УДК 340.12
DOI: https://doi.org/10.21564/2663-5704.61.304630

Трофименко Володимир Анатолійович, кандидат юридичних наук, доцент,
доцент кафедри філософії Національного юридичного університету
імені Ярослава Мудрого, м. Харків, Україна
v.a.trofymenko@nlu.edu.ua
ORCID ID: 0000-0003-2240-3727

ЛЮДИНА ЯК ОБ'ЄКТ КІБЕРЗЛОЧИННОСТІ

Кожна сфера суспільного буття має два боки: позитивний та негативний. Не обійшло це і кіберпростір. Кіберзлочинність, як сфера кіберпростору, постійно зростає, змістовно та технологічно оновлюючись. Одним з напрямків кіберзлочинності, що швидко розвивається, є кібербулінг, метою якого є вплив на людську психіку. Таким чином, кіберзлочинці опановують нові способи впливу на людину. У свою чергу, це вимагає активізації наукових розробок у цій сфері.

Ключові слова: *кіберпростір, кіберзлочинність, булінг, кіберзалякування, технічний прогрес, психічна шкода.*

Постановка проблеми. Безмежність кіберпростору призвела до швидкого збільшення кількості напрямків його розвитку. Його інтенсивний розвиток не дозволяє сьогодні підтримувати достатній рівень безпеки комп'ютерних та мережевих технологій, що існують, хоча вони і не стоять на місці. Тому кіберпростір все більше привертає увагу наукової спільноти. І якщо «білий» кіберпростір цікавить науковців з боку розширення його можливостей для людини та осучаснення її життя, інший його бік все більше непокоїть вчених.

Всепроникненість кіберпростору дозволяє використовувати його проти користувачів для досягнення злочинних та аморальних цілей. Кількість постраждалих зростає, а злочинців важко не тільки знайти, а навіть ідентифікувати. Звертаючись до аналізу кіберзлочинності взагалі або до окремих її проявів науковці намагаються створити певні алгоритми боротьби з нею. Але це переважно пропонується стосовно тих, що вже існують, злочинних інститутів. Різновекторність розвитку кіберпростору не дозволяє зробити планові прогнози для боротьбі з кіберзлочинами. Тому розроблення цієї проблематики продовжується та розширюється. Людина, відкриваючи чергові способи використання кіберпростору, дає науці нові напрямки для розроблень цього питання.

Ураховуючи зазначене, дослідження кібепростору та кіберзлочинності в сучасній науковій традиції займає одну з провідних позицій.

Аналіз останніх досліджень та публікацій. Викликом людству вважають кіберпростір румунські вчені А. Григореску та Р. Чітеску [1]. Майбутнє, як вони пишуть, передбачає передові технології, набагато розвиненіші людські стосунки, але водночас відсутність ефективної взаємодії, передових знань, а також нових меж, яких потрібно досягти. Суспільство майбутнього, на їхню думку, – це технології, необмежені можливості незвіданих зв'язків і викликів. Однак усі ці можливості пов'язано з ризиками, загрозами та вразливими моментами. Інтернет як інструмент, вважають автори, зробив значний внесок у технічний і науковий прогрес людства. Безліч можливостей, які він пропонує, і легкий доступ для кожного громадянина полегшує відсутність єдиної законодавчої бази на міжнародному рівні та ефективного і конкретного контролю над розробленням деяких програм. Це протистояння не завжди має бажаний результат, а стосовно контрольованого розвитку та використання його дуже важко досягти, особливо для державних суб'єктів. Віртуальний світ, таким чином, набирає переваги через залежність, кіберпростір стає тим дивацтвом, що вирівнює успіхи та невдачі людства, шаблоном майбутніх битв, які можуть змінити карту світу, мольбертом, на якому окреслюються наші глибокі емоції. Це дзеркало суспільства і місце, де можна продавати прогнози на майбутнє. Кіберпростір не має кордонів. Як пишуть науковці, це глобалізація в чистому вигляді, нова парадигма сучасності. Це відкриття людини людині на кожному рівні. Ризик є постійним складником технологічного, соціального та економічного розвитку, але знання меж, у яких він може проявлятися, завдяки його передбаченню та діям може зменшити його негативні наслідки. Перед кібератаками вразливим стає все – від критичної інфраструктури країни до безпеки кожної людини. Ефект продукту глобальний, кожна вразливість створює передумови для експоненційного зростання пов'язаного ризику та впливає на безпеку від індивідуального до глобального рівня. Віртуальний світ – це ~~вже~~ світ завтрашнього дня.

