УДК 343.9
DOI https://doi.org/10.32782/1813-338X-2022.3.17

А. В. Бенескул
аспірант
Державного податкового університету
ORCID ID: 0009-0004-5315-3374

ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ У СФЕРІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

У статті досліджено норми міжнародних нормативно-правових документів, щодо стану забезпечення кримінологічної безпеки у сфері використання цифрових технологій. Автором наголошено на тому, що останнім часом досить розширюються цифрові навички у суспільстві та створюються нові цифрові продукти, що свідчить про необхідність підвищення рівня довіри у громадян до новітніх цифрових продуктів. Саме тому, у статті вказано, що сучасні онлайн-сервіси мають не лише створювати щось нове, але й виявляти дезінформацію та спроби шахрайства, захищатися від кібератак, шахрайства та шахрайства в Інтернеті. Також важливо, що висвітлюється питання кримінологічної безпеки дітей в мережі Інтернет, які вчаться розуміти та орієнтуватися у безлічі інформації, до якої вони мають доступ в Інтернет-просторі. Також у статті висвітлюються питання щодо розвитку та вдосконалення співробітництва у сфері протидії розширенню та впливу цифрової злочинності. Наголошено, що у протидії кіберзлочинності, міжнародний підхід передбачає консолідацію зусиль правоохоронних органів різних держав, формування спеціальних підрозділів, діяльність яких спрямована на боротьбу зі злочинністю в цифровому просторі. Досліджено міжнародно-правові нормативні документи та рекомендації щодо забезпечення належного рівня кібербезпеки, що вказує на необхідність формування національної політики з врахуванням дотримання кібербезпеки у кожному напрямі, як вагомого пріоритету, що відображає ключові зміни в середовищі ризику, коли кіберзагрози розвиваються та набирають швидкий темп, що призводить до вчинення різних правопорушень у цій сфері. Джерела загроз розширюються разом з їх мотивацією та технікою, адже суб'єкти цих правопорушень теж часто мають спеціальну освіту в ІТ-сфері, що ускладнює виявлення та запобігання цим правопорушенням. Пріоритет, який тепер надається кібербезпеці, також відображається реальність того, що Інтернет та ІКТ стали важливими для економічного та соціального розвитку і загалом для інфраструктури. Враховуючи, що залежність громадянського суспільства від цифрових технологій зростає щороку і постійно прискорюється завдяки цифровій трансформації та узагальненню таких технологій, як штучний інтелект та постійна комп'ютеризація та цифровізація, то нажаль, паралельно зростає кількість і складність загроз цифровій безпеці, на які необхідно вчасно впливати та запобігати, щоб не допустити до вчинення правопорушень у цій сфері. Поєднання посилення цифрової залежності та загроз для критично важливих видів діяльності у суспільстві повинно в першу чергу зміцнювати цифровий захист критично важливих видів діяльності. Автором, на основі досліджених міжнародно-правових документів, в межах запобігання кіберзлочинності та забезпечення кримінологічної безпеки у сфері використання цифрових технологій запропоновані конкретні заходи щодо їх реалізації.

Ключові слова: *злочинність, кримінологічна безпека, кіберправопорушення, комп'ютерна злочинність, цифровізація, цифрові технології, запобігання злочинності, протидія кіберзлочинності, міжнародні нормативні документи.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій змінив те, як державні органи, підприємства, інші організації та індивідуальні користувачі, які розробляють ці інформаційні системи та мережі керують ними, обслуговують та використовують їх, адже в першу чергу, вони повинні реагувати на загрози та дотримуватися вимог кібербезпеки. Враховуючи напрями міжнародного співробітництва щодо запобігання кіберзлочинності,

вагоме значення має дослідження окремих міжнародних інституційних механізмів протидії злочинам у сфері злочинності у сфері цифрових технологій, адже кожна міжнародна інституція вносить свій вклад у формування засад протидії злочинності у досліджуваній сфері.

