УДК 343.9:004.77:316.4
DOI https://doi.org/10.32782/2524-0374/2021-12/88

КРИМІНОЛОГІЧНИЙ АНАЛІЗ ЯВИЩА КІБЕРЗЛОЧИННОСТІ

CRIMINOLOGICAL ANALYSIS OF THE PHENOMENON OF CYBERCRIME

Пивоваров В.В., к.ю.н., доцент,
доцент кафедри кримінології та кримінально-виконавчого права
Національний юридичний університет імені Ярослава Мудрого

Бабійчук В.С., студентка ІІ курсу магістратури
господарсько-правового факультету
Національний юридичний університет імені Ярослава Мудрого

Бевза Д.О., студент ІІ курсу магістратури
господарсько-правового факультету
Національний юридичний університет імені Ярослава Мудрого

У статті проаналізовано питання про сучасні виклики, які постають перед державою і кожним конкретним індивідом у цифровому середовищі. Акцентовано увагу на необхідності відповідального підходу до цієї проблеми та запобігання її масовому поширенню. Проведено порівняльний аналіз кіберзлочинності та традиційних злочинів, під час якого знайдено певні спільні характеристики. Наведені аналогії між традиційною типологізацією злочинної поведінки та її модерними віртуальними проявами можуть сприяти новим науковим пошукам, оскільки метод аналогії допомагає конкретизувати і спростити розуміння абстрактного, зіставити нові гіпотези з уже вирішеними задачами.

Автори зазначають непотрібність зосередження на питаннях, які не створюють конкретних наукових висновків і нездатні вплинути на прикладну сферу, зокрема висвітлюючи неактуальну, на їхню думку, дискусію щодо термінологічних розбіжностей у підходах до ключових складників понятійного апарату зазначеної теми.

Окрему увагу дослідниками приділено характеристиці особи злочинця цієї категорії суспільно небезпечних діянь. Здійснено власну наукову класифікацію таких осіб із обґрунтуванням їхнього психотипу і сталості діянь. У дослідженні доведено, що хибною є думка суспільства про ототожнення всіх кіберзлочинців із поняттям «хакер». Автори наголошують на тому, що боротьба із кіберзлочинністю неможлива без усунення віктимологічних підстав виникнення такого явища. Саме певний вид поведінки жертви (її недбальство, самовпевненість) часто стає вирішальним фактором, що спонукає зловмисника до дії.

Надважливою визнано потребу протидії кіберзлочинності з боку всіх залучених до віртуального процесу акторів. Причому вказується на безпідставність застосування у цій сфері механізмів, які суттєво обмежують права громадян та не є пропорційними кінцевій меті.

Запропоновано на основі авторського соціологічного дослідження, що охопило різні вікові групи населення України, зосередитися на необхідності підвищення рівня інтернет-грамотності. За результатами опитування підтверджено побоювання щодо відсутності розуміння мережевих операцій і правил їх проведення в умовах значної поширеності використання інтернет-мережі як для особистих, так і для професійних цілей.

Ключові слова: кіберзлочин, цифрові загрози, віктимологія, кіберпростір, комп'ютерний злочин, запобігання кіберзлочинності.

In the article authors analyzed contemporary issues that are encountered by the state and each particular individual in the digital environment. The attention was focused on the necessity of responsible attitude towards the given problems and prevention of the mass distribution. Comparative analysis of cyber crimes and traditional crimes showed some common characteristics between the two. Given analogies relating to conventional typology of criminal behavior and its modern virtual form can contribute to the development of new scientific research, since the analogy method helps to specify and simplify the understanding of the abstract by comparing new hypothesis to previously solved problems.

Authors emphasize on the irrelevance of focusing on the problems that don't contribute to concrete scientific conclusions and are of no use at the practical level. The researches have given special attention to identity of the perpetrator in this category of public security threat.

Authors presented their own classification of the criminals in cyber space with the reasoning for their personality types and regularity of crimes. It is stated that identification of all cyber criminals with the term «hacker» is wrong. It is emphasized that to combat cybercrime it is important to address 'victim' behavior. Often it is the victim's actions (carelessness, complacency) that become the crucial factor that motivates the criminal to act. It is extremely important that all the actors involved in a virtual process acknowledge the need to combat cyber crimes. It is also pointed that the implementation of mechanisms in this sphere that drastically restrict the rights of citizens is unreasonable and does not match the final goal.

