ПИВОВАРОВ В. В.,
кандидат юридичних наук,
доцент кафедри кримінології
та кримінально-виконавчого права
(Національний юридичний університет імені Ярослава Мудрого)

ЛИСЕНКО С. Ю.,
студент V курсу
(Інститут прокуратури та кримінальної юстиції Національного юридичного університету імені Ярослава Мудрого)

УДК 343.9

КІБЕРЗЛОЧИННІСТЬ: КРИМІНОЛОГІЧНИЙ ПОГЛЯД НА ГЕНЕЗИС ЯВИЩА ТА ШЛЯХИ ЗАПОБІГАННЯ

Стаття присвячена кримінологічним аспектам явища кіберзлочинності на національному й міжнародному рівнях, її основним суспільно-економічним чинникам. Обґрунтовується думка щодо транснаціонального, корпоративного характеру світової кіберзлочинності.

Ключові слова: *кіберзлочинність, ціна кіберзлочинності, транснаціональна й корпоративна злочинність.*

Статья посвящена криминологическим аспектам явления киберпреступности на национальном и международном уровнях, её основным общественно-экономическим факторам. Обосновывается мысль о транснациональном, корпоративном характере мировой киберпреступности.

Ключевые слова: *киберпреступность, цена киберпреступности, транснациональная и корпоративная преступность.*

The article is devoted to criminological aspects of the phenomenon of cybercrime at national and international levels, its main socio-economic factors. The idea of transnational and corporate nature of the global cybercrime is being substantiated.

Key words: *cybercrime, value of cybercrime, transnational and corporate crime.*

Вступ. Процеси всесвітньої глобалізації, у тому числі глобалізації інформаційних технологій, з одного боку, нівелюють кордони між територіями держав світу й надають необмежені можливості для вчинення будь-якого впливу на особистість і суспільство, однак, з іншого боку, одним із негативних наслідків глобалізації стала поява й розвиток нового явища злочинності – злочинності у сфері інформаційних технологій.

Зазначимо, що обговорення цього питання серед кримінологів актуалізувалося понад 17 років тому. І вже тоді вчені констатували, що зростання комп'ютерних протиправних зазіхань перестає бути далекою перспективою. Проблема комп'ютерної злочинності набуває яскраво вираженого міжнародного характеру. Виникає необхідність міжнародного співробітництва, створення спеціалізованих підрозділів або цілеспрямованих сил, що володіють професійними знаннями, досвідом, владними повноваженнями для найкращого вирішення завдань у цій сфері злочинності [1].

Очевидно, для України, яка перебуває в постіндустріальному періоді розвитку та процесі лібералізації економіки, проблема так званої «кіберзлочинності» актуалізується з кожним роком, тому що комп'ютери й телекомунікаційні системи охопили всі сфери життєдіяльності людини та держави: інтернет-уряд (e-government), інтернет-банкінг, интернет-охорона здоров'я, інтернет-освіта, нові автоматизовані покоління енергомереж, автоматизовані елементи транспортної інфраструктури, впровадження 3G/4G(LTE) технологій, створення кіберполіції тощо. Тільки за фактами потужних кібератак в Україні практики й учені стали більш активно обговорювати питання інформаційної безпеки. Зломи й атаки ставались і раніше, але тоді вони мали напіваматорський характер і були нечастими, а зараз Україна зіштовхнулась із потужним кіберсупротивом. Нещодавно прийнята стратегія кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в правомірних і моральних інтересах особистості, суспільства й держави, уже встигла стати предметом для дискусій серед фахівців. Зауважують, що стратегія лише визначає перелік напрямів (векторів), у яких державні інституції повинні діяти, щоб убезпечити країну від нових ударів із кіберпростору.

Постановка завдання. Метою статті є визначення кримінологічного генезису сучасного явища кіберзлочинності у вітчизняному й міжнародному контексті й шляхів запобігання йому.

Результати дослідження. Викладене у вступі переконливо свідчить на користь висновку про те, що в Україні якраз «розцвітає» кіберзлочинність. Наочними чинниками цього, звісно, є як банальна безтурботність і необізнаність громадян, а також занадто ліберальне й недосконале кримінальне законодавство у сфері кібершахрайства. Але існує низка важливіших і більш глобальних чинників. Таке становище спонукає науку кримінології до вивчення цього явища, розвитку категоріального апарату тощо.