У зв'язку з цим доцільним є розвиток та вдосконалення співробітництва у сфері протидії розширенню та впливу цифрової злочинності. У протидії кіберзлочинності, міжнародний підхід передбачає консолідацію зусиль правоохоронних органів різних держав, формування спеціальних підрозділів, діяльність яких спрямована на боротьбу зі злочинністю в цифровому просторі. Окрім цього, специфічний характер кібершахрайства передбачає не ізольоване державне протистояння у вирішенні зростаючої проблеми цифрової злочинності, а в першу чергу ефективну протидію їй при активізації міжнародної співпраці і об'єднання зусиль різних організацій.

Аналіз останніх досліджень і публікацій. Окремі аспекти щодо вивчення питання про феномен кримінологічної безпеки в Україні та засад її забезпечення, а також щодо використання мережі Інтернет для запобігання злочинності досліджували такі науковці як, О. М. Бандурка, О.І. Бугера, В.М. Бутузов, В.Д. Гавловський, М.О. Гвоздецька, О.М. Литвинов, В.В. Марков, Т. В. Мельничук, С.А. Мозоль, В.В. Семенов, В.Г. Хахановський, В.П. Шеломенцев та інші, проте поряд з основними характеристиками кримінологічної безпеки та запобігання кіберзлочинності, досить важливим є дослідження стану міжнародно-правового регулювання забезпечення кримінологічної безпеки у сфері використання не лише мережі Інтернет, а загалом цифрових технологій.

Постановка завдання. Метою даного дослідження є вивчення міжнародно-правового досвіду щодо забезпечення кримінологічної безпеки у сфері використання цифрових технологій.

Виклад основного матеріалу. Загалом, вперше проблеми запобігання комп'ютерній злочинності розглядалися на IX Конгресі ООН щодо запобігання злочинності та поводження з правопорушниками, в межах проведення якого була обговорена Стратегія комп'ютеризації кримінального правосуддя. У 2000 році на X Конгресі ООН щодо запобігання злочинності та поводження з правопорушниками, однією із тем Конгресу та семінарів-практикумів було питання щодо злочинів, пов'язані з комп'ютерними мережами. На XI Конгресі ООН «Взаємодія та запобіжні заходи: стратегічні напрями взаємодії у сфері попередження злочинності та кримінального правосуддя» була обговорена тема «Заходи боротьби із злочинами, пов'язаними з використанням комп'ютерів». XII Конгрес ООН «Комплексні стратегії для відповіді на глобальні виклики: системи попередження злочинності та кримінального правосуддя та їх розвиток у світі, що змінюється» прийняв декларацію, яка, серед іншого, відкрила можливості для обговорення нових національних та міжнародних заходів щодо протидії кіберзлочинності. А на XIV Конгресі ООН «Активізація заходів запобігання злочинності, кримінального правосуддя та забезпечення верховенства права: назустріч до здійснення, на період до 2030 року» однією із тем семінару-практикуму була: «Сучасні тенденції у сфері злочинності, останні зміни та нові рішення, зокрема використання сучасних технологій як засобів вчинення злочинів та інструментів боротьби зі злочинністю» [10].

На 57 сесії Генеральної Асамблеї ООН було прийнято резолюцію «Створення глобальної культури кібербезпеки», відповідно до якої Генеральна Асамблея, відзначаючи зростаючу залежність урядів, бізнесу та інших організацій і окремих користувачів щодо інформаційних технологій для ведення бізнесу та надання і обміну інформацією, визначила, що потреба в кібербезпеці зростає разом із участю країн в інформаційному суспільстві [8].

Ефективна кібербезпека – це не лише питання уряду чи закону на практиці правозастосування, але її необхідно вирішувати шляхом профілактики кіберзлочинності та підтримки всього суспільстві в інформаційному середовищі. Уряди країн, бізнес, інші організації, а також окремі власники та користувачі інформаційних технологій повинні знати про відповідні ризики кібербезпеки та профілактичні заходи і повинні брати на себе відповідальність щодо вжиття заходів для підвищення безпеки інформаційних та цифрових технологій.