На вагомість кібербезпеки звертає увагу й австралійський вчений Г. Адамсон [2]. Люди в XXI ст., вважає вчений, значну частину свого життя беруть участь у спілкуванні за допомогою технологій. Це стало виміром людського існування, і після пандемії COVID-19 усе частіше зустрічається в роботі, навчанні та відпочинку. Якщо ми шукаємо значення в цьому комунікаційному просторі, то можемо описати цю комунікаційну технологію як кіберпростір. Кіберпростір, за визначенням Адамсона, – це поєднання засобів масової інформації та технологій у новій формі. У комплекті з власними практиками, поведінкою та маніфестами функціонуючий кіберпростір можна вважати глобальною основою людського існування так само, як чисте повітря чи відсутність пандемії. Незважаючи на те, що кіберпростір стійкий до тотального контролю, він усе ж крихкий і потребує захисту, якщо люди хочуть отримати

його переваги. Кібербезпеку можна вважати просто захистом безпосередніх, практичних і поточних елементів технології. Проте, щоб захистити будь-яку частину кіберпростору, необхідно захистити весь кіберпростір.

Щільному та тісному зв'язку людини та кіберпростору приділяє увагу і група китайських учених – З. Чанг, Р. Ін та Х. Нінг [3]. Простір мислення, пишуть вчені, виник із появою людської цивілізації. З появою та розвитком кіберпростору почала відбуватися взаємодія між цими двома просторами. У зіткненні мислення і технологій, на думку авторів, відбулися нові зміни як у просторі мислення, так і в кіберпросторі. Тому вони поділяють поточну інтеграцію та розвиток простору мислення та кіберпростору на три етапи, а саме: інтернет мозку, інтернет думки та інтернет мислення. На кожному з цих етапів обговорюються зміст і технології досягнення конвергенції та з'єднання просторів. Крім того, передбачається, що інтернет творчості представляє майбутній розвиток простору мислення та кіберпростору.

Дещо іншу позицію стосовно корисності кіберпростору займає словацький вчений С. Галік [4]. Він висловлює свою позицію на прикладі освіти. Кіберпростір цифрових медіа, вважає автор, змінює сучасну освіту двояко: новим підходом до розуміння інформації та новим способом організації цієї інформації. У першому випадку саме об'єктивація інформації сприяє ідеї скороченого типу освіти, заснованої на певному обсязі знань, застосовних на практиці. Але вчений підкреслює той факт, що інформацію не можна сприймати лише як об'єкт, її варто сприймати як контекстну та необмежену семантичну одиницю, яка через новий організаційний рівень стає знанням. На думку дослідника, крім інформації та знань, вищий рівень пізнання потребує неявних людських рис – творчості та мудрості, а також моральних якостей людини. Другий випадок представляє мережеву структуру інформації, яка характеризується циклічною обробкою, оперативним (майже миттєвим) зв'язуванням інформації, яка базується переважно на зображеннях. Цей тип комунікації та організації інформації, пише вчений, є корисним, оскільки він дає нам швидкий спосіб пошуку інформації, а також більше творчості. Однак цілком можливо, що це означає ризик послаблення деяких когнітивних здібностей людини (таких як логічне та абстрактне мислення), що життєво важливі не тільки в науковій діяльності, а й у повсякденному житті. Під впливом комунікації в кіберпросторі сучасна освіта починає різко відходити від дискурсивного (логічного, абстрактного) мислення до асоціативного (особливо образного).