Ми вважаємо, що кіберзлочинність – це сукупність злочинів, учинених у кіберпросторі за допомогою або з опосередкованим використанням комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у межах комп'ютерних систем або мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Відзначимо, що запропонована нами наукова дефініція відповідає критеріям експертів ООН. На їхню думку, термін «кіберзлочинність» охоплює будь-який злочин, який може відбуватися за допомогою комп'ютерної системи або мережі, у межах комп'ютерної системи або мережі чи проти комп'ютерної системи або мережі. Отже, до кіберзлочинів може бути зарахований будь-який злочин, учинений в електронному середовищі [2]. Поняття «кіберзлочинність» і «комп'ютерна злочинність» дуже близькі одне до одного, але не синонімічні. Термін «кіберзлочинність» більш широкий за змістом, ніж поняття «комп'ютерна злочинність», оскільки позначає злочинність, пов'язану як із використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж, тоді як термін «комп'ютерна злочинність» уживається тільки до злочинів, які відбуваються проти комп'ютерів або комп'ютерних даних. У міжнароднім законодавстві аналогічно вживається термін «cybercrime», однак не «computer crime» (Конвенція про кіберзлочинність, прийнята Радою Європи 2001 року, ратифікована Україною в 2005 році). До речі, і чинний Кримінальний кодекс України (розділ XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку») також потребує законодавчих термінологічних правок.

Сьогодні жертвами злочинців, котрі злочинно орудують у віртуальному просторі, можуть стати не тільки окремі громадяни, а й держави. Статистично кількість злочинів, що вчиняються в кіберпросторі, зростає прямо пропорційно кількості інтернет-користувачів (наприклад, щодо кількості користувачів: 2008 рік – 1,5 млрд осіб, 2013 рік – 2,3 млрд осіб, 2015 рік – 3,4 млрд осіб, за прогнозами фахівців, до 2017 року доступ отримають близько 70% від загальної кількості населення світу) [3]. Також варто згадати про ціну кіберзлочинності в її динаміці за останні роки. Так, Symantec – компанія, що спеціалізується на розробці програмного забезпечення в галузі інформаційної безпеки й захисту інформації, наводить такі дані: за 2012 рік від дій кіберзлочинців постраждали 556 млн користувачів «усесвітньої павутини». Сукупні

втрати становили близько 110 млрд доларів США. У своїй звітності за 2015 рік компанія надає суспільству уявлення про цінову політику, яка існує на тіньовому ринку протиправних послуг (наприклад, Ddos атаки – від 10 до 1000 доларів США на день, розробка шкідливого ПЗ для крадіжки платіжних реквізитів – 3 500 доларів США, використання спаму для заволодіння 1000 e-mail – від 0,5–10 доларів США, інші не менш цікаві відомості) [4]. А за підрахунками Mcafee, Incorporated – підрозділу американської компанії Intel Security, втрати від кіберзлочинності за 2013 рік досягли вже 500 млрд доларів США [5].

Однак найбільша частина кіберзлочинності залишається поза межами статистики. Можна погодитися з думкою, що в офіційну статистику потрапляє в найкращому випадку до 20% злочинних діянь, а то й менше. У нашій країні за 2009 рік було зареєстровано 96 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів) в автоматизованих системах, комп'ютерних мережах, у 2010 році – 87, у 2011 році – 67, у 2012 році – 83, у 2013 році – 408, а у 2014 році – 140 злочинів, відповідно [6]. Така «коливальна» статистика очевидно не корелює із прогресивним зростанням кількості інтернет-користувачів, темпи якого значно прискорилися з масовим упровадженням 3G технології передавання даних і нав'язаним виробниками тотальним переходом загалу користувачів послуг рухомого голосового зв'язку на новий технічний рівень портативних комп'ютерів (смартфонів), замість функціонально обмежених, але достатніх для потреб цього сегмента споживачів простих «звонілок» (пенсіонери, малолітні, жителі сільської місцевості, особи низького освітнього і професійного рівня тощо). Уважаємо, що сьогодні офіційна статистика відображає аж ніяк не стан кіберзлочинності, а скоріше стан її реєстрації або стан спроб її реєстрації.

Соціальні втрати від кіберзлочинності вражають. За експертними оцінками, економіки країн Великої двадцятки (G20) втратили загалом близько 2,5 млн робочих місць через поширення контрафактної й піратської продукції, а уряди й споживачі втрачають через кіберзлочинців до 125 млрд доларів США податкових надходжень щороку [7]. Експерти із США оцінюють збиток економіці своєї країни від крадіжок інтелектуальної власності в 300 млрд доларів США щорічно, що відповідає 1% ВВП країни [8]. Інші дослідження, які проводились у Нідерландах, Великобританії й Німеччині, надають схожі за рівнем оцінки втрати ВВП цих країн. З усе більшим поширенням інтернету й розвитком інформаційних технологій ризик таких втрат, супутні ризики й економічні збитки будуть зростати експонентно, якщо безпека й стабільність системи не будуть закладені в саму основу стратегій упроваджуваної інформаційної модернізації.

