Поступове виконання цих завдань завершить формування Національної поліції як органу, призначеного для забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, діяльність якого буде базуватися на принципах верховенства права, дотримання прав і свобод людини, законності, відкритості і прозорості, політичної нейтральності, безперервності, а також взаємодії з населенням на засадах партнерства.

Формування в Україні правоохоронного органу європейського типу прискорить можливість вступу України до ЄС, а також набуття членства в Альянсі, що є беззаперечним і безальтернативним, враховуючи сьогоднішню необхідність подолання військової агресії і терористичної загрози.

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.
2. URL: http://interpol.np.gov.ua/?pa.
3. Про затвердження річної національної програми під егідою Комісії Україна – НАТО на 2017 рік: Указ Президента України від 08.04.2017 № 103\2017.

Лавренко П.Є.,
слухач Криворізького факультету
Дніпропетровського державного
університету внутрішніх справ

ОСОБЛИВОСТІ ДІЯЛЬНОСТІ КІБЕРПОЛІЦІЇ: ДОСВІД КРАЇН ЄВРОПИ ТА США

Удосконалення інформаційних технологій в усьому світі набагато спростило повсякденне життя людей. Але разом з тим і з'явилися нові загрози в кіберпросторі. Анонімність мережі Інтернет, швидкість передачі даних та простота їх використання – тобто те, що є основними причинами технологічного буму і проникнення мережі Інтернет в усі сфери життя – одночасно дозволило використовувати ці переваги для вчинення злочинних діянь. Інформаційні технології впроваджуються і розвиваються набагато швидше, ніж правоохоронні органи можуть реагувати на це зростання. А тому виникає нагальна потреба в законодавчому регулюванні діяльності органів кіберполіції в державах світу. Нижче описано особливості діяльності кіберполіції в країнах-учасницях ЄС та США.

З моменту зародження цивілізації виникло й таке негативне явище, як злочинність. Поява злочинності пов'язана з нормативно-правовою забороною вчинення злочинів. У сучасному світі одним із найпоширеніших видів злочинності є злочини у сфері інформаційних технологій, що має назву кіберзлочинність.

Праобразом сучасних комп'ютерів вважається механічна машина Чарльза Беббіджа, створена у 1822 році. У той час основним завданням Беббіджа було створення машини, здатної обчислювати математичні задачі.

7 квітня 1953 року компанія IBM представила модель 701, перший у світі серійний електронний комп'ютер. Пізніше, в 1981 році, IBM представила персональний комп'ютер під назвою IBM PC. Комп'ютер мав кодову назву, але іноді його називали Acorn, мав процесор 8088, 16 КБ пам'яті, яку можна було розширити до 256 КБ, при цьому використовувалася ОС MS-DOS [4]. Саме з виникненням «персонального комп'ютера» (далі – ПК) у сучасному його розумінні й почала з'являтися кіберзлочинність.

Новітні інформаційні технології дали поштовх не тільки прогресу суспільства, а й стимулювали виникнення і розвиток невідомих раніше негативних процесів, одним з яких є поява нових форм злочинності. Так, наприклад, революція в галузі електроніки/техніки надала злочинцям, їх угрупованням і суспільним групам широкі можливості в плані доступу до нових технічних засобів, які дозволяють їм незаконно привласнювати значні кошти, легалізувати величезні доходи, отримані злочинним шляхом, ухилятися від оподаткування та проводити комплексні заходи з підготовки, вчинення і маскування різних видів злочинів [8, п. 9].

Кіберзлочинність можна визначити як злочини, вчинені в мережі інтернет з використанням комп'ютера в ролі знаряддя злочину, зараження інших систем вірусними програмами тощо. Важко класифікувати комп'ютерні злочини в цілому на окремі групи, оскільки щоденно їх виникає значна кількість.

Кіберзлочинці можуть використовувати комп'ютерні технології для доступу до особистої інформації, комерційних або державних секретів, використання Інтернету з метою експлуатації або в зловмисних цілях. Злочинці також використовують комп'ютери для зв'язку і зберігання документів або даних. Злочинців, які скоюють зазначені незаконні дії, часто називають хакерами.

При кіберзлочинності комп'ютер може виступати у ролі:

- мети – атаки на комп'ютери (наприклад, поширення вірусів);
- зброї – для здійснення шахрайства;
- електронного помічника – для зберігання незаконної або вкраденої інформації тощо.

