4. Рибін О. Хакери злили дані 1,5 млрд користувачів Facebook. URL: https://rg.ru/2021/10/04/hakery-slili-dannye-15-mlrd-polzovatelej-facebook.html.
5. В роботі WhatsApp відбувся збій. URL: https://rg.ru/2022/10/25/v-rabote-whatsapp-proizoshel-sboj.html.
6. В роботі WhatsApp відбувся глобальний збій. URL: https://www.rbc.ru/rbcfreenews/63578d329a7947a58aefbf4c.
7. В роботі WhatsApp відбувся глобальний збій. URL: https://lenta.ru/news/2022/10/25/whatsapp/

Бадалова Т. Г.,
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ,
майор поліції
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОКРЕМІ ПРОБЛЕМНІ ПИТАННЯ ЩОДО ЗДІЙСНЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПІД ЧАС ПРОВЕДЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ПОВ'ЯЗАНИХ З КІБЕЗЛОЧИНАМИ

Становлення інформаційного суспільства в Україні, розвиток та поширення комп'ютерних технологій та комп'ютерної техніки, використання телекомунікаційних мереж майже в усіх сферах життєдіяльності людини полегшило можливість передання інформації, створивши низку проблем, пов'язаних зі створенням безпечних умов використання віртуального простору. У період глобалізації швидкий розвиток інформаційних технологій та комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою та надає широкі можливості для вчинення традиційних злочинів, створюючи при цьому умови для реалізації зовсім нових схем і методів злочинної діяльності. Рівень можливостей, які отримують зловмисники, й тенденція до збільшення кількості злочинів у сфері комп'ютерних інформаційних технологій становлять загрозу не лише демократичним перетворенням та розвитку інформаційного суспільства.

Нині офіційна державна статистика містить відомості про вчинені кримінальні правопорушення, передбачені Розділом XVI КК України, які відображаються у звітах Офісу Генерального прокурора України (далі – ОГП) [1] та у відомчій статистичній звітності Національної поліції України (за даними Офісу Генерального прокурора) представлені в табл. 1.

Таблиця 1

Рік	Облікові кримінальні правопорушення	Кількість осіб, яким вручено повідомлення про підозру
2014	443	207
2015	598	263
2016	865	472
2017	2573	1272
2018	2301	1608
2019	2204	1481
2020	2498	1675
2021	2790	2034

Питома вага злочинності у сфері електронно-обчислюваних машин у структурі злочинності в Україні за 2014 рік становила приблизно 0,08 %, у 2015 р. – 0,01 %, у 2016 р. – 0,15 %, у 2017 р. – 0,49 %, у 2018 р. – 0,5 %, у 2019 р. – 0,49 %, у 2020 р. – 0,7 %, а у 2021 р. (станом на жовтень) – 0,93 % [2]. Рівень судимості за 2014 рік склав 37 осіб, за 2015 – 31 особу, за 2016 – 24 особи, за 2017 – 42 особи, за 2018 – 49 осіб, за 2019 – 50 осіб, за 2020 – 56 осіб. Отже, зазначений показник є досить мізерним порівняно з кількістю облікованих щорічно злочинів [3]. За звітними даними Голови Національної поліції України, ціна кіберзлочинності в Україні за 2019 рік становила 28 мільйонів гривень, а станом на 2020 рік зросла до 241 мільйона гривень [4]. Американська компанія McAfee, яка спеціалізується на комп'ютерній безпеці, та Центр стратегічних і міжнародних досліджень (CSIS) стверджують, що хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів, або 820 мільярдів євро [4]. Аналізуючи дані за 2020 рік щодо структури, можемо дійти висновку, що найбільшу питому вагу серед злочинів, передбачених розділом XVI КК України (49 %) становлять дії з несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ).

На сьогодні в українському законодавстві відсутнє визначення поняття «кіберзлочин» або «кіберзлочинність», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку (розділ XVI Кримінального кодексу України (далі – КК України)) [5], зокрема: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361-1 КК України); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних

машинах 8 (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 361-2 КК України); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 КК України); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363-1 КК України). Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Банківська система України є однією зі сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет. А враховуючи, що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більшу увагу злочинців.

Важливу роль у боротьбі та розслідуванні кіберзлочинів мають значення міжнародні угоди, Конвенції Ради Європи, рішення Ради Европейского Союзу та ін.

Питання кібербезпеки перебуває на особливому контролі з боку міжнародної спільноти, про що свідчить прийняття 23 листопада 2001 р. Конвенції про кіберзлочинність, яку Україна ратифікувала 07.09.2005 [6].

У преамбулі цієї Конвенції вказано, що вона «*є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва*».

Конвенція закріплює чимало різних положень, які декларують можливості отримати міжнародну допомогу країнам-учасницям у боротьбі з кіберзлочинністю, серед яких слід виділити принцип надання міжнародно – правової допомоги, це насамперед пов'язано з отриманням необхідної інформації або документів, які суттєво впливають на процес доказу скоєного кримінального правопорушення.

Поняттям міжнародна правова допомога включає в себе проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою.