Based on author's sociological study that covered different age groups of Ukrainians, the researchers come to the conclusion that there is a strong need for the increase of Internet literacy. Results of the survey show that there is a certain confusion as for network operations and particular safety rules amidst the growing increase of internet usage for personal and professional purposes.

Key words: cybercrime, digital threats, victimology, cyberspace, computer crime. cybercrime prevention.

Постановка проблеми. Поява цифрових технологій стала вихідною точкою для суттєво нового соціокультурного середовища – категорії мережевих взаємовідносин. Інтернет, який пов'язує великі та малі соціальні групи, конкретних індивідів між собою, не лише видозмінив сталі типи взаємодії, але і сформував сукупність технічних інструментів, потрібних для оптимізації, автоматизації та спрощення певних аспектів життя. Втім, не існує нововведень, які фактор недосконалості людської природи не здатний обернути на потенційні загрози для подальших етапів суспільного розвитку. Таким чином, модернізація охопила і девіантну екосистему правопорушень. Всесвітня мережа суттєво спростила механізм виконання традиційних злочинів та наразі продовжує породжувати нові кримінальні техніки.

Сучасні кримінологічні концепції, що диференціюють злочинність за соціальними, культурними та іншими матеріальними характеристиками, здатні результативно протидіяти їй як явищу загалом та ефективно запобігати індивідуальним проявам протиправної поведінки, виявляючи епіцентри злочинності, цільову аудиторію із девіантними відхиленнями та інше. Натомість виокремити виключні характеристики, що потурають вчиненню кіберзлочину, значно складніше. Визнані кримінологічною наукою соціальна відчуженість, ізольованість правопорушників та аспект маргінальності не завжди співставні із категорією кіберзлочинності. Тому потрібно застосовувати нові методики і підходи до вивчення кіберзлочинів, аналізувати неправомірну поведінку в інтернет-просторі та виявляти потенційно віктимологічні прояви у діях інтернет-користувачів.

Наразі активно провадяться міждисциплінарні дослідження щодо вивчення характеру комп'ютерної злочинності, аналізу показників ефективності превентивних

заходів. Причому у результативності цих наукових пошуків зацікавлені і держава, і приватний сектор, оскільки національна безпека, стан економіки, а також інтереси приватного характеру залежать від захищеності одного із найцінніших ресурсів XXI сторіччя – інформації. Тому ми вбачаємо в обраній нами для дослідження темі актуальне практичне значення.

Аналіз останніх досліджень і публікацій. Дослідження теоретичних аспектів кримінологічної характеристики кіберзлочинності знаходять своє відображення у працях численних зарубіжних і вітчизняних науковців. Зокрема, проблемні питання сучасної інтернет-злочинності вивчає О.В. Таволжанський. Стан і тенденції кіберзлочинності на міжнародному і національному рівнях стали предметом наукових доробків Н.В. Сметаніної. Роль психологічного портрету для превенції та розкриття кіберзлочинів у своїх працях висвітлює М. В. Карчевський. Криміналісти В. М. Шевчук та В. Ю. Шепітько досліджують аспект використання інформаційних технологій для встановлення особи злочинця. Запобігання корпоративним проявам кіберзлочинності висвітлює у своїх працях В.В. Пивоваров. Зарубіжні науковці Ш. Шольберг, Д. Паркер, С. Хантінгтон присвятили праці питанням кіберзлочинності у контексті міжнародно-правового регулювання, проблемам організованої злочинності в інтернет-просторі, а також розробленню методів протидії комп'ютерним злочинам. Відтак тема кіберзлочинності є відносно відомою і доволі розробленою в межах наук кримінального циклу, проте за умови стрімкого розвитку суспільних інтернет-відносин і невпинного технологічного прогресу науковий доробок цього напряму потребує постійного і систематичного доопрацювання та актуалізації. Зокрема, зростає потреба у дослідженнях суто практичного спрямування, які надають власне трактування провідним аспектам кримінологічного аналізу кіберзлочинності, детально характеризуючи осіб, які вчиняють кіберзлочини.

