актів, що безпосередньо регламентують правопорушення у сфері ІТ, належать, зокрема: Конвенція Ради Європи про кіберзлочинність (2001) [4], Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав (2010) [5], Африканська конвенція про кібербезпеку та захист персональних даних (2014) [6]. Зазначимо також, що деякі міжнародні договори, що регулюють міжнародне співробітництво в боротьбі з іншими видами правопорушень, можуть бути застосовні до такої категорії справ.

Наприклад, Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності (2000) [7] і Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії (2000) [8] можуть стати основою для міжнародного співробітництва, коли вчинене правопорушення підпадає під дію цих договорів.

Конвенція ООН проти транснаціональної організованої злочинності (2000) може застосовуватися у випадку вчинення правопорушення у сфері ІТ, якщо останнє має транснаціональний характер і вчинено організованою групою осіб (пункт "b", частини 1, статті 3 Конвенції) [7]. Факультативний протокол може бути застосований до

виробництва, поширення, поширення, імпорту, експорту, пропозиції, продажу або зберігання дитячої порнографії, коли ці дії здійснюються онлайн (пункт c, частини 1, статті 3 Протоколу) [8].

Вищезазначені договори створюють правову основу для гармонізації законодавства та взаємодії правоохоронних органів та судів у досліджуваній сфері. Утім, вважаємо, що наведеної правової бази недостатньо для створення комплексного та надійного механізму боротьби з правопорушеннями у сфері ІТ. Механізму, який вимагає налагодження системи взаємної допомоги для забезпечення заходів впливу щодо осіб, що вчиняють транснаціональні правопорушення у сфері ІТ.

Крім того, підвищений інтерес вчених-міжнародників викликають питання забезпечення інформаційної безпеки як елементу міжнародної безпеки в рамках регіональних угод. Так, зауважимо, що регіональні угоди створюють правові режими, що в окремих випадках можуть стати підставою виникнення юридичних колізій, призвести до суперечливої судової практики і надати укриття правопорушникам.

Вважаємо, що окрему увагу доцільно приділити Конвенції Ради Європи про кіберзлочинність (2001) та іншим регіональним конвенціям, заснованим на її положеннях. Конвенція вважається найбільш детальним і прогресивним договором у цій сфері, що передбачає гармонізацію законодавства в аспекті захисту прав людини, боротьби з кіберзлочинністю, юрисдикції та взаємної правової допомоги.

На думку делегатів Конгресу із запобігання злочинності та кримінального правосуддя під егідою ООН, Конвенція Ради Європи могла б стати універсальною правовою базою для міжнародно-правового співробітництва у боротьбі з кіберзлочинністю. Проте деякі держави стверджували, що конвенція містить положення, які могли становити загрозу суверенітету та національній безпеці (зокрема, це стосувалося статті 32 (b) Конвенції, яка присвячена транскордонному доступу до комп'ютерної інформації) [9].

Механізм приєднання до Конвенції РЄ про кіберзлочинність досить складний для держав, які не є членами РЄ. Відповідно до ст. 37 держава-кандидат, яка прагне приєднатися до конвенції, повинна отримати одностайну згоду держав-учасниць конвенції та згоду Комітету міністрів Ради Європи. Остаточне рішення держави-учасниці з цього питання не повинно підтверджуватися жодними аргументами [4]. Тож, незважаючи на те, що кількість держав-учасниць Конвенції РЄ про кіберзлочинність, які не є членами РЄ, зросла за останні п'ять років, було б недоцільно стверджувати, що Конвенція може бути універсальною правовою базою для боротьби з правопорушеннями.

