УДК 340.132.6:341.48

ХАХАНОВСЬКИЙ В.Г., *доктор юридичних наук, професор,* професор кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ.
ORCID: https://orsid.org/0000-0001-5676-5641.
ГАВЛОВСЬКИЙ В.Д., *кандидат юридичних наук, с.н.с.,* головний науковий співробітник Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю при РНБО України.

ТЛУМАЧЕННЯ ТА КЛАСИФІКАЦІЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЯК КІБЕРЗЛОЧИНІВ

Анотація. *Розглянуто проблеми тлумачення та класифікації кіберзлочинів, проведено аналіз статистичної звітності Національної поліції України щодо показників про кіберзлочинність. Пропонується перелік "традиційних" кримінальних правопорушень, які можуть відноситися до категорії кіберзлочинів. Надаються рекомендації щодо кваліфікації окремих кіберзлочинів.*

Ключові слова: *кіберзлочин, класифікація кіберзлочинів, статистичні показники, "традиційні" кримінальні правопорушення як кіберзлочини.*

Summary. *The problems of interpretation and classification of cybercrimes are considered, the analysis of statistical reporting of the National Police of Ukraine on indicators of cybercrime is carried out. A list of "traditional" criminal offenses that may fall into the category of cybercrime is proposed. Recommendations on the qualification of individual cybercrimes are provided.*

Keywords: *cybercrime, classification of cybercrimes, statistical indicators, "traditional" criminal offenses as cybercrimes.*

Аннотация. *Рассмотрены проблемы толкования и классификации киберпреступлений, проведено анализ статистической отчетности Национальной полиции Украины относительно показателей о киберпреступности. Предлагается перечень "традиционных" уголовных правонарушений, которые могут относиться к категории киберпреступлений. Даются рекомендации в отношении квалификации отдельных киберпреступлений.*

Ключевые слова: *киберпреступление, классификация киберпреступлений, статистические показатели, "традиционные" уголовные правонарушения как киберпреступления.*

Постановка проблеми. Злочинність, яка є невід'ємною частиною суспільства, існувала в усі часи, існує вона й у віртуальному просторі як кіберзлочинність. Водночас офіційного, закріпленого в міжнародних документах визначення кіберзлочинності поки не існує. Тим не менш це не заважає визначати діапазон спеціальних слідчих повноважень і можливостей в сфері міжнародного співробітництва, які більшою мірою стосуються виявлення електронних доказів вчинення будь-якого злочину, зокрема, в межах Конвенції Ради Європи про кіберзлочинність (далі – Конвенція).

Разом з тим, відносно кримінальних правопорушень, що становлять основу кіберзлочинності, деякі визначення необхідні. Зокрема, для розробки правових заходів боротьби з цим видом правопорушень на національному рівні, для збирання та аналізу статистичних даних, вироблення системи єдиного обліку на глобальному рівні тощо.

Крім того, для боротьби з кіберзлочинністю необхідно, в першу чергу, мати перелік суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну

відповідальність та/або яке визнано злочином міжнародними договорами України, тобто перелік злочинів, які можуть кваліфікуватися як кіберзлочини.

Варто зазначити, що термін "кіберзлочинність" часто вживається поряд з термінами "комп`ютерна злочинність", "злочинність в сфері високих інформаційних технологій" тощо. Причому нерідко ці поняття використовуються як синоніми. Тобто доктринальні підходи до розуміння поняття кіберзлочин є різними. Проте попри наявні альтернативні дефініції саме термін кіберзлочинність найбільшою мірою відображає сутність зазначеного явища.

В національному законодавстві України – в Законі України "Про основні засади забезпечення кібербезпеки України" від 05.10.17 р. № 2163-VIII, кіберзлочинність визначається як сукупність кіберзлочинів. А кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Результати аналізу наукових публікацій. Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як Н.М. Ахтирська, В.М. Бутузов, В.О. Голубєв, М.В. Гуцалюк, С.В. Демедюк, В. Шеломенцев та ін. [2 – 7]. Проте у вітчизняному законодавстві не існує чіткого визначення поняття кіберзлочин. Дискутуються також різні точки зору щодо класифікації кіберзлочинів. У зв'язку з появою новітніх інформаційних технологій та способів вчинення кіберзлочинів, ці питання потребують подальшого дослідження та ретельного вивчення як науково-теоретичної проблеми.