Існує багато інструментів й методів проведення кіберзлочинності, в тому числі електронні листи шахраїв, фішинг – вид інтернет-шахрайства з використанням соціальної інженерії для отримання доступу до конфіденційної інформації користувачів – логінів і паролів, підроблені веб-сайти, карти скіммінгу пристроїв – вид шахрайства з банківськими картами, комп'ютерних вірусів тощо. У більшості випадків ви можете бути в безпеці від кіберзлочинності, будучи проінформовані про тип загроз, використовуючи спеціальне програмне забезпечення, наприклад антивірусні програми.

Завдяки Інтернету комп'ютерна кримінальна епідемія стрімко розвивається. За оцінками Інтерполу, швидкість зростання рівня злочинності в глобальній комп'ютерній мережі є найбільшою, порівняно з іншими видами злочинів, серед яких торгівля наркотиками та зброєю. За оцінкою голови зовнішньополітичного відомства Великої Британії В. Хейга, глобальна шкода від кіберзлочинів становить понад трильйон доларів США на рік. За даними опитування, проведеного компанією Symantec, майже дві третини користува-

чів Інтернету хоча б одноразово ставали жертвами кібернетичного злочину [10, с. 3-4].

Злочини у сфері інформаційних технологій дуже часто є міжнародними, тобто злочинці діють в одній державі, а їх жертви знаходяться в іншій. Тому для боротьби з такими злочинами особливе значення має міжнародне співробітництво. 23 листопада 2001 р. в м. Будапешті Радою Європи було укладено Міжнародну конвенцію про кіберзлочинність ETS №185, до якої у 2005 році приєдналася Україна [9].

Відповідно до Конвенції кожна держава-учасниця зобов'язана створити необхідні правові умови для надання таких прав і обов'язків компетентним органам по боротьбі з кіберзлочинністю: виїмка комп'ютерної системи, її частини або носіїв; виготовлення та конфіскація копій комп'ютерних даних; забезпечення цілісності і збереження комп'ютерних даних, що стосуються справи; знищення або блокування комп'ютерних даних, що знаходяться в комп'ютерній системі, та ін.

З метою забезпечення ефективної протидії таким негативним проявам більшість розвинутих держав світу побудували свою політику в правоохоронній сфері шляхом створення окремих відомств чи служб, що спеціалізуються на протидії міжнародній кіберзлочинності (США – Federal Bureau of Investigation, Великобританія – National Crime Agency, Китай – People's Police, Японія – National Police Agency, Франція – Office central de lutte contre la criminalite liee aux technologies de l'information et de la communication тощо) [7, с. 88].

Як вже наголошувалося, кіберзлочинність нині є найбільш гострою проблемою для всіх країн, оскільки носить міжнародний характер, а тому у всьому світі створюються національні агенції, комітети, служби тощо протидії кіберзлочинності. Так, у США боротьбою із кіберзлочинністю займається Federal Bureau of Investigation, у Великобританії – National Crime Agency, у Китаї – спеціально створене бюро Cyber Security and Technology Crime Bureau, у Франції – Office central de lutte contre la criminalite liee aux technologies de l'information et de la communication.

Організація Північноатлантичного договору (НАТО) також активно займається питанням протидії кіберзлочинності. Створено Об'єднаний центр передових технологій з кібероборони – Cooperative Cyber Defence Centre of Excellence. 28 жовтня 2008 Північноатлантична рада надала Об'єднаному центу акредитацію при НАТО та статус Міжнародної військової організації. Центр проводить дослідження і навчання в сфері кіберзахисту. У січні 2013 р. в Гаазі, Нідерланди, почав роботу Європейський центр по боротьбі з кіберзлочинністю [2]. В Україні також планується відкрити Об'єднаний центр передових технологій з кібероборони при НАТО за підтримки фахівців НАТО і консультантів турецької компанії HAVELSAN [6].

У Великобританії створено регіональні поліцейські кіберпідрозділи The Police Central e-crime Unit. Управління з податкових та митних зборів Її Величності (HMRC) створило нову команду по боротьбі з кіберзлочинністю [5]. Національне агентство протидії злочинності Великобританії наголошує на тому, що

кіберзлочинність нині перевершила всі інші форми злочинності в Сполученому Королівстві. За оцінкою агентства від 7 липня 2016 року кібершахрайство складає 36% із загальної злочинності, а комп'ютерне зловживання – 17%. Тому наголошується на необхідності удосконалення правоохоронних органів і зміцнення ділового партнерства по боротьбі з кіберзлочинністю [1].