Але людина в кіберпросторі не завжди виступає порядним користувачем. Про кібердевіацію як новий соціальний феномен, пише польський дослідник В. Мінсевіч [5]. Метою його досліджень є концептуалізація та регламентація значення терміна «соціальна кібердевіація». На думку автора, необхідно ви-

значити, чи можна вказувати на існування стандартів серед віртуальної онлайн-спільноти, які визнаються більшістю її учасників. Номінальне визначення кібердевіації як порушення норм, що панують у віртуальній спільноті, є відправною точкою для класифікації дій, які порушують норми в кіберпросторі. Градація поведінки, вважає вчений, вказує на те, що ситуації в інтернеті – це діяльність: низької інтенсивності, орієнтована насамперед на соціальні, а не правові норми; середньої інтенсивності, де критерієм є порушення правової норми; високої інтенсивності, що юридично карається та неприйнятна в усій спільноті, явно порушує соціальні норми.

Зважаючи на великий спектр проявів кібердевіації, одним з найбезпечніших проявів якої є кіберзлочинність, дослідження цього феномену в сучасній науці лише зростає.

Формулювання мети. Метою публікації є демонстрація того, як розвиток кіберзлочинності сприяє збільшенню негативного впливу на людину. На прикладі кібербулінгу показано, як психіка людини поступово включається у сферу зацікавленості кіберзлочинців.

Викладення основного матеріалу. Розвиток сучасних технологій призводить до того, що певна їх частина використовується для порушення верховенства права. Про це пише іспанський вчений Ф. Пінеда [6]. Зараз, пише він, людство переживає прискорену технологічну революцію, особливо у сфері комунікацій, де звичайна пошта поступилася місцем електронній пошті, з'явилася можливість замінити розмови віч-на-віч телефонними дзвінками, і навіть миттєвий зв'язок можна встановити через відеоконференцію. Ці приклади, на його думку, здаються лише початком великої трансформації в найближчі роки. Подібним чином у сфері інформації відкриваються прояви нового цифрового виміру з появою приладів, що дозволяють зчитувати дані за допомогою світлових приладів, або з узагальненням використання інтернету, який став джерелом найважливішої інформації у світі. Технологічний прогрес і цифровізація інформації, вважає науковець, вплинули на стільки сфер, що навіть існування нового цифрового світу, нового суспільства або кіберсуспільства, відмінного від традиційного аналогового світу, було захищено. Однак дослідник робить висновок, що універсальність і транснаціональність цих нових способів комунікації та інформації, з усіма перевагами, не позбавлені значних ризиків для свобод людей, навіть для верховенства права, однією з основних функцій якого є гарантування, ефективність і захист цих свобод, які тепер можуть бути пошкоджені використанням нових технологій.

Про небезпеку кіберпростору попереджає також група іспанських учених – Ф. Вера, Дж. Гуірао та А. Інфантес [7]. Вони представляють підхід до проблеми безпеки в кіберпросторі з соціокультурної точки зору. Дослідники починають з характеристики нового простору через стратифіковану модель,

що надає актуальності людям як агентам, які використовують і надають значення технологічній інфраструктурі. Автори показують, як розширення кіберпростору паралельно спричинило зростання кіберзлочинності в її різних формах – кіберзлочинності, кібертероризму, кібервійни тощо. Не ігноруючи важливість базової технології, вони зосередилися на ролі людського фактору, аналізуючи основні кіберзагрози, яким піддаються люди, і залучених учасників. Нарешті, науковці зазначають, що швидкий розвиток кіберпростору за масштабами та глибиною забезпечить дивовижні задоволення певних людських потреб, але водночас збільшить вразливість користувачів, відкривши сценарій високого ризику, з яким суспільству доведеться зіткнутися, щоб створити необхідну довіру для гарантування безпеки та свободи людей у новому середовищі. У цьому сценарії, як роблять висновок вчені, соціальні науки відіграють важливу роль, оскільки проблеми, що стосуються нашої безпеки та наших прав, не можуть розглядатися як суто технічне питання.