Метою статті є визначення класифікацій кіберзлочинів, які надаються в офіційних документах, зокрема ООН, ЄС, та дослідженнях науковців, через які розкривається поняття кіберзлочинність, визначення переліку кримінальних правопорушень, які можуть відноситися до категорії кіберзлочинів та аналіз статистичної звітності Національної поліції України щодо показників про кіберзлочини.

Виклад основного матеріалу. Підхід щодо класифікацій кіберзлочинів, через які розкривається поняття кіберзлочинність, є досить загальним, але водночас відображає специфіку даного виду злочинів.

Насамперед, варто зазначити, що Конвенція про кіберзлочинність є єдиним зобов'язуючим міжнародним інструментом у сфері протидії кіберзлочинності. Вона містить набір основних принципів для будь-якої країни, що розробляє національне законодавство з протидії кіберзлочинності. Разом з тим, наведена в Конвенції класифікація, на думку низки західних і вітчизняних дослідників, не є всеосяжною. Спочатку в Конвенції кіберзлочини поділялися на чотири групи. Потім, на початку 2002 р. на додаток до Конвенції ухвалили протокол, який доповнив перелік злочинів поширенням інформації расистського й іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, релігійній або етнічній приналежності. Із розвитком науково-технічного потенціалу і громадських відносин у кіберпросторі згаданий список буде, на жаль, розширюватися. До того ж зазначені в Конвенції злочини пов'язані з деякими, але не з усіма діями, які посягають на громадську безпеку. Разом з тим, іншу думку висловлюють науковці, яким імпонує система кіберзлочинів, передбачена Конвенцією.

У звіті Комітету внутрішніх справ Парламенту Великобританії щодо кіберзлочинності у 2013 році кіберзлочини поділяють на три категорії:

– виключно мережеві злочини, де цифрові системи є основною ціллю, що одночасно виступають і засобами посягання. Ця категорія включає в себе посягання на

комп'ютерні системи для знищення інфраструктури інтернет-технологій та незаконне заволодіння даними;

– існуючі злочини, що були переведені в площину кіберзлочинів через використання Інтернету;

– використання Інтернету з метою торгівлі наркотиками та як допоміжний інструмент для вчинення інших видів злочинів [8].

У спільному повідомленні Європейської Комісії у 2013 р. до Європейського Парламенту, Ради, Європейського економіко-соціального комітету та Комітету регіонів кіберзлочинність також розкривається через три основні категорії:

– традиційні види злочинів (шахрайство, підробка документів і т.п.), що вчиняються з використанням електронних комунікаційних мереж та інформаційних систем;

– розміщення незаконного контенту в електронних медіа;

– атаки на інформаційні системи, блокування програмного забезпечення сайтів і хакерство [9].

Більшість дослідників, які вивчають проблему кіберзлочинності, пропонують поділяти кіберзлочини на види залежно від об'єкта та предмета посягання. Найпоширеніший поділ як варіант – це комп'ютерні злочини та злочини, вчинені за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв для доступу до кіберпростору. Ця позиція підтримується і тим, що на Десятому Конгресі Організації Об'єднаних Націй з профілактики злочинності і поводження з правопорушниками, де розглядалися заходи щодо боротьби зі злочинами, які пов'язані з використанням комп'ютерної мережі, поняття про кіберзлочини розглядалося з точки зору двох аспектів: кіберзлочини в "широкому" і "вузькому" сенсі.

1. Кіберзлочин у вузькому сенсі (комп'ютерний злочин): будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є порушення безпеки комп'ютерних систем і обробки ними даних.

2. Кіберзлочин у широкому розумінні (як злочин, пов'язаний із комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію чи розповсюдження інформації за допомогою комп'ютерних систем або мереж.

Разом із тим, у доповіді цього ж Конгресу вказується, що термін "комп'ютерні злочини" був розроблений для охоплення як абсолютно нових форм злочинності, орієнтованої на комп'ютери, мережі і їх користувачів, так і більш традиційних злочинів, які в даний час вчиняються з використанням або за допомогою комп'ютерного обладнання [10].