Метою роботи є кримінологічний аналіз сучасних кримінальних цифрових загроз із погляду на кримінологічні та соціологічні суспільно-поведінкові моделі (аномії, віктимної поведінки тощо) на основі власного емпіричного дослідження, а також розроблення сукупності практичних методів запобігання і протидії кіберзлочинності.

Виклад основного матеріалу. Комп'ютери органічно інтегрувались у наявний суспільний уклад, проте на всіх етапах їх вдосконалення сприймалися дуалістично. Заслужений професор соціології Джефрі Ч. Александр у своїй монографії указував на бінарність нового технологічного явища, вирізняючи дві сторони: сакральну – розумні машини зроблять нашу цивілізацію більш здоровою і щасливою, людина стане вільною у виборі життєвого шляху і спокійно вдосконалюватиме навички соціального взаєморозуміння, натомість працюватиме замість неї машина; і профанну – технологізація призведе до руйнувань, маніпуляцій, викривлення і спотворення наявної дійсності [1]. Отдже, підтверджуючи власну двоїсту природу, технології не лише значно спростили процес виконання операцій пошуку, обліку, обрахунку тощо, але і стали середовищем (засобом) для вчинення нового типу правопорушень.

Специфіка цифрових загроз у розрізі кримінологічного аналізу полягає у відносній новизні явища. Якщо звичні злочини досліджувалися науковцями-теоретиками і практиками не одне сторіччя, то історія кіберзлочинів умовно обліковується лише із 1994 року (атака проти «Citibank»). Багатоаспектність, поширеність, відсутність сталих характеристик явища і трансформація узвичаєних підходів істотно гальмують процес всебічного вивчення феномену. Подібний стан речей обумовлений ще деякими особливостями. Стандартний, доцільніше сказати, фізичний злочин зазвичай охоплюється певним географічним районом (регіоном). Кібер– натомість залишається метафізичним (абстрактним), оскільки традиційні предметно-об'єктивні умови вчинення злочину під дією технологій або трансформуються, або стають непридатними для виокремлення. Наприклад, часовий проміжок учинення злочину не завжди підлягає визначенню, адже віртуальні правопорушення навіть не прив'язані до часового поясу. Місце та обстановка вичерпуються однорідним кіберпростором, спосіб полягає у послідовних методах взаємодії із електронним пристроєм, у використанні певних технічних прийомів, алгоритмів і безпосередньому впливі на третіх осіб через посередника – персональний комп'ютер [2].

Зазначимо, що наразі поширеною практикою є віднесення до сфери проблематики під час дослідження віртуальних правопорушень відсутності уніфікованого підходу до придатної термінології. Проте ми не вбачаємо у цьому критичного бар'єру для провадження наукових пошуків. Одне лише чітке визначення не здатне нейтралізувати проблему. Зокрема, в національному законодавстві, наукових працях широко використовується термінологія на кшталт кіберзлочин (або комп'ютерний злочин), але це ані прямо, ані опосередковано не впливає на зниження фактичної кількості правопорушень цього виду, лише мінімально регулює кількість зареєстрованих у системі проваджень за тією чи іншою статтею залежно від формулювання диспозиції. Тим не менше, ми погоджуємось із тезою, що ототожнення понять «комп'ютерний злочин» і «кіберзлочин» є помилковою тенденцією, оскільки перше є ширшим і поглинає наступне [3]. Працюючи із подібними квазі-явищами, слід пам'ятати, що результативний складник вивчення суспільних процесів за своєю специфікою слабко підлягає формалізації, адже створюється під впливом системи суб'єктивних факторів. Таким чином, відсутність доктринальної єдності є характерною для всіх теоретико-прикладних наук, до яких відносять і кримінологію, тож цей (семантичний) чинник не повинен викликати зайвих диспутів, що дезорієнтують і відволікають наукову спільноту.

Практична частина нашого дослідження орієнтована на аналіз основних рис особи кіберзлочинця, специфіку злочину та його віктимологічний складник. Якщо абстрагуватися від розбіжностей і розбити злочини на прості категорії (об'єкт, суб'єкт і похідні), можна прокласти певні паралелі між традиційною типологізацією злочинної поведінки та її модерними віртуальними проявами. Наприклад, злочини проти основ національної безпеки і віртуальна інформаційна війна, кібертероризм; правопорушення проти життя і здоров'я та доведення до самогубства внаслідок систематичного цькування особи у соціальних мережах або вбивство внаслідок зламу системи автоматичного управління транспортним засобом; правопорушення проти статевої свободи і розбещення неповнолітніх під час спілкування в інтернеті; правопорушення проти власності та віртуальні фішинг, вішинг, кеш-трепінг тощо.