Вивченню глобальної географії кіберзлочинності ті її рушійних сил приділяють увагу С. Чен, М. Хао, Ф. Дінг, Д. Дженг, Дж. Донг, С. Чанг, К. Гуо, С. Гао [8]. Кіберзлочинність, вважають вони, завдає шкоди світовій економіці, національній безпеці, соціальній стабільності та індивідуальним інтересам. Поточні зусилля щодо подолання загроз кіберзлочинності зосереджені насамперед на технічних заходах. Автори розглядають кіберзлочинність як соціальне явище та будують теоретичну основу, яка об'єднує соціальні, економічні, політичні, технологічні фактори та фактори кібербезпеки, що впливають на кіберзлочинність. Учені пропонують свої моделі дослідження кіберзлочинності: узагальнені лінійні моделі (GLM) використовуються для визначення основних факторів, що впливають на кіберзлочинність, тоді як моделювання структурними рівняннями (SEM) використовується для оцінки прямого та непрямого впливу різних факторів на кіберзлочинність. Результати GLM, на думку вчених, показують, що включення широкого набору соціально-економічних факторів може значно покращити пояснювальну силу моделі, а кіберзлочинність тісно пов'язана з соціально-економічним розвитком, тоді як їхній вплив на кіберзлочинність відрізняється залежно від рівня доходу. Крім того, результати SEM, додатково розкривають причинно-наслідкові зв'язки між кіберзлочинністю та численними контекстуальними факторами, демонструючи, що технологічні фактори слугують посередниками між соціально-економічними умовами та кіберзлочинністю.

Дослідженню перетину кіберзлочинів і вуличних злочинів приділяють увагу нідерландські науковці Е. Люкфелдт та Р. Рокс [9]. Вони проаналізували чотирнадцять голландських кримінальних розслідувань мереж, які вчиняли кіберзлочини, щоб отримати розуміння офлайнових і локальних аспектів цієї діяльності. По-перше, вони перевірили, чи залучено мережі

в цих випадках також до іншої кримінальної діяльності, крім кіберзлочинів. По-друге, вчені проаналізували походження та розвиток цих мереж, приділяючи особливу увагу їх ролі або офлайн-взаємодіям на реальних вулицях. По-третє, автори досліджували, чи містяться у справах відомості, які б свідчили про наявність вуличної культури, що інформує про діяльність правопорушників. Цей аналіз як кримінальної діяльності, так і походження та розвитку мереж кіберзлочинців підкреслює, як вважають вони, постійну важливість офлайнового світу. Ідучи далі, базуючись на їхніх мовних практиках, мотивах і нейтралізаціях, автори доводять, що основні члени, рекрутери та грошові мули в різних випадках вбудовані в голландську вуличну культуру. Таким чином, випадки кіберзлочинності також можна інтерпретувати як цифрову диверсифікацію традиційних вуличних (економічних) злочинів, а отже, як емпіричні приклади вуличних правопорушників, які адаптуються до розвитку технологій.

Людському фактору у кіберзлочинності приділяють увагу канадський вчений Б. Дюпон та американський дослідник Т. Холт [10]. Вони підкреслюють центральну роль людського фактора в кіберзлочинності та потребу в розробленні міждисциплінарної програми досліджень, яка б допомогла краще зрозуміти постійну еволюцію онлайн-шкоди та розробити ефективніші відповіді на неї. Термін «людський фактор», пишуть автори, розуміється дуже широко і охоплює індивідуальний, інституційний та суспільний виміри. Він охоплює індивідуальну поведінку людей і соціальні структури, які забезпечують колективні дії груп і спільнот різного розміру, а також різні типи інституційних угруповань, які формують реакцію суспільства. Це дозволяє вченим відобразити складну взаємодію між правопорушниками, машинами та жертвами, вийшовши за межі статичних типологій і запропонувавши більш динамічний аналіз екології кіберзлочинності та поведінки, що лежить в її основі.

