Юридичні науки

УДК 343.9

Степлюк Катерина Вячеславівна

студентка

Національного юридичного університету імені Ярослава Мудрого

Степлюк Екатерина Вячеславовна

студентка

Национального юридического университет имени Ярослава Мудрого

Stepliuk Ekateryna

Student of the

Yaroslav Mudryi National Law University

Науковий керівник:

Ткачова Олена Вікторівна

кандидат юридичних наук,

доцент кафедри кримінології та кримінально-виконавчого права

Національний юридичний університет імені Ярослава Мудрого

КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ: СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ
КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА: СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ
CRIMINOLOGICAL CHARACTERISTIC OF CYBERCRIME: CURRENT STATE AND TRENDS OF DEVELOPMENT

Анотація. *У статті автор розглядає і аналізує роль та місце явища кіберзлочинності у сучасному світі. Наведено кількісні і якісні кримінологічні показники кіберзлочинності шляхом аналізу даних статистичної звітності Генеральної прокуратури України за січень-жовтень 2018 року. Особлива увага приділяється характеристиці*

портрету комп'ютерного злочинця. У даній статті також розглянуто політико-правові, соціально-економічні, організаційно-управлінські та культурно-психологічні фактори детермінації кіберзлочинності. На основі отриманих результатів, зроблено відповідні висновки щодо тенденції зростання кіберзлочинів та потреби протидії таким діянням.

Ключові слова: *кіберзлочинність, кримінологічна характеристика, кіберзлочинець, фактори детермінації кіберзлочинності.*

Аннотация. *В статье автор рассматривает и анализирует роль и место явления киберпреступности в современном мире. Приведены количественные и качественные криминологические показатели киберпреступности путем анализа данных статистической отчетности Генеральной прокуратуры Украины за январь-октябрь 2018 года. Особое внимание уделяется характеристике портрета компьютерного преступника. В данной статье также рассмотрены политико-правовые, социально-экономические, организационно-управленческие и культурно-психологические факторы детерминации киберпреступности. На основе полученных результатов, сделаны соответствующие выводы относительно тенденции роста киберпреступлений и потребности противодействия таким деянием.*

Ключевые слова: *киберпреступность, криминологическая характеристика, киберпреступник, факторы детерминации киберпреступности.*

Summary. *In this article the author analyzes the role and place of the phenomenon of cybercrime in the modern world. The quantitative and qualitative criminological indicators of cybercrime are given by analyzing statistical reporting data of the General Prosecutor's Office of Ukraine for January-October 2018. Particular attention is paid to characterizing a computer offender's portrait. This article also examines political, legal, socio-*

economic, organizational and administrative and cultural-psychological determinants of cybercrime. Based on the results, the correct conclusions are made about the growth trends in cybercrime and the needs to act against such.

Key words: *cybercrime, criminological characteristic, cybercriminal, determinants of cybercrime.*

Актуальність теми дослідження. У сучасному світі все більше виробництв і послуг спираються на інформаційні технології. Виробництво і постачання енергії, очищення і постачання питної води, керування транспортом, освітлення міст, зв'язку, доступ людей до інформації, охорона здоров'я, оплата товарів і послуг, волевиявлення під час виборів і референдумів, і навіть електронне урядування – все це реалії нашого життя. Ми залежимо від безперервності та коректності функціювання комп'ютерних систем об'єктів критичної інфраструктури, і атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства.

Окремі питання кіберзлочинності неодноразово були предметом наукових досліджень як вітчизняних, так і зарубіжних учених. Зокрема, цій проблематиці присвячені праці О. Амеліна, Ю. Батуріна, В. Бутузова, В. Голубєва, О. Дзьобаня, В. Дзюндзюка, Р. Калюжного, М. Карчевського, М. Кравцової, В. Лісового, В. Навроцького, В. Номоконова, Д. Пашнєва, В. Пилипчука, М. Погорецького, В. Сташиса, В. Шеломенцева, О. Юрасова та інших.

Під *кіберзлочинністю* розуміють соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності(кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [1, с. 7]. ООН під явищем кіберзлочинності розуміє будь-які злочини, що

вчиняються у комп'ютерній мережі або за допомогою неї і не має на увазі виключно складні кіберзлочини вищого порядку, що потребують для їхнього вчинення надвисоких інтелектуальних здібностей чи довготривалого планування. Прояви кіберзлочинності мають кримінально-правові межі, що визначаються переліком злочинів, ознаки яких закріплені у ст.ст.361,361¹,361²,362,363,363¹ КК України.

Варто звернути увагу, що в науковій юридичній літературі наведені такі ознаки кіберзлочинів, що відрізняють їх від «звичайних» злочинних посягань і значно підвищують їх суспільну небезпечність. По-перше, кіберзлочин не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого. По-друге, кіберзлочин є «автоматизованим» злочином (суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч). По-третє, суб'єкт кіберзлочину не підвладний обмеженням, які існують у реальному, фізичному світі. Так, кіберзлочини можуть бути вчинені моментально, а тому потребують швидкої реакції на них. По-четверте, кіберзлочинність і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це можливо стосовно злочинів, що вчиняються у реальному, фізичному світі [7, с. 130].