У свою чергу, основний пласт злочинів, звичайно із певними застереженнями, поділяється на політичні, корисливі, агресивні, анархічні та необережні [4]. Віддаючи данину загальноприйнятій кримінологічній доктрині та користуючись аналогією як методом наукового пізнання, ми пропонуємо залежно від наведених вище типів злочинів розподілити кіберзлочинців на категорії:

– ідейні (імпульсивні). Такі особи зазвичай раніше не притягувалися до кримінальної відповідальності, можуть як володіти певними специфічними знаннями і навичками, так і бути аматорами; у підсумку основною метою їхньої діяльності є виклик системі;

– корисливі, які нерідко мають судимості за посягання на відносини власності. Причиною вчинення злочину є отримання матеріальної вигоди. Такі часто працюють групами, ґрунтовно планують діяльність і нерідко є найманцями (залежно від виду посягання можуть бути і простими шахраями, і професійними «чорними» хакерами»);

– анархічні (вандали). Такі особи мають антиальтруїстичні наміри і використовують комп'ютер як засіб для вчинення антисоціальної злочинної поведінки, суб'єктивно вважаючи, що суспільство загалом, конкретних осіб чи організації потрібно дезорганізувати.

Відповідно, кіберзлочини у контексті нашого дослідження ми пропонуємо стратифікувати на три різновиди: такі, в яких технічний пристрій виступає об'єктом суспільно-небезпечної діяльності; є проміжним інструментом між декількома етапами досягнення злочинної мети; є лише засібом (платформою) для планування злочину.

Із метою аналізу структури особи кіберзлочинця за А.Ф. Зелінським розроблений загальний психологічний портрет такого правопорушника [5, с. 57]. Для ефективного і ґрунтовного аналізу ми маємо звузити спектр осіб і зупинитися лише на деяких протиправних діяннях, пов'язаних із мережею, водночас опускаючи зазначену нами типологізацію за мотивом. Таким чином, ми вважаємо за доцільне дослідити структуру «хакера», оскільки саме цей збірний образ міцно увійшов у сучасну масову культуру та, найголовніше, відомий навіть людям, які мають доволі віддалене уявлення про сутність інформаційних технологій. Якщо вдаватися до семантики, сам термін англійського походження (від «hack») дослівно позначає атаку, злам. Хакер сприймається суспільством як винахідлива особа, яка володіє спеціальними знаннями у галузі програмування і здатна нестандартним чином обійти системи безпеки на комп'ютері.

Подібний зломщик є особою чоловічої статі, неодружений, раніше не судимий та не має дітей. Вік знаходиться в межах від 14 до 25 років, причому пікова активність припадає на 16-річчя. Пояснюється це особливостями вікової психології, адже саме юнацтво є періодом амбіцій, пошуків себе і прагненням життєвого успіху за відсутності досвіду і відповідних ресурсів; соціолог Роберт К. Мертон назвав такий розрив між цілями та засобами аномією. Хакери є надзвичайно продуктивними і невибагливими у питаннях харчування, побутового комфорту. Освіта – переважно вища або середня спеціальна (наприклад молодший спеціаліст за технічним фахом). Місце проживання – віддалені райони міст, житло орендоване. Ціннісні орієнтири суперечливі, особа не вважає себе порушником, уявляє себе анонімним генієм. Такі люди є інтровертами, коло довірених осіб у них дуже обмежене. Працюють наодинці. Акцентуємо, що ми розглянули лише «класичного» хакера», це поняття є значно вужчим за кіберзлочинця та охоплює тільки усталену у суспільстві (лінгвістичну) форму сприйняття цього явища.