Конвенція про кіберзлочинність була укладена в 2001 році і, отже, не врахувала всі сучасні тенденції правопорушень у сфері ІТ. У зв'язку з цим Конвенційний комітет (T-CY) видає рекомендації, спрямовані на сприяння ефективному використанню та реалізації Конвенції в світлі правових, політичних і технологічних розробок [10]. Незважаючи на позитивні результати, досягнуті щодо тлумачення Конвенції Ради Європи, окремі тенденції потребують вирішення лише за допомогою спеціального правового інструменту. Зокрема, існує широко поширена практика використання хмарних обчислень для комерційних і приватних цілей, що створює нові проблеми для збору електронних доказів. Тож у 2017 році держави-учасниці Конвенції погодилися розпочати підготовку протоколу до неї, щоб допомогти правоохоронним органам зберігати докази на іноземних серверах кількох юрисдикцій [11].

Зазначимо також про Конвенцію про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав (2010), зміст якої в основному було розроблено на основі вищезгаданої Конвенції Ради Європи. Примітно, що Конвенція надає перелік правопорушень, однак вимагає від держав-учасниць криміналізувати певну поведінку без пояснення об'єктивних причин (ст. 14–15 Конвенції, яка передбачає «інші злочини, пов'язані з порнографією» та «порушення приватного життя за допомогою ІТ») [5]. Важливо, що положення Конвенції закріплюють важливі правові аспекти щодо взаємної правової допомоги. Зокрема, взаємна правова допомога надається лише на підставі запиту, надісланого одним центральним органом безпосередньо до іншого. У свою чергу, держава-учасниця може відмовити у наданні будь-якої правової допомоги, якщо її законодавством не передбачено відповідальності за

такі дії (ст. 32 Конвенції) [5].

Африканська конвенція про кібербезпеку та захист персональних даних (2014) є комплексним договором, який розширює перелік правопорушень порівняно з Конвенцією Ради Європи, приділяючи особливу увагу витоку комп'ютерних даних і правопорушенням, пов'язаним із обігом контенту. Зокрема, ст. 28 договору регламентує, що «держави-учасниці, які не мають угод про взаємну правову допомогу, зобов'язуються розглядати підписання угод про взаємну правову допомогу відповідно до принципу подвійної відповідальності, одночасно сприяючи обміну інформації, а також ефективному обміну даними між державами-учасницями на двосторонній або багатосторонній основі» [6]. Конвенція переважно залишає осторонь питання взаємної правової допомоги у справах, заохочуючи держав-учасниць регулювати їх у конкретних міжнародних угодах.

Зазначимо, що Конвенція Ради Європи про кіберзлочинність (2001) і Африканська конвенція про кібербезпеку та захист персональних даних (2014) встановлюють механізми моніторингу, функції яких багато в чому відрізняються.

Зокрема, Конвенційний комітет (T-CY) було створено відповідно до ст. 46 Конвенція Ради Європи про кіберзлочинність (2001) з метою координації консультацій держав-учасниць у сферах сприяння ефективному виконанню Конвенції, включаючи виявлення будь-яких проблем, пов'язаних з цим, а також наслідків будь-якої заяви чи застереження, зроблених згідно з Конвенцією; обмін інформацією про важливі правові, політичні або технологічні розробки, що стосуються кібербезпеки, збір доказів в електронній формі; розгляд можливого доповнень або змін положень Конвенції [4].

Положення статті 32 Африканської конвенції регламентують ширший механізм, ніж той, який закріплює Конвенція Ради Європи, і виконує низку функцій, що охоплюють усі сфери, що регулюються цим актом. Зокрема, передбачено формулювання та сприяння прийняттю узгоджених кодексів поведінки для використання державними службовцями у сфері кібербезпеки; подання звітів Виконавчій раді щодо виконання Конвенції; встановлення партнерських відносин з державними органами, громадянським суспільством, міжурядовими та неурядовими організаціями в досліджуваній сфері тощо [6].

Отже, регіональні договори встановлюють диференційовані правові режими, що в окремих випадках можуть стати підставою виникнення юридичних колізій, призвести до суперечливої судової практики і надати укриття для правопорушників. Зі свого боку, Конвенція Ради Європи про кіберзлочинність (2001) не може створити універсальний механізм міжнародного співробітництва у боротьбі з правопорушеннями у сфері ІТ. Тож наведений міжнародний акт містить складний механізм приєднання, який є доцільним для регіонального договору, однак неприйнятним для будь-якої конвенції універсального характеру. Крім того, варто акцентувати увагу на відсутності глобального консенсусу щодо змісту окремих положень Конвенції Ради Європи стосовно транскордонного доступу до комп'ютерних даних.