В Україні територіальний розподіл цього виду злочинів схематично такий: найбільша кількість злочинів за період 2009–2012 років була зареєстрована в Дніпропетровській, Донецькій, Запорізької областях, а в 2013–2014 роках – у містах Київ, Одеса, Дніпропетровськ. В окремих областях України такі злочини не реєструвалися взагалі (Хмельницька, Закарпатська, Чернівецька області).

На окрему увагу заслуговує такий протиправний феномен сучасності, як «кібервійна». Ні для кого сьогодні не є особливим секретом той факт, що давно в інтернет-просторі точиться боротьба за свідомість і настрої громадян, практикується різного роду шпигунство. Прийняття Україною вищезгаданої Стратегії, відновлення доктрини кібербезпеки в РФ, наміри країн під панування ООН підписати документ із умовною назвою «Пакт про електронний ненапад» лише підтверджують факт занепокоєння й побоювання урядів країн світу в цій сфері. Потужна атака в кіберпросторі здатна паралізувати й заблокувати найбільш важливі сегменти телекомунікаційної мережі в країні, дестабілізувати банківську систему та економіку держави загалом. Як приклад можна згадати доволі часті атаки на фінансові установи (сайти, внутрішні мережі, створення сайтів-двійників для викрадення конфіденційних даних), урядові заклади (так, у 2014 році в Україні був серйозно атакований Центрвиборчком), об'єкти інфраструктури (у 2015 році відключення енергомереж АЗС в Україні пояснили кібератакою). Яскравим прикладом, який ілюструє небезпеку на наддержавному, світовому рівні, є історія із вірусом «Stuxnet», який був створений для знищення ядерних центрифуг іранської ядерної програми. Через низку помилок у програмах він проникав у си-

стему керування й відправляв двигунам центрифуг команди, що призводили вихід останніх із ладу. Навряд чи варто пояснювати потенційну загрозу потрапляння такого програмного продукту у володіння будь-якої терористичної організації. Під загрозою опинились також і установи охорони здоров'я. Вони крокують у ногу з часом і сміливо впроваджують у свою інфраструктуру новітні технології, які дають змогу поліпшити якість обслуговування, досягти мультикерованості методів лікування, дистанційно стежити за станом здоров'я своїх пацієнтів. Незважаючи на весь цей прогрес, тут існує зворотний бік медалі. До подібних технологій (наприклад, електронні крапельниці, кардіостимулятори) можливо одержати несанкціонований доступ, і зробити непоправне – позбавити людину життя. Усім знайома й широко рекламована на сьогодні система «Розумний будинок», яка керує вашим будинком (квартирою або офісом), звісно, заощаджує ваш час, кошти на опалення й електроенергію. Дистанційне відкриття цифрового замка, доступ до встановлених камер спостереження, одержання доступу до сигналізації (для її відключення), крадіжка цифрових даних, інсценування пожежі, затоплення приміщення та інші негаразди – усього лише мала частина ціни прогресу у випадку зламу цієї системи.

Один із найнебезпечніших різновидів кіберзлочинності – кібертероризм. На відміну від традиційного, цей вид тероризму використовує в терористичних акціях новітні досягнення науки й техніки в галузі комп'ютерних і інформаційних технологій, радіоелектроніки, генної інженерії, імунології. Нині існує безліч тактичних схем, у межах яких терористичні групи використовують інтернет у своїх цілях (збір грошей для підтримки терористичних рухів; створення сайтів із докладною інформацією про терористичні рухи, їхні цілі й завдання, публікація на цих сайтах даних про час і зустрічі людей, зацікавлених у підтримці терористів; використання інтернету для інформаційно-психологічного впливу, у тому числі ініціація «психологічного тероризму», тощо).

Інтегрування інноваційних технологій у промисловість вимагає високого рівня безпеки, тому що у випадку несанкціонованого доступу в систему виробництва виникає загроза масового забруднення навколишнього середовища та навіть загроза загибелі працівників і появи техногенних жертв серед населення. Сучасних аварійно небезпечних виробництв в Україні достатньо: атомні електростанції, хімічні виробництва, склади особливо токсичних і отруйних речовин, військові об'єкти.