Визнаючи також наявність прогалин у доступі та використанні інформаційних технологій, держави мають ефективно налагоджувати міжнародне співробітництво в боротьбі із злочинністю, пов'язаною із інформаційними технологіями та створювати глобальну культуру кібербезпеки. Тому кожна держава має взяти до уваги потребу в глобальній культурі кібербезпеки; враховувати елементи дотримання кібербезпеки, зокрема, в рамках їхніх зусиль

щодо розвитку у себе в суспільстві культури кібербезпеки при застосуванні та використанні інформаційних технологій; підкреслює необхідність сприяння передачі інформаційної технології країнам, що розвиваються, і створенню в них потенціалу з метою надання їм допомоги у вжитті заходів у сфері кібербезпеки.

Прийняті в 2002 році Рекомендації ОЕСР щодо безпеки інформаційних систем і мереж: до культури безпеки» встановлювали межі принципів, які застосовуються до всіх учасників для підвищення безпеки інформаційних систем і мереж з метою сприяння економічному процвітанню та соціальному розвитку суспільства. Вони згодом були переглянуті і в 2015 р. вказану рекомендацію було замінено на «Рекомендацію Ради щодо управління ризиками цифрової безпеки для економічного та соціального процвітання» [3; 5].

Таким чином, Рекомендація 2015 року, яка замінила Рекомендації ОЕСР 2002 року, вказує на переваги цифрового середовища та необхідність інтеграції управління ризиками цифрової безпеки в процес прийняття економічних і соціальних рішень.

А в грудні 2019 року, вказані Рекомендації були доповнені Рекомендацією ОЕСР щодо цифрової безпеки критично важливих видів діяльності. Ця Рекомендація, звертає увагу, що цифрова трансформація впливає на всю економічну та соціальну діяльність, стимулюючи інновації та створюючи значні вигоди, але також наражає цю діяльність на зростаючий ризик порушення цифрової безпеки, що є наслідком потенційних навмисних або ненавмисних загроз, які мають транскордонний характер, використовують вразливі місця та викликають інциденти, що впливають на доступність, цілісність і конфіденційність даних, апаратного забезпечення, програмного забезпечення та мереж, на які покладається ця діяльність [7]. Враховуючи, вказані ризики, у досліджуваному міжнародно-правовому акті містяться чіткі рекомендації і стратегічні підходи, щодо забезпечення безпеки цифрового середовища у суспільстві.

Також необхідно звернути увагу на стратегічний документ, що прийнятий Європейським Союзом «Цифровий компас 2030», який містить напрями розвитку сучасного та більш вдосконаленого цифрового майбутнього. Проаналізувавши зазначений документ, можна виокремити такі основні конкретні цілі для кожного: кваліфіковане населення та висококваліфіковані фахівці у галузі цифрових технологій; безпечна та ефективна стала цифрова інфраструктура; цифрова трансформація бізнесу; оцифрування державних послуг [2].

Останнім часом досить розширюються цифрові навички у суспільстві та створюються нові цифрові продукти, проте необхідно, щоб і був значний рівень довіри у громадян до новітніх цифрових продуктів. Тому, сучасні онлайн-сервіси мають не лише створювати щось нове, але й виявляти дезінформацію та спроби шахрайства, захищатися від кібератак, шахрайства та шахрайства в Інтернеті, і в першу чергу звертати увагу на дітей, які вчаться розуміти та орієнтуватися у безлічі інформації, до якої вони мають доступ в Інтернеті. Це свідчить про зростання кількості інтернет-загроз для дітей, зокрема: грумінг в цифровому середовищі, сексуальні зловживання і сексуальна експлуатація тощо, що потребує необхідності захисту їх у цифровому середовищі.

Так, Міжнародний союз електрозв'язку (МСЕ) є спеціалізованою агенцією Організації Об'єднаних Націй з інформаційно-комунікаційних технологій (ІКТ), покликаний здійснювати законодавчі, управлінські, виконавчі та консультативні функції, надавати технічну підтримку, розробляти стандарти і правила у сфері електрозв'язку та формулювати рекомендації, спрямовані на активізацію розвитку телекомунікацій та підвищення якості послуг [6].