Визнаючи кіберзлочинність як проблему, що постійно зростає, ФБР в США створили кібер-відділи – Cyber Division, в результаті чого спеціально навчені кібер-команди тепер працюють в штаб-квартирі ФБР і в кожному з 56 відділень Бюро з розслідування кіберзлочинів, в тому числі комп'ютерних вторгнень, крадіжок інтелектуальної власності, персональних даних, дитячої порнографії та шахрайства. ФБР стверджує, що місія таких кібер-відділів полягає в тому, щоб: 1) реагувати, координувати, контролювати кіберрозслідування злочинів, пов'язаних з Інтернетом, комп'ютерних мереж і систем, зокрема загроз, пов'язаних з терористичними організаціями, іноземними урядами, і/або організованою злочинністю; 2) створювати і підтримувати державні/приватні об'єднання з використанням спеціальної освіти і професійної підготовки, щоб максимально протидіяти тероризму, контррозвідки, і з боку правоохоронних органів з кіберзлочинністю; та 3) запроваджувати і використовувати новітні технології у боротьбі із кіберзлочинністю [3].

Для оптимізації оперативного співробітництва між усіма державними органами і поліпшення координації заходів щодо захисту та реагування на злочини в кіберпросторі, в ФРН створено декілька відомств протидії кіберзлочинності: Національний центр захисту від кіберзлочинності (National Cyber Response Centre). Він звітує перед Федеральним відомством інформаційної безпеки (BSI) і безпосередньо співпрацює з самим відомством та Федеральним управлінням цивільного захисту та допомоги при стихійних лихах. Діяльність таких органів закріплено в Стратегії інформаційної безпеки ФРН, що була прийнята у 2011 році [12].

Протягом минулого року в Європі проводилася масштабна міжнародна операція з виявлення та затримання злочинців («дропів»), які допомагають кібершахраям відмивати і знімати готівку, що були вкрадені з рахунків юридичних та фізичних осіб через мережу Інтернет.

Операцію було організовано в рамках кампанії EMMA (European Money Mule Action), організатором якої є Європейський центр по боротьбі з кіберзлочинністю (European Ciber Crime Centre (EC3). Таку ініціативу підтримали Європол, Агентство ЄС, що співпрацює з судовими та поліцейськими органами країн-членів ЄС (Євроюст), та Європейська банківська федерація.

Для виконання основної мети кампанії – боротьби зі збільшенням кількості «дропів» – було створено ефективне транскордонне співробітництво між правоохоронним і банківським сектором. Зокрема, до міжнародної операції приєдналися правоохоронні, судові органи і банківські установи з 14 країн ЄС, України, Молдови, Сполучених Штатів Америки, а також Федеральне бюро розслідувань (ФБР) і Секретна служба США.

Результатом операції стала ідентифікація по всій Європі 580 «дропів», збиток від злочинної діяльності яких склав 23 млн. євро. Національними пра-

воохоронними органами в ході операції було опитано 380 підозрюваних; за посередництво у відмиванні грошей заарештовано 178 осіб. Співробітники Департаменту кіберполіції України відзвітували про проведені слідчі (розшукові) дії на території України під час фінального засідання в Гаазі. Співпраця правоохоронців і банкірів виявилася настільки успішною, що тепер в планах ЕС3 – створити основу для постійної спільної роботи фахівців обох сегментів.

Наступним етапом кампанії EMMA стане розповсюдження інформації про те, як не стати «дропом» випадково, адже, як показує практика, багато осіб допомагають шахраям відмивати і переводити вкрадені через мережу Інтернет кошти, не усвідомлюючи, що за це передбачено кримінальну відповідальність. Злочинці вербують необачних громадян, обіцяючи швидкий і легкий заробіток: «дроп» пропонують здійснювати певні транзакції, отримуючи за це відсоток від перерахованих сум. Насправді відкриваються рахунки, на які надходять кошти, отримані незаконним шляхом (в тому числі у результаті фішингу та вішингу – видів шахрайства у сфері електронних платежів і карткових розрахунків з використанням методів соціальної інженерії), а потім невеликими сумами переводять ці кошти на рахунки злочинців. За даними ЕС3, більше 90% шахрайських грошових переказів пов'язані з кіберзлочинністю.