До того ж у виступі Генерального секретаря ООН "Висновки дослідження з питання про ефективні заходи щодо запобігання високотехнологічним та комп'ютерним злочинам і боротьби з ними" вживається термін "традиційні злочини": *"Використання нових технологій у злочинних цілях призвело до виникнення абсолютно нових форм злочинності. З іншого боку, більш традиційні злочини в даний час вчиняються новими методами, які дають змогу збільшити вигоди або знизити ризики для злочинців"* [11].

Зарубіжні вчені, зокрема доктор Майк Макгуайр та Саманта Даулінг (Англія), також уважають, що кіберзлочинність є загальним терміном, що використовується для опису двох різних, але тісно пов'язаних між собою злочинних діянь: кіберзалежні та кіберутворюючі (злочини, пов'язані з кіберпростором).

Кіберзалежні – це злочини, які вчиняються з використанням комп'ютерів,

комп'ютерних мереж чи інших комунікаційних форм ІКТ. Такі, наприклад, як поширення вірусів та інших шкідливих програм, DDoS атаки, зламування серверів для захоплення мережевої інфраструктури або веб-сторінок. Кіберзалежні злочини спрямовані на пошкодження комп'ютерів та джерел мережі.

Кіберутворюючі (злочини, пов'язані з кіберпростором) – це традиційні злочини, масштаби яких збільшуються або досягаються за допомогою комп'ютерів, комп'ютерних мереж або інших ІКТ. На відміну від кіберзалежних злочинів, вони все ще можуть бути вчинені без використання ІКТ [12].

Отже, щодо класифікації кіберзлочинів, можна дійти висновку, що більшість дослідників, які вивчають проблему кіберзлочинності, пропонують поділяти кіберзлочини на види залежно від об'єкта та предмета посягання:

– нові злочини, що стали можливими завдяки новітнім комп'ютерним технологіям (злочини, передбачені розділом XVI Кримінального кодексу України);

– традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету.

В Україні найбільш повно статистичні дані про кіберзлочини відображаються у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України (у розд. XVII "Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції", де, крім злочинів, окреслених розд. XVI КК України, зазначається ще низка інших злочинів, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176 "Порушення авторського права і суміжних прав" і ст. 185 "Крадіжка", чч. 3 і 4 ст. 190 "Шахрайство", ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення", ст. 229 "Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару" і ст. 231 "Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю", чч. 3, 4 і 5 ст. 301 "Ввезення, виготовлення, збут і розповсюдження порнографічних предметів" КК України.

Крім цього, окремі показники про обліковані кіберзлочини, передбачені іншими статтями КК України, відображені в інших статистичних звітах, зокрема злочини, передбачені ст. 376-1 "Незаконне втручання в роботу автоматизованої системи документообігу суду" – в Таблиці 1.19 ("Злочини проти правосуддя") у Єдиному звіті про кримінальні правопорушення, який готується Генеральною прокуратурою України (за 2019 рік обліковано 34 кримінальні правопорушення).

У розділі II "Участь служб та підрозділів Національної поліції у розкритті кримінальних правопорушень (за видами), досудове розслідування за якими закінчено" (Звіт про результати роботи підрозділів Національної поліції України (форма № 1-АВ)) кіберполіцією у 2019 році розкрито (розслідувано) кримінальних правопорушень, передбачених статтями КК України:

– ст. 156 "Розбещення неповнолітніх" – 15;

– ст. 191 "Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем" – 16;

– ст. 357 "Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження" – 11.

У розділі V "Відомості про окремі види кримінальних правопорушень, що зареєстровані у звітному періоді, та окремі показники результатів роботи по боротьбі з наркоманією" зазначено, що у 2019 році виявлено 421 факт збуту наркотичних засобів, психотропних речовин або їх аналогів, а також отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів із використанням всесвітньої мережі Інтернет.