Аналізувати феномен кіберзлочинності не можна у відриві від віктимологічного складника, адже у багатьох випадках фактором, який сприяє вчиненню правопорушення, стає поведінка жертви. Наразі спостерігається поширення таких видів шахрайства, як вішинг (утворене шляхом сполучення англ. слів «voice» та «fishing») і смішинг (від сполучення слів СМС та фішинг). Жертвами подібних правопорушень традиційно стають літні люди або сугестивні особи, які легко піддаються зовнішньому впливу незалежно від віку. Шахраї ретельно обирають потенційних потерпілих, використовуючи відомості із відкритих джерел, рідше – вдаються до зламу конфіденційної інформації. Зазначимо, що сучасна людина нерідко сама оприлюднює досьє на себе у мережі, чим значно спрощує зловмисникам завдання.

Визначальною причиною віктимізації і високої віктимності громадян є ілюзія безпеки, оскільки, як нами вже неодноразово зазначалося, кіберпростір є квазітериторією, метаявищем для усвідомлення. Людина навіть не замислюється про можливі загрози, вступаючи в анонімні відносини, які майже не регулюються нормативно. Відсутність елементарних знань про основи поведінки в мережі, надмірна розважливість і легковажність робить особу надпростою жертвою для будь-якого охочого шахрая. Як зазначалося, жертв кіберзлочинів можна поділити на випадкових і конкретно обраних. Із ними важко не погодитись, оскільки на практиці саме випадкові особи можуть потрапити під фармінг (поширений не необмежене коло осіб), а конкретно обрані – під кіберпереслідування (здійснюється із певною метою щодо визначеної особи) [6, с. 125]. Важливу роль у превенції злочинності у сфері інформаційних технологій відіграє поміркована поствіктимна поведінка, адже зазвичай лише після реального потрапляння у роль жертви особа замислюється про необхідність "гігієнічної" поведінки в мережі. У цьому контексті необхідним постає усунення зі світогляду жертви абстрактного підходу до розуміння кіберзлочину та усвідомлення нею реальної можливості отримати відшкодування заподіяної шкоди [7, с. 329].

У свідомості людини діяння стає злочином, коли викликає спротив, моральне презирство аж ніяк не в момент закріплення його у кримінальному законодавстві. Тому першочерговим заходом у сфері врегулювання інтернет-відносин має стати саме мінімізація природної латентності щодо кіберзлочинів у світогляді населення. Наступним можливим засобом протидії кіберзагрозам є створення національного Інтернету, що суперечливо сприймається у різних колах суспільства. Проте утворення суверенітету інформаційного простору, консолідація операторів національного сегменту, навпаки, зробить Інтернет більш уразливим, громіздким і нестійким. У разі відмови мережі монооператора вся країна залишиться без зв'язку. Крім того, буде дуже важко утримувати баланс між безпекою приватних даних конкретного індивіда, загальнодержавною безпекою і правом на вільний доступ до інформації. Більше того, поява 5G технологій (сателітів зв'язку SpaceX) майже виключає можливість створити закритий кіберпростір. Окрім того, утримувати потенційну систему надзвичайно складно і матеріально нерентабельно. Тож доцільніше стандартизувати міжнародні норми задля уникнення інтерлокальних колізій.

Із метою доведення зазначених висновків і тверджень у жовтні 2021 року нами було проведено емпіричне кримінологічне дослідження, під час якого опитано за пілотною програмою малої вибірки 109 респондентів із 20 запитань щодо сприйняття українцями цифрових загроз та отримано досить репрезентативні результати щодо рівня загальної інтернет-грамотності сучасних користувачів. Під час дослідження нами протестовані 6 вікових груп: 10-15 р. – 10,1 %; 16-18 р. – 15,6%; 19-25 р. – 56,9%; 26-45 р. – 10,1%; 46-60 р. – 5,5%; 61-99 р. – 1,8%. Очікувано найактивнішою виявилася група 19-25 років, а найменш активною – 61-99 років. На запитання: «Чи готові ви повністю відмовитися від використання піратських сервісів?» 20,2% опитаних відповіли «так»; 35,8% – «ні»; 22,9% – «не можу сказати напевне»; 21,1% – «частково». Цікавим для аналізу є віковий розподіл відповідей на це запитання. Більшість респондентів у віці 10-15 років готові відмовитися від піратських сервісів. Люди цього покоління не застали піку популярності таких сервісів, сайтів, неліцензійних ігор, контрафактних фільмів. Підлітки користуються стрімінговими сервісами, платними підписками, онлайн-кінотеатрами тощо, вже розуміючи, що за медіафайли в інтернеті слід сплачувати кошти, як і за будь-який інший товар.