Однією з його ініціатив є саме захист дітей в мережі Інтернет і на виконання цієї функції Союзом були розроблені Керівні настанови щодо захисту дитини в цифровому середовищі. Рекомендації спрямовані на захист дітей в усіх сферах і від усіх ризиків цифрового світу і, як такі, виділяють передовий досвід галузевих заінтересованих сторін, який можна враховувати в процесі проєктування, розробки та керування політиками захист дітей у цифровому середовищі на рівні компаній. Вони скеровують учасників індустрії не тільки в тому, як управляти і стримувати незаконну онлайнову діяльність, якій вони зобов'язані протидіяти за допомогою своїх послуг, але і в тому, як вирішувати інші питання, які можуть не вважатися злочинами в різних юрисдикціях [11].

Як бачимо, дослідження міжнародно-правових нормативних документів та рекомендацій щодо забезпечення належного рівня кібербезпеки вказує на необхідність формування національної політики з врахуванням дотримання кібербезпеки у кожному напрямі, як вагомого пріо-

оритету. Це відображає ключові зміни в середовищі ризику, коли кіберзагрози розвиваються та набирають швидкий темп, що призводить до вчинення різних правопорушень у цій сфері. Джерела загроз розширюються разом з їх мотивацією та технікою, адже суб'єкти цих правопорушень теж часто мають спеціальну освіту в ІТ-сфері, що ускладнює виявлення та запобігання цим правопорушенням. Пріоритет, який тепер надається кібербезпеці, також відображається реальність того, що Інтернет та ІКТ стали важливими для економічного та соціального розвитку і загалом для інфраструктури. Нове покоління стратегій кібербезпеки спрямоване на стимулювання економічного та соціального розвитку, напрямів захисту суспільства, що залежать від кіберпростору, від кіберзагроз, зберігаючи відкритість Інтернету як платформи для інновацій і нових джерел зростання. Проте, виклики кіберзагрозам теж досить великі та постійно трансформуються і видозмінюються, тому правоохоронні органи повинні мати сучасний фундаментальний підхід, який необхідний для боротьби з кіберзагрозами у відкритому доступі.

Загалом, сама кіберзлочинність була визначена в 2000 році на Десятій сесії ООН «Конгрес із запобігання злочинності та кримінального правосуддя», де було визначено що комп'ютерна злочинність стосується будь-якого кримінального діяння, «які можуть бути вчинені з використанням комп'ютерної системи або мережі, в межах комп'ютерної системи чи мережі, або проти комп'ютерної системи або мережі», що в принципі, охоплювало будь-яке правопорушення, яке може бути вчинене в електронному навколишньому середовищі [9].

Проте, вже на одинадцятому Конгресі ООН «Запобігання злочинності та кримінальне правосуддя (2005)», було запропоновано «сформулювати концептуальну модель запобігання комп'ютерним злочинам». Таким чином, розглядали комп'ютерні злочини як поведінку, яка заборонена законом та/або судовою практикою, що: а) є спрямованою власне на комп'ютерну сферу та комунікацію інформаційних цифрових технологій; б) включає використання цифрових технологій у вчиненні правопорушення; або с) включає використання комп'ютера як інструмента у процесі вчинення інших злочинів, і, відповідно, джерелом електронних процесуальних доказів виступає саме комп'ютер» [4].

14-й Конгрес ООН із запобігання злочинності та кримінального правосуддя проходив у березні 2021 року в Кіото, як найбільше та найрізноманітніше зібрання політиків, практиків, академічних кіл, міжурядових організацій та громадянського суспільства у сфері запобігання злочинності та кримінального правосуддя. Питання кіберзлочинності теж було розглянуто в межах Конгресу, зокрема більшість правопорушень, які підпадають під цей термін включають кіберзлочини, що вчиняються заради прибутку, який вони приносять і досить часто вчиняються організованими злочинними групами. Використання інформаційних технологій для кримінальних цілей та методи кіберзлочинців постійно розвиваються зі швидкістю технічних досягнень в ході розвитку національних і міжнародних стандартів та механізмів. В межах Конгресу була розглянута Програма з кіберзлочинності, що спрямована на підтримку держав-членів у формуванні спеціалізованого міжнародного слідчого співробітництва в галузі кіберзлочинності [1].