Варто зазначити, що об'єктивна сторона, суб'єкт, суб'єктивна сторона, кваліфікований та особливо кваліфікований склад злочину, передбаченого ст. 301 КК України, у цілому збігаються з відповідними ознаками посягання, предметом якого є твори, що пропагують культ насильства і жорстокості (ст. 300 КК України). При цьому кримінальні правопорушення, передбачені ст. 301 КК України, вчинені з використанням високих інформаційних технологій, враховуються у звіті, а передбачені ст. 300 КК України – не враховуються.

Отже не всі традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету, відображаються у звітах як кіберзлочини.

Частина вітчизняних науковців до кіберзлочинів відносять злочини, передбачені статтями розділу XVI КК України та злочини, показники про які відображаються у звіті Національної поліції України "Звіт про результати роботи підрозділів Національної поліції України" (у розд. XVII "Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції").

Водночас деякі науковці, зокрема професор Савченко А.В., вважають, що крім кримінальних правопорушень, зазначених у вищевказаному звіті, під категорію кіберзлочинів можуть підпадати й інші злочини, передбачені КК України, за умови, що знаряддям їх вчинення будуть інформаційні мережеві технології та (або) їх наслідки позначатимуться у кіберпросторі [13].

До кіберзлочинів можуть належати такі злочини:

– дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України);

– посягання на територіальну цілісність і недоторканність України (ст. 110);

– державна зрада (ст. 111);

– диверсія (ст. 113);

– шпигунство (ст. 114);

– розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132);

– незаконне розголошення лікарської таємниці (ст. 145); надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (ч. 1 ст. 158);

– порушення таємниці голосування (ст. 159);

– порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через Інтернет) (ст. 161);

– порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163);

– розголошення таємниці усиновлення (удочеріння) (ст. 168);

– порушення недоторканності приватного життя (ст. 182);

– розголошення комерційної або банківської таємниці (ст. 232);

– завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259);

– незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (в частині збуту через Інтернет) (ст. 263);

– заклики до вчинення дій, що загрожують громадському порядку (ст. 295);

– ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300);

– сутенерство або втягнення особи в заняття проституцією (ст. 303);

– незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307);

– викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через Інтернет) (ст. 312);

– викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (в частині збуту через Інтернет) (ст. 313);

розголошення державної таємниці (ст. 328); передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330);

– погроза або насильство щодо працівника правоохоронного органу (ст. 345);

– погроза або насильство щодо журналіста (ст. 345–1);

– погроза або насильство щодо державного чи громадського діяча (ч. 1 ст. 346);

– погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (ч. 1 ст. 350);

– незаконне втручання в роботу автоматизованої системи документообігу суду (ч. 1 ст. 376);

– розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381);

– розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387); погроза або насильство щодо захисника чи представника особи (ч. 1 ст. 398);

– розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422);

– пропаганда війни (ст. 436);

– виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 4361).

Варто також вказати на існування певних проблемних питань кваліфікації кіберзлочинів. Як зазначають фахівці, основним критерієм відмежування злочинів, передбачених статтями 361 – 363-1 КК України, від інших злочинів, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу вчинення злочину, є об'єкт посягання. Так, особливістю кримінально-правової кваліфікації злочинів проти власності,

вчинюваних із використанням комп'ютерної техніки, визнається необхідність вирішення питання про доцільність додаткової кваліфікації дій винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. Відповідаючи на це питання, слід керуватися тим, що використання комп'ютерної техніки при вчиненні злочинів проти власності утворює самостійний склад злочину лише тоді, коли заподіяно певну шкоду відповідному об'єкту – відносинам власності на комп'ютерну інформацію, коли певну інформацію було незаконно знищено, блоковано, модифіковано. А в тих випадках, коли певні інформаційні системи використовуються за призначенням, додаткова кваліфікація не потрібна [14].

Також наразі існує проблема кримінально-правової кваліфікації дій, які користувачі комп'ютерів вчиняють у сфері обігу криптовалют та застосування штучного інтелекту.