Співпраця України з Європейським центром із боротьби з кіберзлочинністю не обмежилася участю правоохоронців в операції EMMA. Протягом 2016 року відбулися три робочі зустрічі Групи радників з фінансових питань Правління ЕС3. Під час однієї із зустрічей українська сторона представила європейським партнерам концепцію Національної програми сприяння безпеці електронних платежів і карткових розрахунків Safe Card, яка зараз реалізується в Україні Асоціацією ЄМА (Українська міжбанківська асоціація членів платіжних систем «ЄМА») за підтримки Державного департаменту США.

Також у жовтні 2016 року Україна приєдналася до глобальної освітньої програми протидії шахрайству з використанням шкідливого ПО на мобільних пристроях Europole Mobile Malware Awareness Campaign. Зараз триває робота зі створення української версії сервісу www.nomoreransom.org, який покликаний допомогти жертвам кібервимагань [11].

Кіберзлочинність набуває все більш розповсюдженого характеру в усіх країнах світу, у тому числі й в Україні. А тому, задля можливості виявляти і розслідувати факти кіберзлочинності, правоохоронні органи потребують кваліфікованих фахівців і дослідників, наприклад комп'ютерних судово-медичних експертів, спеціально навчених працівників органів прокуратури з питань протидії кіберзлочинності, а також удосконалення Департаменту кіберполіції України та підвищення кваліфікації співробітників.

В першу чергу необхідним є подальше розроблення міжнародного законодавства, що закріплює та регулює статус і діяльність спеціально створених органів боротьби із кіберзлочинністю, а також міжнародна консолідація таких органів.

---

1. Cybercrime Overtakes Traditional Crime in UK. URL: https://krebsonsecurity.com/2016/07/cybercrime-overtakes-traditional-crime-in-uk.
2. European Cybercrime Centre (EC3) at Europol. URL:

https://www.europol.europa.eu/ec3.

3. URL: https://fbiretired.com/skillset/fbi-cyber-crime.

4. Margaret Gold, April 27, 2012. URL: http://overtheair.org/blog/2012/04/when-was-the-first-computer-invented.

5. Minister for the Cabinet Office and Paymaster General: Progress on the UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. URL: http://www.cabinetoffice.gov.uk/sites/default/files/resources/ WMS_Cyber_Strategy_3-Dec-12_3.pdf.

6. В Украине появится центр НАТО по кибербезопасности. URL: http://vesti-ukr.com/politika/233144-v-ukraine-pojavitsja-tsentr-nato-po-kiberbezopasnosti.

7. Демедюк С. В. Кіберполіція України. *Наше право.* 2015. № 6. С. 87–93. URL: http://nbuv.gov.ua/UJRN/Nashp_2015_6_15.

8. Доповідь генерального секретаря Організації Об'єднаних Націй «Вплив організованої злочинної діяльності на суспільство в цілому». *Матер. Комісії ООН із запобігання злочинності та кримінального правосуддя*. Відень, 13–23 квіт., E / CN. 15/1993/3.

9. Конвенція про кіберзлочинність. URL: http://zakon3.rada.gov.ua/laws/show/994_575.

10. Орлов Ю. Ю. Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України. Бібліогр., 7 назв.

11. Отмывание средств, украденных мошенниками в Интернете: как случайно не стать участником преступной схемы. URL: https://ema.com.ua/money-funds-stolen-by-fraudsters-on-the-internet.

12. Стратегія інформаційної безпеки ФРН, 2011 р. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile.

Чепеляк Карина Валеріївна,
курсант факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник – *к.ю.н., доцент* ***Поливанюк В.Д.***
(Дніпропетровський державний
університет внутрішніх справ)

СПІВПРАЦЯ УКРАЇНИ З НАТО ЯК СТРАТЕГІЧНИЙ КРОК ДО ЄВРОІНТЕГРАЦІЙНОГО ПРОСТОРУ

Актуальність даної теми зумовлена тим, що на сучасному етапі розвитку в Україні поширюється тенденція широкого розгляду проблем стосовно євроатлантичної інтеграції, що є результатом створення цілої мережі спеціалізованих державних інституцій, які покликані досліджувати євроінтеграційні процеси. Висвітлення цієї теми у засобах масової інформації не дає змогу повно охопити аспект євроінтеграційних проблем, котрі в багатьох випадках розглядаються безсистемно. В результаті цього це негативно позначається у зовнішньополітичній стратегії нашої держави.

Незаперечним є той факт, що українське суспільство проходило досить складний шлях у трансформаціях своїх поглядів у питаннях НАТО і ЄС, починаючи з їх несприйняття у 1990-х р.. і завершуючи усвідомленням біль-