Висновки. Отже, як бачимо, більшість як соціальних так і економічних видів діяльності у суспільстві все більше залежать від цифрових технологій. Окремі з цих видів діяльності є досить важливими, а інколи мають навіть критичний вплив на суспільство, оскільки їх порушення можуть суттєво вплинути на безпеку громадян, їх здоров'я безпеку суспільства загалом, на ефективне функціонування органів державної влади чи інших інституцій громадянського суспільства, необхідних для економічного та соціального процвітання в більш широкому сенсі.

Так, зокрема, цифрове перетворення таких критично важливих видів діяльності, таких як для прикладу: охорона здоров'я, водопостачання, енергопостачання, телекомунікації та банківські послуги, дедалі більше наражає їх на загрози кібербезпеці, які можуть вплинути на безпеку та функціонування основних послуг або економічного та соціального процвітання в більш широкому сенсі. Саме тому, залежність громадянського суспільства від цифрових технологій зростає щороку і постійно прискорюється завдяки цифровій трансформації та узагальненню таких технологій, як штучний інтелект та постійна комп'ютеризація та цифровізація. Проте, нажаль, паралельно зростає кількість і складність загроз цифровій безпеці, на які необхідно вчасно впливати та запобігати, щоб не допустити до вчинення правопорушень. Поєднання посилення цифрової залежності та загроз для критично важливих видів діяльно-

сті у суспільстві повинно в першу чергу зміцнювати цифровий захист критично важливих видів діяльності.

Враховуючи, викладене вище, а також досліджені міжнародно-правові документи, пропонуємо, в межах запобігання кіберзлочинності та забезпечення кримінологічної безпеки у сфері використання цифрових технологій наступні заходи:

− розвиток заходів національного характеру та міжнародне співробітництво у кримінальних провадженнях, зокрема щодо посилення заходів виявлення кіберзлочинності, відмивання коштів, одержаних злочинним шляхом та незаконної торгівлі культурними цінностями, а також щодо екстрадиції, взаємної правової допомоги та конфіскації, стягнення та повернення доходів, одержаних злочинним шляхом;

− посилення міжнародного правоохоронного співробітництва, шляхом підвищення потенціалу та кваліфікації існуючої системи правоохоронних органів, які зосереджені на запобіганні кіберзлочинності;

− необхідність покращення взаємної правової допомоги та співпраці на початкових стадіях транскордонних кримінальних проваджень, що стосуються злочинності у сфері цифрових технологій та спрощення процедури взаємної правової допомоги і міжвідомчої слідчої співпраці;

− створення централізованих навчальних курсів по актуальним та сучасним напрямам запобігання кіберзлочинності для слідчих, враховуючи постійні трансформаційні процеси у сфері цифровізації суспільства, що будуть забезпечені експертами у сфері запобігання кіберзлочинності, а також наявність сучасного комп'ютерного обладнання;

− вдосконалення онлайн-дослідницької мережі, за підтримки міжнародних агентств і приватного сектору, що надасть можливості для більшого обміну інформацією, спілкування між експертами в усьому світі з питань комп'ютерної злочинності, порівняльного аналізу і передачі знань про запобігання та боротьбу з комп'ютерними злочинами та розвиток відповідних інструментів навчання, які мають бути доступними на міжнародному рівні, щоб ділитися знаннями та інформацією щодо способів і засобів виявлення, запобігання та боротьби з новими видами кіберзлочинності.