Зауважимо, що автентичність регіональних договорів відображається у фрагментарності їх положень. Регіональне зосередження уваги на конкретних потребах в обговорюваній сфері ускладнює створення надійного та ефективного механізму міжнародного співробітництва у забезпеченні кібербезпеки. Вважаємо, що процес розробки регіональних договорів повинен супроводжуватися всебічним дослідженням наявних договорів.

Висновки. Підсумовуючи зазначимо, що розглянуті вище акти створюють правову основу для гармонізації законодавства та взаємодії правоохоронних органів і судів у досліджуваній сфері. Однак вважаємо, що наведеної правової бази недостатньо для створення комплексного та надійного механізму боротьби з правопорушеннями у сфері ІТ.

Регіоналізація міжнародно-правової взаємодії у забезпеченні кібербезпеки має свої позитивні та негативні сторони. З одного боку, регіональна угода є найкращим способом вирішити проблему в межах певного регіону. З іншого боку, різні підходи до легальності дій, вчинених в Інтернеті або з використанням комп'ютерних технологій, можуть завадити взаємній правовій допомозі або екстрадиції між країнами, що належать до різних регіонів. Зауважимо також, що автентичність регіональних договорів відображається у фрагментарності їх положень. Тому регіональне зосередження уваги на конкретних потребах в обговорюваній сфері ускладнює створення надійного та

ефективного механізму міжнародного співробітництва у забезпеченні кібербезпеки. Вважаємо, що процес розробки регіональних договорів має супроводжуватися всебічним теоретико-правовим дослідженням наявних актів.

Важливо, що Конвенція Ради Європи про кіберзлочинність (2001) не може створити універсального механізму міжнародного співробітництва у боротьбі з правопорушеннями у сфері ІТ у зв'язку з тим, що договір містить складний механізм приєднання, який є доцільним для регіонального договору, однак неприйнятним для будь-якої конвенції універсального характеру. Крім того, варто акцентувати на відсутності глобального консенсусу щодо змісту окремих положень Конвенції Ради Європи стосовно транскордонного доступу до комп'ютерних даних.

Тому, зважаючи на значущість співпраці із протидії правопорушенням у сфері ІТ та з урахуванням фрагментарності та розрізненості положень регіональних договорів, що можуть перешкодити ефективному співробітництву, нагальним є вироблення державами узгоджених підходів та укладання відповідного міжнародного договору під егідою Організації Об'єднаних Націй.

Список використаних джерел

1. Chang J. 10 Cybersecurity Trends for 2022/2023: Latest Predictions You Should Know - Financesonline. URL: https://financesonline.com/cybersecurity-trends/.

2. Appazov A. Legal Aspects of Cybersecurity. Faculty of Law University of Copenhagen, 2020. 70 p. URL: https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.

3. Kremer J.-F., Müller B. Cyberspace and international relations: Theory, prospects and challenges. 2014. URL: https://doi.org/10.1007/978-3-642-37481-4.

4. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. : станом на 7 верес. 2005 р. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.

5. Arab Convention on Combating Information Technology Offences : of 21.12.2010. URL : https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

6. African Union Convention on Cyber Security and Personal Data Protection of 27.06.2014. URL : https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

7. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності : Конвенція Орг. Об'єдн. Націй від 15.11.2000 р. : станом на 4 лют. 2004 р. URL : https://zakon.rada.gov.ua/laws/show/995_789#Text.

8. Факультативний протокол до Конвенції про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії : Протокол Орг. Об'єдн. Націй від 01.01.2000 : станом на 3 квіт. 2003 р. URL: https://zakon.rada.gov.ua/laws/show/995_b09#Text.

9. Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice : of 25.04.2005. URL: https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_e_V0584409.pdf.