У віковій групі 16-18 років 53% респондентів обрали варіант «ні», по 23,5% – «не можу сказати напевне» і «частково», відповідь «так» не обрав жоден респондент; у групі 19-25 років – 24% «так», по 21% – «не можу сказати напевне» і «частково», 34% – «ні». Особи віком 26-45 р. відповіли таким чином: «так» – 27%, «не можу сказати напевно» – 27%, «частково» – 18%, «ні» – 27%. Дорослішання зазначених трьох груп припало на занепад, розквіт і становлення піратської ери Інтернету, тому не дивно, що

більшість у кожній із цих вікових категорій або взагалі не готові відмовитися від використання піратських джерел, або лише ладні певним чином його обмежити. Найбільший відсоток повної неготовності показує наймолодша із трьох груп; ми це пов'язуємо із віковою психологією, етапом сепарації від родини і відносною матеріальною нестабільністю.

Вікова група 46-60 р.: «так» – 17%, «не можу сказати напевне» – 33%, «ні» – 50%. Щодо вікової групи 61-99 р. ми зазначимо, що останній результат є певною мірою оціночним, оскільки в опитуванні взяло участь лише дві особи найстаршої вікової групи. Звичним залишається те, що люди у зрілому віці не завжди готові платити кошти за контент, який споживають у мережі. Пояснити це можна невисоким ступенем інтеграції цього покоління в інтернет-середовище і неоднозначне сприйняття локальних правил гри.

Відвідування піратського сайту і скачування безкоштовного контенту може загрожувати вірусами та занесенням шкідливого програмного забезпечення. Оскільки децентралізований файлообмін передбачає, що комп'ютер стає сервером для іншого, користувачі власноруч перетворюють свої пристрої на архіви різної, не завжди легальної інформації. Загалом тема піратства в українському сегменті інтернету є дуже актуальною і може слугувати темою для написання окремої статті. Історія «EX.UA», поширеність неліцензійних програм (зокрема у навчальних закладах тощо) є нині окремим культурним феноменом.

На запитання «Чи вважаєте ви себе інтернет-грамотними?» респонденти відповіли таким чином: «ні» – 18,3%; «більше так, ніж ні» – 67%; «відмінно знаю, як безпечно користуватись мережею» – 14,7%. На запитання «Чи вважаєте ви інтернет-загрози провідною небезпекою сучасності?» 45% відповіли «так», 9% – «ні», 46,8% – «існують більш важливі проблеми». Думки респондентів розділилися. Значна частина опитаних не вважає кіберзлочинність основним викликом XXI століття, решта відносить інтернет-загрози до ключових небезпек. Такий розподіл яскраво показує і пріоритетність державної політики, спрямованої на багато напрямків, повністю не охоплюючи жодного.

Згідно з опитуванням поняття «програміст», «хакер», «розробник» ототожнюють 9,2 % опитаних; вони вважають, що тільки поняття «програміст» і «хакер» утворюють синонімічний ряд 6,4%, на варіанті «мають різне значення» зупинилися 84,4% опитаних. Ми пов'язуємо такі результати зі стрімким зростанням ринку ІТ-послуг. Окрім того, не можна відкидати факт, що провідною віковою групою в опитуванні стала працездатна молодь, яка завжди цікавиться інноваціями та їх створює.

Запитання і відповіді на них показали рівень лояльності до явища хакерства: «Ваше ставлення до «професії» хакера» (13,8% – «позитивне», 4,6% – «надзвичайно позитивне», 29,4% – «негативне», 8,3% – «вкрай негативне», 44% – «нейтральне»;) і «Чи вважаєте ви хакерство етичним видом зайнятості?» (8,3% – «так», 59,6% – «ні», 32,1% – «користь від діяльності виправдовує ступінь посягання на етичні аспекти»), які свідчать, що, попри розуміння певного негативного забарвлення цього виду діяльності, 62,4% громадян схвалюють або висловлюють «мовчазну згоду» такій діяльності, обираючи нейтралітет. Картина вичерпно ілюструє окремі причини високої латентності кіберзлочинності.