Список використаної літератури:

1. 14th UN Crime Congress – Kyoto, Japan (hybrid format)–7-12 March 2021. International cooperation vital to address all forms of crime, terrorism & new & emerging forms of crime. URL: https://unis.unvienna.org/pdf/2021/Crime_Congress/06_international_cooperation_terrorism_FINAL.pdf
2. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions 2030 Digital Compass: the European way for the Digital Decade. Brussels, 9.3.2021 COM(2021) 118 final. URL: https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf
3. Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document. OECD (2015). URL: https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf
4. Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Bangkok, 18-25 April 2005. URL: https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_e_V0584409.pdf
5. OECD Guidelines for the Security of Information Systems and Networks Towards a culture of security. OECD publications, 2, rue André-Pascal, 75775 PARIS CEDEX 16 PRINTED IN FRANCE. URL: https://www.oecd.org/sti/ieconomy/15582260.pdf (дата звернення: 27.01.2022)
6. Official site International Telecommunication Union (ITU). URL: https://www.itu.int/en/about/Pages/default.aspx
7. Recommendation of the Council on Digital Security of Critical Activities. OECD/LEGAL/0456. Adopted on: 11/12/2019. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456
8. Resolution adopted by the General Assembly [on the report of the Second Committee (A/57/529/Add.3)] 57/239. Creation of a global culture of cybersecurity. General 31 January 2003. URL: file:///C:/Users/%D0%9B%D1%8E%D0%B4%D0%BC%D0%B8%D0%BB%D0%B0/Downloads/A_RES_57_239-EN.pdf
9. Resolution adopted by the General Assembly. A/RES/54/125 26 January 2000. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. URL: https://digitallibrary.un.org/record/404748#record-files-collapse-header
10. United Nations Congresses on Crime Prevention and Criminal Justice 1955–2020. 65 years of achievement. URL: https://unis.unvienna.org/pdf/2020/CrimeCongress/65-years-brochure_en.pdf
11. Захист дітей у цифровому середовищі: рекомендації для індустрій. Міжнародний союз електрозв'язку 2020. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP_Guidelines_Industry_UA_fin66.pdf

Beneskul A. V. Ensuring criminology security in the sphere of use of digital technologies: international legal aspect

The article examines the norms of international legal documents regarding the state of ensuring criminological security in the field of digital technologies. The author emphasized that recently digital skills in society are expanding and new digital products are being created, which indicates the need to increase the level of trust among citizens in the latest digital products. That is why, the article states, modern online services must not only create something new, but also detect misinformation and fraud attempts, protect against cyber attacks, fraud and online fraud. It is also important that the issue of criminological safety of children on the Internet is covered, as they learn to understand and navigate the multitude of information they have access to in the Internet space. The article also covers issues related to the development and improvement of cooperation in the field of combating the expansion and influence of digital crime. It was emphasized that in combating cybercrime, the international approach involves consolidating the efforts of law enforcement agencies of various states, forming special units whose activities are aimed at combating crime in the digital space. International legal normative documents and recommendations for ensuring an adequate level of cyber security have been studied, which indicates the need to form a national policy taking into account the observance of cyber security in every direction, as a significant priority, reflecting key changes in the risk environment, when cyber threats are developing and gaining a rapid pace, which leads to the commission of various offenses in this area. The sources of threats expand along with their motivations and techniques, because the subjects of these crimes also often have special education in the IT field, which makes it difficult to detect and prevent these crimes. The priority now given to cyber security also reflects the reality that the Internet and ICT have become important for economic and social development and for infrastructure in general. Given that the dependence of civil society on digital technologies is growing every year and is constantly accelerating due to digital transformation and the generalization of such technologies as artificial intelligence and permanent computerization and digitalization, unfortunately, the number and complexity of digital security threats that need to be affected in a timely manner are increasing in parallel. and prevent in order to prevent the commission of offenses in this area. The combination of increasing digital dependence and threats to critical activities in society should primarily strengthen the digital protection of critical activities. The author, on the basis of researched international legal documents, within the scope of preventing cybercrime and ensuring criminological security in the use of digital technologies, proposed specific measures for their implementation.

Key words: *crime, criminological security, cybercrime, computer crime, digitalization, digital technologies, crime prevention, combating cybercrime, international normative documents*