Викладені вище основні напрями кіберзагроз для суспільства, попри їх зовнішню різноманітність (від банківського шахрайства до тероризму), мають, на нашу думку, одну принципово схожу рису. Кіберзлочинність – це явище, яке за природою свого існування практично виключає індивідуальну злочинну дію, яка тривалий час розглядалась у радянській і пострадянській кримінології через призму механізму індивідуальної злочинної поведінки. Також ми не можемо в цьому питанні обмежитись уявленнями про традиційну співучасть у злочині чи її більш деталізовані кримінальним законом форми, оскільки такий погляд штучно стримує кримінологічний погляд на природу кіберзлочинності. Усі наведені форми і способи вчинення кіберзлочинів, здобуті нами емпіричним шляхом із відкритих джерел, свідчать про «надгруповий», корпоративний характер кіберзлочинності, який яскраво підкреслюється їх транснаціональними виявами. Сучасна кримінологія зібрала ще недостатньо відомостей про особу кіберзлочинця. Однак можемо вважати, найбільш резонансні, масштабні, тяжкі за наслідками і нерозкриті кіберзлочини очевидно вчиняються не одинаками – «злочинними романтиками». Останні, можливо, існують, але в катастрофічній меншості на тлі загальної кількості добре організованих, спланованих і профінансованих кіберзлочинів. Справжню ж загрозу становлять ті злочини та злочинці, за якими вбачається корпоративний, транснаціональний, геополітичний інтерес: промислове й військове шпигунство в галузі високих технологій, «війна за розуми», усунення конкурентів на ринку товарів чи послуг, боротьба злочинними методами за ресурсні території, за лідерство в освоєнні навколоземного простору тощо. Традиційне, енциклопедичне розуміння корпорації як об'єднання приватних капіталів із наступним утворенням юридичної особи на сучасному етапі світового розвитку є надто звуженим і абстрагованим. Варто звернути увагу на дві здавна відомі мети ство-

рення корпорацій: отримання прибутку (приватні цілі) та перехоплення окремих державних функцій (публічні цілі) [9, с. 47–48]. У контексті тенденцій світової глобалізації позначені цілі корпорації діють синергетично, взаємно підсилюючи одна одну: збільшення капіталу збільшує владний вплив, а зростання влади продукує поглинання і примноження капіталів.

З огляду на наведене доходимо висновку, що саме корпорації переважно контролюють інформаційний і технічний сегменти «всесвітньої мережі», адже очевидно, що за своєю природою ця мережа є недержавною й наддержавною, і це не означає її неконтрольованості чи анонімності, скоріше зовсім навпаки. Корпорації-виробники програмного забезпечення й обчислювальних пристроїв взаємодіють між собою, контролюючи свої сегменти і стимулюючи один одного. Ніби для мети технічного прогресу, накопичуються величезні банки даних постійного зберігання, і вже зараз учені-цивілісти всерйоз обговорюють право особистості на «цифрове забуття». Усе перелічене й подібне в контексті віртуального функціонування особи, економіки та держави дає нам ґрунтовні підстави стверджувати, що за природою свого походження кіберзлочинність не є стихійним явищем, яке, за традиційною кримінологічною схемою, нібито складається з непов'язаних між собою індивідуальних протиправних вчинків. Скоріше навпаки: на рівні суспільного світового устрою це система цілеспрямованих дій, контрольованих і організованих на наддержавному, транснаціональному рівні. Держава як утворення класичних владних інститутів часто залишається «поза грою» в намаганнях протистояти кіберзлочинності, оскільки «поле гри» є приватним, однак шкода завдається тотальна – національна, міжнародна, світова.

Надміру високою є латентність кіберзлочинів, і ця обставина істотно перешкоджає як науковому осмисленню явища, так і практичній боротьбі з ним. Першочерговими чинниками латентності вважаємо такі: 1) слабку оснащеність правоохоронних органів засобами комп'ютерної техніки, низька кваліфікація співробітників правоохоронних органів. За умови транснаціонального характеру діяння навіть технічна фіксація самої злочинної дії, наслідків і зв'язку між ними перетворюються на серйозну проблему; 2) високий рівень технічної кваліфікації й технічного прикриття осіб, які є виконавцями злочину.