Задля дослідження інтегрованості населення до кіберпростору ми поставили такі запитання: «Вид вашої професійної діяльності якось пов'язаний із Інтернетом?» (33% відповіли «так», 38,5% – «так, опосередковано», 28,4% – «ні»), «Ви здебільшого здійснюєте покупки онлайн чи надаєте перевагу походам до крамниці?» (57,8% зупинились на відповіді «50 на 50»; 30,3% надають перевагу крамницям; 11,9% здебільшого купують в інтернеті). Отже, більшість із опитаних працює в Інтернет-сфері або активно використовує його для роботи. Окрім цього, майже 70% здійснюють покупки онлайн. Ці результати демонструють високу активність громадян щодо здійснення операцій в Інтернеті, зокрема розрахункового характеру.

Наступні запитання демонструють нам ступінь розуміння проявів девіантної поведінки у віртуальному світі, а також розуміння сутності поведінкових патернів в Інтернеті загалом. «Які із наведених варіантів є посяганням на безпеку в інтернет-середовищі»: «ведення акаунту у соціальній мережі від імені іншої особи» – 52,3% від усіх опитаних; «розміщення неправдивої або такої, що дискредитує інших осіб, інформації» – 68,8%; публікування особистої інформації про особу без її згоди – 85,3%; «анонімне або від власного імені спілкування у грубій формі з іншою особою» – 33,9 %. Хоча всі ці пункти є девіантною поведінкою, дуже малий відсоток опитаних обрав усі можливі варіанти. «Які із тверджень є актуальними для вас»: «анонімність в Інтернеті є абсолютною» – 5,6%; «персональні дані перебувають у повній безпеці» – 17,8%; «персональні дані можуть бути розкриті у випадках загрози національній безпеці з метою захисту інших осіб» – 42,1%; «свобода дій в Інтернеті є абсолютною» – 13,1%; «не погоджуюсь із жодним» – 40,2%. Попри прийнятні показники, більшість осіб неповністю розуміють власні права та обов'язки щодо взаємодії із кіберпростором, а також переоцінюють ступінь захищеності приватної інформації.

Задля аналізу фактора готовності людей реагувати у складі громадянського суспільства чи самостійно протидіяти негативним явищам в інтернет-середовищі ми поставили таке запитання: «Ви побачили неприйнятний контент у мережі (наприклад шахрайство, цькування, неправомірне використання об'єктів права інтелектуальної власності інших осіб), ваші дії»: «повідомлю службу підтримки, якщо це шахрайство» – 20,2%; «повідомлю, якщо це цькування» – 7,3%; «повідомлю, якщо це посягання на інтелектуальну власність» – 0,9%; «в усіх зазначених випадках» – 43,1%; «ігноруватиму подібний контент» – 28,4%. Громадяни продемонстрували доволі високий показник готовності до протидії порушенням в інтернеті. Втім, більшість готова повідомляти тільки про випадки шахрайства, чималий відсоток схильний проявляти байдужість.

Очевидний зв'язок простежується між відповідями на запитання: 1) «Чи стикались ви з інтернет-шахраями?», 2) «Якщо з акаунту добре знайомої вам людини надійде прохання перейти за посиланням (для участі в опитуванні, конкурсі тощо), Ви: …», 3) «Якщо з акаунту добре знайомої вам людини надійде прохання зробити грошовий переказ, Ви: …». Особи, які відчули на собі негативні наслідки кіберзлочинів, більш поміркована ставляться до власної безпеки у мережі. Отже, перше питання: «так» – 48,6%; «особисто ні, але знаю про такий негативний досвід членів родини, друзів, колег» – 41,2%; «ні» – 10,1%. Фактично майже кожен із опитаних повідомив, що він особисто або хтось із його оточення стикались із кіберзлочинами. Друге запитання: «зробите це, але спочатку дізнаєтесь про подробиці» – 71,6%; «проігноруєте» – 11,9%; «не вагаючись, виконаєте прохання» – 16,5%. Третє питання: «зробите це, але спочатку дізнаєтесь подробиці» – 63,3%; «проігноруєте» – 31,2%; «залежить від суми переказу: якщо незначна, то без вагань надішлете» – 5,5%. Проте спонукає до роздумів такий аспект: проігнорували нашу письмову пропозицію пройти опитування приблизно 5% осіб, а додаткових подробиць про дослідження прагнули отримати лише 2%. І це велика проблема в аспекті зростання кількості випадків зламу акаунтів у соціальних мережах. Майже кожен із нас готовий відреагувати на прохання про допомогу з боку близької людини, а такими щирими почуттями нерідко спекулюють зловмисники. Посилання для «опитування», конкурсу, розіграшу призів і подібне можуть бути вірусними або перенаправляти на сторінку-дублікат, яка зчитує персональні дані (паролі, банківські картки).