Так, у березні 2018 р. дослідники з університету RWTH Aachen University (Німеччина) виявили, що блокчейн Bitcoin містить близько 1600 файлів, де є сцени жорстокого поводження з дітьми, при цьому не менше 8 файлів є порнографічним контентом. Блокчейн містить зовнішні посилання на 274 відеофайли, присвячені жорстокому поводженню з дітьми, та близько 142 посилань на darkweb. За словами вчених, знахідка може поставити блокчейн поза законом, водночас на сьогодні не існує жодних судових постанов з цього приводу, очевидно через складність кримінально-правової кваліфікації. Усі, хто бере участь у процедурі майнінгу або володіє біткоїнами, можуть бути причетними до появи порнографічного контенту в ланцюзі [15].

На практиці у працівників правоохоронних та судових органів виникає багато проблем щодо кваліфікації кіберзлочинів. Особливо це стосується випадків вчинення такого виду злочинів, що посягають на декілька об'єктів, охоронюваних кримінальним законом.

Найчастіше помилки зустрічаються при кваліфікації одного діяння, яке, на перший погляд, містить ознаки декількох складів злочинів. Отже, основною проблемою, вирішення якої впливає на правильність кваліфікації кіберзлочинів, є визначення наявності або відсутності у вчиненому ідеальної сукупності злочинів.

Під час вчинення кіберзлочину шкода може завдаватися: 1) суспільним відносинам, які виникають в ході забезпечення (за допомогою ІТС) життєдіяльності людини, суспільства, держави; 2) традиційним суспільним відносинам, охоронюваним кримінальним законом, які забезпечуються за допомогою ІТС; 3) традиційним суспільним відносинам, охоронюваним кримінальним законом, для нанесення шкоди яким використовуються ІТС, які, у свою чергу, не зазнають при цьому шкоди.

Перша група відносин охороняється розділом XVI Особливої частини КК України. Ці відносини є частиною другої та третьої групи відносин, але в другій групі вони зазнають шкоди разом із традиційними відносинами кримінально-правової охорони, а в третій – ні.

Ідеальною сукупністю злочинів вважається два або більше злочини, вчинені одним діянням. Відповідно до вказаних груп відносин, що зазнають шкоди при вчиненні такого діяння у випадку вчинення кіберзлочину, можна виділити три групи цих злочинів, що будуть мати свої особливості кваліфікації відповідно до діючого КК України: 1) злочини в сфері використання ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж, мереж електрозв'язку; 2) злочини, що кваліфікуються за ст. КК України відповідно до об'єкту посягання з додатковим посиланням на статті розділу XVI ОЧ КК України; 3) злочини, що кваліфікуються за статтями КК України відповідно до об'єкту посягання без додаткового посилання на статті розділу XVI КК України.

Тобто діяння з першої та третьої групи є одиничними злочинами, а з другої – ідеальною сукупністю злочинів. Але в практиці застосування норм КК України в протидії кіберзлочинам діяння, що відносяться до різних із вказаних груп, часто плутаються. Найчастіше, злочини другої групи кваліфікуються тільки за однією статтею, і навпаки, злочини першої чи третьої групи кваліфікуються за декількома статтями, хоча не потребують додаткової кваліфікації. При цьому стаття, яка застосовується при кваліфікації другої групи злочинів, або із розділу XVI КК України , або інша – відповідно до безпосереднього об'єкту посягання. Очевидно, що в обох цих випадках частина злочину кваліфікацією не охоплюється, що порушує принципи повноти і точності кваліфікації, а у разі кваліфікації одного діяння, яке містить один склад злочину, за двома статтями порушується ще й принцип заборони подвійного інкримінування.

Як свідчить узагальнення судової практики, значна частка кіберзлочинів припадає на випадки, коли посягання в сфері використання ІТС здійснюється з корисливих мотивів з метою викрадення чи заволодіння чужим майном із заподіянням матеріальної шкоди і є способом вчинення таких злочинів проти власності, як шахрайство (ст. 190 КК України) або привласнення чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК України). У більшості випадків суди кваліфікують такі дії за сукупністю злочинів: за статтею розділу XVI КК України і тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було використання ІТС.