Згідно до вимог ст. 542 КПК України міжнародне співробітництво під час кримінального провадження полягає у вжитті необхідних заходів з метою надання міжнародної правової допомоги шляхом вручення документів, виконання окремих процесуальних дій, видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування, передачі засуджених осіб та виконання вироків. Міжнародним договором України можуть бути передбачені інші, ніж у цьому Кодексі, форми співробітництва під час кримінального провадження.

Під час міжнародного співробітництва у сфері протидії кіберзлочинів реалізується у відповідності до чинного законодавства, але аналіз законодавства, вказує про відсутність спільного та узгодженого підходу до міжнародного співробітництва.

Одними із основних проблем міжнародного співробітництва під час розслідування кримінальних правопорушень у сфері кіберзлочинів є недосконаліть чинного законодавства України, щодо здійснення міжнародно – правової допомоги. Це насамперед стосується отримання відповідних ухвал щодо тимчасових доступів до інформації та документів.

Розглянемо проблематику проведення екстрадиції за злочинами, передбаченими ст. 361 КК України на прикладі кримінального провадження, внесеного до Єдиного реєстру досудових розслідувань СУ ГУНП в Дніпропетровській області.

Так, згідно з матеріалів кримінального провадження: «*в період часу з лютого 2016 року по березень 2016 року невстановлені особи за допомогою програмного забезпечення здійснили втручання в локальну обчислювальну мережу Публічного Акціонерного Товариства «БКД», міжнародну систему «Society for Worldwide Financial Telecommunications» – «S. W. I. F. T.», та отримали доступ до операційних дій з міжнародного переказу грошових коштів. Тобто невстановлені особи, отримавши доступ до локальної обчислювальної мережі ПАТ «БКД», увійшли до системи «S. W. I. F. T.», та використовуючи отримані злочинним шляхом платіжні документи, внесли в них фіктивні дані. Після обробки платіжних документів, системою «S. W. I. F. T.» було підтверджено операцію і здійснено переказ грошових коштів, з кореспондентських рахунків ПАТ «БКД» на рахунки банку Туреччини. Після цього невстановлені особи видалили створені ними файли, що призвело до зупинки роботи системи «S. W. I. F. T.». В результаті злочинних дій невстановлених осіб ПАТ «БКД» було спричинено значну матеріальну шкоду у розмірі 951 838, 95 доларів США, 1 468 593 доларів США, 1 833 956, 18 євро».*

У подальшому під час проведення досудового розслідування вказаного кримінального провадження СУ ГУНП у порядку ст. 552 КПК України та Європейської конвенції про взаємну правову допомогу в кримінальних справах 1959 року звернулася до компетентних органів Туреччини з запитом про надання міжнародної правової допомоги та висловила своє прохання здійснити тимчасовий доступ до речей та документів банківських рахунків банків Туреччини. Формування вказаного запиту довго тривало у зв'язку з тим, що треба було отримати відповідні ухвали та здійснити переклад на дуже рідкісну мову – турецьку. Також СУ ГУНП планувалися заходи, щодо арешту відповідних банківських рахунків, але судом на підставі ч. 7 ст. 173 було відмовлено у зв'язку з тим, що власники рахунків банків Туреччини не викликано у засідання суду для вирішення питання щодо арешту. Вказані слідчим суддею в ухвалі про відмову обставини не можливо було здійснити у зв'язку з тим, що офіційно сповістити турецьку сторону про розгляд клопотання про арешт майна можливо лише за міжнародним запитом. Всі заходи, щодо підготовки всіх необхідних матеріалів та їх переклад тривав більш ніж 2 місяці, що негативно впливало на повернення грошових коштів та отримання інформації, щодо власників рахунку та рух коштів по вказаним рахункам.

Ситуацію щодо повернення грошових коштів до ПАТ «БКД» вдалося вирішити лише завдяки співпраці ПАТ «БКД» та банків Туреччини, у подальшому запит було надіслано до компетентних органів Туреччини та отримано необхідну інформацію, але завдяки співробітників ПАТ «БКД» вдалося уникнути зняття з рахунків банків Туреччини грошових коштів у розмірі 951 838, 95 доларів США, 1 468 593 доларів США, 1 833 956, 18 євро.

На нашу думку слід враховувати законодавства іноземних держав під час здійснення міжнародного співробітництва та внести відповідні зміни до ст. ст. 170 – 173 КПК України, щодо розгляду клопотань про арешт майна у випадку здійснення міжнародно – правової допомоги та внести відповідні зміни до глави 44 КПК України, при цьому слід розробити відповідний механізм застосування чинного законодавства України та не допускати випадки втрати можливості отримання доказів під час здійснення міжнародно-правової допомоги у кримінальних провадженнях даної категорії кримінальних правопорушень.

Список використаних джерел:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: Єдиний звіт Офісу Генерального прокурора. URL: https://www.gp.gov.ua/ua/stat_n_st?dir_id=113653&libid=100820.
2. Судова статистика. Форма № 7 «Звіт про склад засуджених». URL: http://court.gov.ua/inshe/sudova_statystyka/
3. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf.
4. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://tsn.ua/groshi/kiberzlochinci-u2020-roci-zavdali-u-sviti-zbitkiv-na-trilyon-dolariv-doslidzhennya-1683076.html.
5. Головкін Б. М., Голіна В. В., Лисодєд О. В. Кримінологія: підручник. Право, 2020. 259 с.
6. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.