Сучасний стан кіберзлочинності в Україні проявляється через опис і пояснення її кількісних та якісних кримінологічних показників. Аналіз даних офіційної статистичної звітності за останні сімнадцять років свідчить про тенденцію стабільного та стрімкого зростання рівня кіберзлочинів. За звітний період січень-жовтень 2018 року абсолютна кількість зареєстрованих кіберзлочинів сягнула 2082 [2], що майже вдвічі більше за січень-жовтень 2017 року [3]. Кількість кіберзлочинів від усіх кримінальних правопорушень за звітний період становить 0,5%. Найбільшу питому вагу становлять злочини, передбачені ст.362 КК

України - 48% та 44% - злочини, передбачені ст.361 КК України. За січень-жовтень 2018 року обліковано 0 особливо тяжких кіберзлочинів та 1470 тяжких, що складають 70% від усіх зареєстрованих злочинів у цій сфері(характер злочинності) [2]. Аналіз географії кіберзлочинів в Україні виявив залежність її поширення від фактору урбанізації. Найбільша кіберкримінальна активність фіксується за ранжиром в Дніпропетровській області, м. Києві, а також Харківській, Запорізькій та Черкаській областях. Найнижча – в Чернівецькій, Херсонській, Сумській, Кіровоградській областях. Крім того, слід відзначити випадки реєстрації кіберзлочинів на залізниці (Одеська залізниця), що засвідчує поступову експансію кіберзлочинності на більшість сфер життєдіяльності нашого суспільства [1; 9]. На жаль, зазначені вище статистичні показники не відбивають реальний стан кіберзлочинності, оскільки цей різновид злочинів має високий рівень латентності. За експертними оцінками, рівень латентності кіберзлочинів становить 90-95% [1, с. 8].

Успішна боротьба з кіберзлочинами неможлива без всебічного аналізу образу мислення і особи порушника. У результаті проведеного аналізу статистичної звітності Генеральної прокуратури України за січень-жовтень 2018 року встановлено, що в більшості своїй кіберзлочинці – це працездатні, які не працюють і не навчаються (50%), чоловіки (67%), віком 18-28 років (34%), віком 29-39 років(30%), громадяни України (100%), які мають повну вищу і базову вищу освіту(57%), студенти вищих навчальних закладів(57%) та професійно-технічних навчальних закладів(43%), виявлені особи, які раніше вчиняли злочин(фактичний рецидив)(10%), з яких особи, судимість яких не знята і не погашена(юридичний рецидив)(36%) [4].

В ідеалі особу кіберзлочинця треба характеризувати щодо кожного окремого різновиду злочинів у кожній із груп, оскільки специфіка вчинення, мотивація та рівень професіоналізму у сфері комп'ютерних

технологій та комп'ютерної безпеки значно відрізняється для кожного із них. Деякі розмежовують кіберзлочинців за формою прояву на активні (кібертероризм, погрозу фізичної розправи, кіберпереслідування та кіберсталкінг) та пасивні (кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство та поширення спаму та вірусних програм) [5, с. 294]. Та деякі спільні риси портрета комп'ютерного злочинця можна виділити:

1) *фізіологічна характеристика*: можливі аутистичні розлади (синдром Аспергера), ескапізм (втеча від дійсності, прагнення піти від реальності, від загальноприйнятих норм суспільного життя у світ ілюзій та псевдо діяльності), адикція (залежність від мережевого світу у кіберзлочинця, може мати навіть прояв хворобливого стану, коли потяг до проведення усього часу у комп'ютерному просторі призводить до нехтування усіма іншими проявами матеріального та соціального життя), делінквентна поведінка (співвідноситься як частина та ціле із девіантною поведінкою і проявляється як загальна асоціальна спрямованість та схильність до порушення правил людського співжиття та вчинення правопорушень);

2) *психоемоційна складова*: високі та надвисокі інтелектуальні здібності, посидючість,здатність чекати роками результатів власних дій, бажання поглузувати з уразливості системи, певним чином самоствердитися, почуття вищості та самолюбства, скритність;

3) *мотивація та тип*: наявна корислива мета майже у всіх злочинах, отримати ігрові засоби чи викликати інші суспільні процеси [6, с. 201].

Детермінаційний комплекс кіберзлочинності репрезентований широким спектром протиріч політико-правового, соціально-економічного, організаційно-управлінського та культурно-психологічного характеру. *Політико-правові фактори детермінації* кіберзлочинності: неузгодженість позицій урядів різних держав з питань інформаційної

політики та дотримання прав особи у кіберпросторі; відсутність єдиної державної стратегії України щодо забезпечення кібернетичної безпеки.

Відстоюється думка, що *соціально-економічні фактори* кіберзлочинності не є для неї специфічними, але, тим не менш, суттєвими, а саме: розшарування населення за майновою ознакою, падіння рівня життя, безробіття, інфляція; трансформація господарської діяльності міжнародного рівня з превалюванням її сегменту в кіберпросторі; нарощування обсягів міжнародних безготівкових розрахунків (в тому числі й з активізацією трудової міграції), інтернет-банкінгу є кореляційними та обумовлюючими чинниками кіберзлочинності.