Наприклад, Печерський районний суд м. Києва визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток комерційного банку, як службова особа, що виконує адміністративно-господарські функції, зловживаючи своїм службовим становищем, маючи доступ до бази даних про клієнтів та їх рахунки, що містилась у його робочому комп'ютері, діючи з метою заволодіння грошовими коштами, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дубліката та банкоматів М. зняв і привласнив готівкою з рахунку клієнта грошові кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч. 4 ст.191 КК України як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах. Крім того, суд кваліфікував дії М. ще й за сукупністю з ч. 3 ст. 362 КК України, оскільки М., будучи особою, яка мала право доступу до інформації, що оброблялася на комп'ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації і заподіяло значну шкоду.

Проте в деяких випадках суди кваліфікують зазначені дії лише за статтями розділу XVI Особливої частини КК України.

Так, Красногвардійський районний суд м. Дніпропетровська визнав Є. винним за ч. 1 ст. 361 КК України і призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих мотивів, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із ЗАТ КБ "ПриватБанк" надавала послуги з прискореного перерахування платежів за комунальні послуги і мобільний зв'язок через мережу Інтернет. У результаті такої діяльності Є. протягом певного часу викрадав грошові кошти з рахунків клієнтів ЗАТ КБ "Приват-Банк".

Автори узагальнення, з якого взяті ці приклади, вважають що в останньому випадку, оскільки Є. шляхом обману неодноразово заволодівав грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання в роботу ЕОМ є способом вчинення злочину проти власності, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст. 190 КК України (шахрайство). Вважаємо,

що тут дійсно наявна сукупність злочинів, але вона вже врахована в КК України в ч. 3 ст. 190, отже потрібна кваліфікація за цією нормою без додаткових посилань на норми КК України [16].

Одною із загальних проблем кримінально-правової кваліфікації є питання кваліфікації ідеальної сукупності злочинів, а саме поглинання одного злочину іншим, який був його частиною. Ця проблема досі потребує вирішення вченими.

Т.І. Созанський формулює правило стосовно злочинів, які мають додаткові об'єкти посягання: "Якщо ці об'єкти співвідносяться як основний і додатковий, то діяння кваліфікується як одиничний злочин, якщо ж обидва (чи більше) об'єкти є основними, то діяння утворює ідеальну сукупність злочинів". Але далі він вказує, що визначити, коли об'єкт є додатковим, а коли він переходить у основний, особливо при оцінці кіберзлочину, доволі складно. Він пропонує, як один із варіантів вирішення цього питання, визначати суспільну небезпечність посягань на відносини, які охороняються цими об'єктами. Якщо суспільна небезпечність відносин, що охороняються додатковим об'єктом, є більшою, ніж основного об'єкта, то діяння утворює ідеальну сукупність [17].

У практичну площину цю рекомендацію перевів Пленум Верховного Суду України у постанові, яка стосується судової практики застосування норм про множинність злочинів. У п. 11 цієї постанови вказано: "Якщо у складі злочину передбачене діяння, яке у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання про його кримінально-правову оцінку необхідно вирішувати з урахуванням того, наскільки охоплюється складом цього злочину таке діяння, а також з урахуванням змісту санкцій відповідних статей (частин статей) ОЧ КК України. У випадках, коли складом певного злочину охоплюється вчинене одночасно з цим злочином відповідне діяння і санкцією статті (частини статті) ОЧ КК України встановлене за цей злочин більш суворе максимальне основне покарання, ніж за відповідне діяння, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує".

Таким чином, слід визнати за правило кваліфікації кіберзлочинів, які через посягання на відносини в сфері використання ІТС посягають на інші "традиційні" відносини, які забезпечуються цими ІТС, наступне: у разі, коли складом певного злочину охоплюється вчинене одночасно з цим злочином діяння, передбачене статтею Розділу XVI і санкцією статті (частини статті) КК України встановлене за цей злочин більш суворе максимальне основне покарання, ніж за діяння, передбачене статтею Розділу XVI КК України, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує.

Висновки.

Сьогодні офіційного, закріпленого в міжнародних документах визначення кіберзлочинності поки не існує. Класифікації кіберзлочинів, які надаються в офіційних документах, зокрема ООН, ЄС, та дослідженнях науковців, через які розкривається поняття кіберзлочинність також різняться.

У вітчизняному законодавстві нині також не існує чіткого визначення поняття кіберзлочину. Дискутуються різні точки зору щодо класифікації кіберзлочинів. Відсутній перелік "традиційних" злочинів, які можуть відноситися до категорії кіберзлочинів, а отже і відсутня офіційна статистична звітність щодо облікованих кіберзлочинів.