Показово, що особи, які вже стикались із шахрайськими діями у мережі, і ті, які не мають подібного досвіду, однаково низько оцінили дієвість державних структур у запобіганні цифровим загрозам. На запитання «Як за п'ятибальною шкалою оцінюєте здатність державних структур захистити ваші права в Інтернеті?»: в 1 бал – 30,3%; 2 бали – 33%; 3 бали – 26,6 %; 4 бали – 9,2%; 5 балів – 0,9%. Отже, владним структурам потрібно працювати не лише над відповідним технічним забезпеченням і кваліфікацією кадрів, але і приділити достатню увагу маркетинговій стратегії задля створення позитивного іміджу в очах громадськості.

Висновки. «Краще запобігти, ніж боротися» – принцип, який яскраво знаходить своє втілення у можливих стратегіях протидії кіберзлочинності. Непоправні наслідки (втрата інформації, розкриття конфіденційних даних, зупинка роботи цифрових сервісів тощо) та їхнє миттєве настання доводять необхідність застосування цього принципу. Боротьба із кіберзлочинами ускладнюється метафоричністю кіберреальності та анонімністю віртуального злочинного світу. Крім цього, протидія цифровим загрозам гальмується внаслідок недооцінення і невикористання наявних надбань технологічного прогресу.

Проведені в цій роботі аналогії між традиційною типологізацією злочинної поведінки, вже давно унормованої кримінальним законодавством, та її модерними віртуальними проявами, а також запропонований авторами узагальнений кримінологічний портрет злочинця не претендують на вичерпність та, вочевидь, не охоплюють детальною класифікацією всіх потенційно можливих суб'єктів кіберзлочинів, оскільки структура цифрової злочинності надзвичайно різноманітна за своєю природою. Тим не менш зазначені узагальнені типології і портрети можуть використовуватися для подальших наукових розробок, а також у практичній діяльності правоохоронних органів. Проаналізовані основні аспекти віктимної поведінки інтернет-користувачів також можуть використовуватися спеціалізованими органами для проведення профілактичних заходів серед користувачів.

Наостанок ми зазначимо, що найслабкішим місцем у структурі будь-якої соціально зумовленої системи є людина, індивід. Очевидно, жодна якісна законодавча техніка не може осягнути і передбачити можливі варіанти трансформації та видозміни цифрових загроз і кіберзлочинів. Тому нині найбільш дієвим і радикальним заходом протидії кіберзлочинності залишається просвіта і просвітництво серед, підкреслимо, всіх без винятку вікових прошарків населення. Лише окремі прогалини в цій роботі здатна закривати поміркована практична діяльність відповідних державних структур.

ЛІТЕРАТУРА

1. Александер Дж. Сакральная и профанная информационная машина. Смыслы социальной жизни: культурсоциология. Пер. с англ. Г.К. Ольховикова, ред. Д.Ю.Куракина. Москва : Праксис. 2013.
2. Бабійчук В.С. «Кібертероризм та протидія йому». *Young Scientist*. 2019. № 4 (68). С. 103-107.
3. Пивоваров В.В. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3. ч. 2. с. 177–182.
4. Головкін Б.М. Корислива насильницька злочинність в Україні: феномен, детермінація, запобігання: монографія. Харків : Право, 2011. 440 с.
5. Зелинский А.Ф Криминология : курс лекций. Харків : Прапор, 1996. 260 с.
6. Віктимологія : навч. посіб. / за ред. В. В. Голіни і Б. М. Головкіна. Харків : Право, 2017. 308 с.
7. Фоменко О.В. Кіберзлочинність: сучасний стан та особливості віктимологічної профілактики. *Юридичний науковий електронний журнал*. 2017. № 6. С. 328-330. URL: http://lsej.org.ua/6_2017/97.pdf (дата звернення: 03.11.2021)