Висновки. Як обґрунтовувалось вище, кіберзлочинність має за своєю природою транснаціональний і корпоративний характер. Розуміння генезису цього виду злочинності ставить перед науками соціального та юридичного напряму, у тому числі перед наукою кримінології, комплексне завдання щодо першочергового створення державних концепцій кібербезпеки держави, закріплення поняття, місця й норм державності в кіберпросторі, а на їх основі – стратегій боротьби з кіберзлочинністю, ужиття рішучих організаційних, новаторських дій щодо створення спеціалізованих поліцейських підрозділів кібербезпеки. Як зазначалось, це завдання комплексне. Тому фахівцям-науковцям потрібно на упередження розглядати необхідність унесення змін до системоутворювальних законів і конституцій держав.

На сучасному етапі боротьба зі злочинністю з використанням міжнародних комп'ютерних мереж ускладнюється, за оцінками експертів ООН, унаслідок трьох основних причин: 1) для розслідування злочинів в електронному середовищі потрібні спеціальні знання й досвід; 2) інтернет являє собою відкрите середовище, що надає користувачам можливості виконувати певні дії за межами кордонів держави, ігноруючи територіальну кримінальну юрисдикцію; 3) відкриті структури міжнародних комп'ютерних мереж дають користувачам змогу вибирати для свого фізичного перебування такі країни, у яких діяння, учинені в електронному середовищі, не тягнуть відповідальності. Наявність «інформаційних притулків» може стримувати зусилля інших держав щодо боротьби зі злочинністю з використанням комп'ютерних мереж [2].

Перспективно необхідні радикальні заходи загальносоціального й спеціально-кримінологічного характеру, спрямовані на оздоровлення соціального середовища проживання людей, поступова зміна ідеології людського існування від орієнтації на споживання й соціальний паразитизм до установки на самовдосконалення особистості й соціальну користь існування індивіда, формування законослухняного громадянина, а також на оперативне професійне втручання в злочинну діяльність. Багато із цих заходів тривалі, економічно обтяжливі, вимагають нетрадиційного підходу й нових ідеологічних державних рішень [1].

Погрози кіберзлочинності реальні й стають усе більш серйозними. Виникає необхідність правового врегулювання питань кібербезпеки як на національному, так і на міжнародно-правовому рівнях. В Україні зараз відсутні комплексні дослідження з питань кіберзлочинності як явища, що охоплюють собою весь спектр злочинів, учинених у глобальних інформаційних мережах. Дослідження показує, що серед заходів запобігання злочинам у кіберпросторі найбільш дієвими варто вважати технологічні, організаційні і правові комплекси. Перші кроки зроблені, і сподіваємось, що створення кіберполіції в нашій державі вплине на рівень цих злочинів, підтвердженням чого стануть позитивні зрушення в офіційних статистичних джерелах.

Список використаних джерел:

1. Голина В.В. Проблемы в компьютерной преступности / В.В. Голина, В.В. Пивоваров // Фінансова злочинність : зб. матеріалів Міжнар. наук-практ. семінару, Харків 12–13 лют. 1999 р. / редкол.: В.І. Борисов (голов. ред.) та ін. – Х. : Право, 2000. – С. 62–73.

2. Преступления, связанные с использованием компьютерной сети. Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями [Электронный ресурс]. – Режим доступа : http://www.un.org/russian/topics/crime/docs10.htm.

3. World Internet Usage [Електронний ресурс]. – Режим доступу : http://www.internetworldstats.com/stats.htm.

4. 2015 Internet security threat report. By Symantec [Електронний ресурс]. – Режим доступу : https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.

5. 2013 Threats Predictions. By McAfee Labs. Report [Електронний ресурс]. – Режим доступу : http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf.

6. Статистична звітність форми № 1 (річна) «Єдиний звіт про злочинність» // Офіційний веб-сайт Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу : http://www.mvs.gov.ua.

7. Frontier Economics London, Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy: A Report commissioned by Business Action to Counterfeiting and Piracy (London, Frontier Economics Ltd, 2011): 47.

8. The National Bureau of Asian Research, “The IP Commission Report: The report of the commission on the theft of American intellectual property,” National Bureau of Asian Research (May 2013) [Електронний ресурс].. – Режим доступу : http://www.lingvo-online.ru/ru/Search/Translate/GlossaryItemExtraInfo?text=%d0%ba%d0%b8%d0%b1%d0%b5%d1%80%d0%bf%d1%80%d0%b5%d1%81%d1%82%d1%83%d0%bf%d0%bd%d0%be%d1%81%d1%82%d1%8c&translation=cybercrime&srcLang=ru&destLang=en.

9. Большая советская энциклопедия : в 51 т. – 2-е изд. – М. : Советская энциклопедия, 1953. – Т. 23 : Корзинка – Кукунор / гл. ред. Б.А. Введенский. – 1953. – 636 с.