Організаційно-управлінські фактори кіберзлочинності полягають у недоліках соціального контролю(ігнорування користувачами всіх рівнів вимог інформаційної безпеки, вади фінансового та наукового забезпечення її функціонування; дефектах в системі організації і практичного забезпечення технічного захисту комп'ютерних мереж; низькому рівні підготовленості правоохоронних органів з питань протидії кіберзлочинності тощо.

Культурно-психологічні фактори обумовлюються соціально значущою активністю у віртуальному середовищі, для певних секторів якого характерним є ціннісно-світоглядний вакуум, знеособлення суспільних відносин та девальвація їх олюдненого значення. Функціонування індивідууму в таких умовах сприяє його соціальній дезорганізації, конфлікту зі складовими реальних сфер життєдіяльності, який вирішується на базі закріплених антисуспільних установок, концентровано виражених у комплексі сваволі та ілюзій [1, с. 9-10].

Суспільна небезпека злочинів у сфері комп'ютерної інформації полягає в тому, що неправомірний доступ або зміна комп'ютерної інформації може порушувати діяльність різних систем забезпечення держави: оборони, енергетики, транспорту та спричинити не тільки

матеріальний збиток, але і людські жертви [8, с. 109]. Останнім часом швидко розвивається тенденція зростання кількості кіберсуїцидів, що є видом злочину проти життя і здоров'я. В даному випадку спостерігається аутоагресія, яка знаходить вихід через пошук в мережі однодумців та спільне здійснення суїцидальних дій. В даному випадку провідним мотивом є прагнення позбавитись болю, що виникає в кризових ситуаціях і який суб'єктивно сприймається як нестерпний, або ж бажання шляхом смерті утекти від проблем, з якими індивід не здатен впоратись. Найбільшим і відомим сайтом для самогубців Wired називає alt.suicide.holiday, скорочено a.s.h., що можна перевести, як «прах». Учасники цієї групи називають себе Ешера (Ashers), а ЗМІ вважають цей ресурс винним як мінімум в трьох випадках суїциду. Кореспонденти журналу Wired, поговоривши з родичами загиблих, готові підтвердити ще сім смертей, пов'язаних з a.s.h., протягом січня 2003 року [9, с. 257]. Першим зафіксованим фактом вбивства, здійсненим за допомогою мережі Інтернет, був випадок, що відбувся в лютому 1998 р. в США. Важко поранений свідок злочину був захований в закритому госпіталі на території військової бази, проте злочинці через Інтернет-мережу змінили режим роботи кардіостимулятора і апарату вентиляції легенів, що призвело до смерті свідка. Та складність виявлення дій комп'ютерного злочинця полягає в його можливості скоювати злочини в кіберпросторі, у якого не має державних кордонів, що багаторазово збільшують ступінь її суспільної небезпеки.

Висновок. Надшвидкий науково-технічний прогрес безпосередньо пов'язаний із тією ситуацією, в якій опинився світ кіберзлочинності. Кіберзлочинці створюють нові методи скоєння злочинів та знаходять помилки в системах безпеки швидше, ніж ті, хто їм протидіє. Збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від

традиційних видів злочинів. Тому існує нагальна потреба продиктована часом здійснювати активну протидію таким діянням.

Література

1. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук : 12.00.08 / М. О. Кравцова ; Харк. нац. ун-т внутр. справ. - Харків, 2016. - 16 с.
2. Єдиний звіт про кримінальні правопорушення по державі за жовтень 2018 року Генеральної прокуратури України від 07 листопада 2018 р. [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113654&libid=100820#
3. Єдиний звіт про кримінальні правопорушення по державі за жовтень 2017 року Генеральної прокуратури України від 06 листопада 2017 р. [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113654&libid=100820#
4. Єдиний звіт про осіб, які вчинили кримінальні правопорушення за жовтень 2018 року Генеральної прокуратури України від 07 листопада 2018 р. [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113654&libid=100820#
5. Кримінологія: підручник / В.В. Голіна, Б.М. Головкін, М.Ю. Валуйська та ін., за ред. В.В. Голіни, Б.М. Головкіна. - Х.: Право, 2014. – С. 294.
6. Ткачова О.В., Науменко К.В. Кримінологічна характеристика кіберзлочинця. Юридичний науковий електронний журнал №2/2018 [Електронний ресурс]. – Режим доступу: http://www.lsej.org.ua/2_2018/54.pdf

7. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. - 2010. - № 3 (19). - С. 129–136.
8. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08 . - Иркутск, 2008. - С. 269.
9. Гаркуша Ю.О. Кримінологічна характеристика злочинів, пов'язаних з використанням соціальних мереж. Порівняльне аналітичне право. - №6/2015. - С. 255-258 [Електронний ресурс]. – Режим доступу: http://www.pap.in.ua/6_2015/78.pdf