Отже, сьогодні є нагальна потреба визначитися з переліком "традиційних" злочинів, які можуть відноситися до категорії кіберзлочинів, внести зміни до відомчої статистичної звітності Національної поліції України.

Аналіз такої статистичної звітності надав би можливість проаналізувати динаміку цього виду злочинності, структуру злочинності, стан криміногенної ситуації у цій сфері на основі облікованих злочинів та розробляти на їхній основі організаційно-правові заходи для більш ефективної протидії кіберзлочинності на національному рівні. Зокрема, для протидії вчиненню "традиційних" злочинів з використанням мережі Інтернет, відповідальність за які передбачена Кримінальним кодексом України, необхідно розробити методичні рекомендації щодо кримінально-правової кваліфікації "традиційних" злочинів, вчинених з використанням мережі Інтернет.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Законі України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

2. Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *ПРАВО.* – (Наук. вісник Ужгородського націон. ун-ту). 2016. Вип. № 36. С.123-126.

3. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб. / В.М. Бутузов та ін. – (Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з проблем боротьби з організованою злочинністю, Служба безпеки України, Нац. акад. СБУ). Київ, 2011. 404 с.

4. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний ун-т "ЗІДМУ", 2003. 296 с.

5. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі "Даркнет". *Інформація і право*. № 3(26)/2018. С. 111-117. URL: http://nbuv.gov.ua/UJRN/In fpr_ 2018_3_13

6. Демедюк С.В., Марков В.В. Кіберполіція України. *Наше право*. 2015. № 6. С. 87-93. URL: http:// nbuv.gov.ua / UJRN/ Nashp_ 2015_6_15

7. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. Вип. 1. С. 312-320. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_37

8. Столяр О. Міжнародно-правові проблеми визначення та класифікації "кіберзлочинів". URL: http://www.jurnaluljuridic.in.ua/archive/2017/4/43.pdf

9. Home Affairs Committee E-crime Fifth Report of Session 2013–14. URL:https://publications. parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf

10. Joint communication to the European parliament, the Council, the European economic and social committee and the committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 02.2013. URL: http://eur-lex.europa.eu/legal-content/EN/NOT/ ?uri=celex:52013JC0001

11. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. м. Вена, 10 – 17 апреля 2000 года. URL: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-RU.pdf; https://digitallibrary.un.org/ record/432653/files/A_CONF.187_10-RU.pdf?version=1

12. Экономический и Социальный Совет ООН. Комисся по предупреждению преступности и уголовному правосудию. м. Вена, 8 – 17 мая 2001 года. URL: https://www.google. com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjGip3Ys8Df AhXQp4sKHTltB9wQFjAAegQICBAC&url=https%3A%2F%2Fwww.unodc.org%2Fdocuments%2Fc ommissions%2FCCPCJ%2FCCPCJ_Sessions%2FCCPCJ_10%2FE-CN15-2001-04%2FE-CN15-2001-4_R.pdf&usg=AOvVaw1dtJrz_5oLSWMd4q4AwGnb

13. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications. URL: https://assets.publishing.service.gov.uk/government/uploads/ system/uploads/attachment_data/file/246749/horr75-summary.pdf

14. Науково-практичний коментар Закону України “Про основні засади забезпечення кібербезпеки України” / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

15. У блоках Bitcoin виявили сліди дитячої порнографії. URL: https://www.Volyn news.com/news/all/u-blokakh-Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi-

16. Узагальнення щодо кваліфікації сукупності злочинів. – (Опрацьовано суддею Верховного Суду України М.І. Грицівим та головним консультантом управління вивчення та узагальнення судової практики Верховного Суду України В.В. Антощуком). URL: http://www. viaduk.net/clients/vsu/vsu.nsf/(documents) /AFB1E90622E4446FC2257B7C00499C02

17. Созанський, Т.І. Кваліфікація сукупності злочинів: автореф. дис. ...канд. юрид. наук : 12.00.08. – (Львів. держ. ун-т внутр. справ). Львів, 2009. 18 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~