10. Guidance Notes. Cybercrime. URL : https://www.coe.int/en/web/cybercrime/guidance-notes.

11. Council of Europe. Cybercrime: Towards a Protocol on evidence in the cloud. URL : https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud.

Надійшла до редакції 04.12.2022

References

1. Chang, J. 10 Cybersecurity Trends for 2022/2023: Latest Predictions You Should Know - Financesonline. URL: https://financesonline.com/cybersecurity-trends/.

2. Appazov, A. Legal Aspects of Cybersecurity. Faculty of Law University of Copenhagen, 2020. 70 p. URL : https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.

3. Kremer, J.-F., Müller B. Cyberspace and international relations: Theory, prospects and challenges. 2014. URL : https://doi.org/10.1007/978-3-642-37481-4.

4. Konventsiia pro kiberzlochynnist [Convention on cybercrime] : Konventsiia Rady Yevropy vid 23.11.2001 r. : stanom na 7 veres. 2005 r. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukr.].

5. Arab Convention on Combating Information Technology Offences of 21.12.2010. URL : https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf.

6. African Union Convention on Cyber Security and Personal Data Protection : of 27.06.2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

7. Konventsiia Orhanizatsii Obiednanykh Natsii proty transnatsionalnoi orhanizovanoi zlochynnosti [United Nations Convention against Transnational Organized Crime] : Konventsiia Orh. Obiedn. Natsii vid 15.11.2000 r. : stanom na 4 liut. 2004 r. URL : https://zakon.rada.gov.ua/laws/show/995_789#Text. [in Ukr.].

8. Fakultatyvnyi protokol do Konventsii pro prava dytyny shchodo torhivli ditmy, dytiachoi prostytutsii i dytiachoi pornohrafii [Optional protocol to the Convention on the Rights of the Child on child trafficking, child prostitution and child pornography] : Protokol Orh. Obiedn. Natsii vid 01.01.2000 : stanom na 3 kvit. 2003 r. URL : https://zakon.rada.gov.ua/laws/show/995_b09#Text. [in Ukr.].

9. Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice : of 25.04.2005. URL : https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_e_V0584409.pdf.

10. Guidance Notes. Cybercrime. URL: https://www.coe.int/en/web/cybercrime/guidance-notes.

11. Council of Europe. Cybercrime: Towards a Protocol on evidence in the cloud. URL : https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud.

ABSTRACT

Vlada Litoshko, Karine Mkrtchian. Theoretical and legal aspects of the basis of cooperation of states in combating offenses in the sphere of information technologies. Offenses in the field of information technologies pose a real threat to social relations at the domestic level and the international legal order. Organized criminal groups use new technological means for illegal purposes, causing harm to individuals and legal entities. The specified torts are distinguished by a high degree of latency and in many cases acquire a transnational character, which causes difficulties in their disclosure, bringing the guilty persons to justice, and also actualizes the need to consolidate the efforts of competent authorities of states around the world. The problem of combating offenses in the field of information technologies has been repeatedly considered in the documents of regional international organizations and the United Nations. It should also be noted that cooperation in the field under study is defined as one of the strategic conditions contributing to the achievement of goals in the field of sustainable development.

Since each regional legal regime is unique and has its own characteristics, the article considers the possible consequences of such regionalization. Based on the conducted research, the author concludes that the regionalization of international legal cooperation in the fight against cybercrime has its positive and negative sides and has led to a situation that can be partially explained by the transnational nature of offenses in this area. On the one hand, a regional agreement is the best way to solve a problem within a certain region. On the other hand, different approaches to the legality of actions carried out on the Internet or with the use of computer technologies can hinder mutual legal assistance or extradition between countries belonging to different regions.

Thus, taking into account the importance of cooperation in combating offenses in the field of information technologies, the fragmentation and disparity of the provisions of regional treaties, it is urgent for states to develop coordinated approaches and conclude a corresponding international treaty under the auspices of the United Nations. Regional international legal regulation, in turn, is characterized by fragmentation and diversity.

***Keywords*:** *combating offences, international cooperation, information technology offences, information security, cyber security*.