Ролі особи в запобіганні кіберзлочинам приділяє увагу естонський вчений К. Кікерпіл [11]. Як важливий соціальний інститут, пише автор, протидія злочинності традиційно перебуває в компетенції органів державної влади. Однак безперервне зростання використання онлайн-ресурсів і відповідальність уряду за запобігання кіберзлочинам створили екосистему, яка потребує розширення можливостей окремих осіб. Вчений формулює концепцію внутрішніх сфер захисту, щоб показати, як традиційно суспільні обов'язки вимагають посиленого сприяння з боку окремих осіб, щоб належним чином захистити те, що вони цінують. У контексті кіберзлочинності кримінологічні теорії, які обмежено розглядають особу як об'єкт злочину та особу, яка найімовірніше запобіжить йому, швидко застарівають. Органи державної влади або не можуть втручатися, або відмовляються від втручання від імені громадян, щоб ефективно стримувати тиск із боку кіберзлочинців. Таким чином, існує потреба

в підході, який починається з окремих осіб та їх ціннісних мотивацій. Отже, пише вчений, концепція внутрішніх сфер захисту – це новий погляд на запобігання кіберзлочинам. Внутрішні сфери базуються на індивідуальних цінностях, зокрема цінності безпеки, і беруть кіберзнання як відправну точку для захисту таких цінностей, тобто шляхом дій зі зменшення ризику та використання відповідних інструментів.

Крім питань кіберзлочинності та місця людини в цій сфері, дослідники звертають увагу і на окремі прояви злочинної діяльності. Найбільш небезпечним її проявом, з точки зору впливу безпосередньо на людину та її психіку, є кібербулінг або кіберзалякування. Але вивчення цього явища ускладнюється відсутністю єдиного способу його розуміння. На це звертає увагу група вчених з Південної Кореї та Сінгапуру – Дж. Чан, Дж. Лі, Дж. Кім, С. Лі [12]. Виктимізація кібербулінгу, пишуть вони, є міжнародним явищем, яке швидко поширюється в усьому світі. Однак дослідження показали суперечливі висновки щодо визначення, вимірювання та поширеності віктимізації та вчинення кібербулінгу. Щоб надати огляд шкал, що існують, і запропонувати шляхи стандартизації вимірювання кіберзалякування, вчені проаналізували 64 міжнародних дослідження вимірювання кіберзалякування з використанням таких категорій: загальні характеристики, визначення кіберзалякування, характеристики вибірки дослідження, розмір вибірки, тип – пристрій або соціальні медіа, часові рами, тип опитування, метод об'єднання елементів, субшкали, надійність і валідність. Цей аналіз показав, що тільки 46 з 64 досліджень пояснюють поняття «кібербулінг». Крім того, лише 15 досліджень повністю або частково дотримувались рекомендованих методик при розробленні шкали. Хоча більшість інструментів кіберзалякування, на думку вчених, показали помірну або високу надійність, при цьому лише половина досліджень оцінювала валідність вимірювань кіберзалякування, причому значна частина з них перевіряла валідність конструкції. На основі цього дослідники дійшли висновку, що існує потреба в узгодженому та стандартизованому визначенні кіберзалякування для використання в усьому світі, яке може бути найважливішим фактором у вимірюванні поведінки кіберзалякування.

Цьому ж питанню приділяють увагу й австралійські вчені В. Шинода, К. Бассі та Т. Джонс [13]. Сфера кіберзалякування, на їхню думку, швидко розширилася за останні 20 років і особливо робить сильний акцент на різноманітних маргінальних групах молоді. Проте автори звертають увагу на те, що література в цій галузі, визначає кіберзалякування дуже різними способами, не враховуючи того, як різні групи молоді самі визначають і застосовують термін «кіберзалякування». Дослідники розглядають, як культурне, сексуальне та гендерне розуміння та інтерпретація кібербулінгу молодими людьми можуть бути використані для усунення прогалин у сучасних академічних

уявленнях про кібербулінг (це явище). Авторами було проведено напівструктуровані інтерв'ю з 19 молодими людьми, які дали інформацію про їх розуміння, інтерпретацію та досвід кібербулінгу. Отримані вченими дані значною мірою свідчать про те, що плутанина щодо терміну та визначення кіберзалякування серед дослідників також відображається на популяції різних молодих людей, які розуміють та інтерпретують кіберзалякування. Незрозуміло, чи було ці суперечливі визначення пов'язано з плутаниною серед молоді, чи з тим, що вчені та політики не змогли повідомити громадськості чітке визначення кіберзалякування. Як результат, вчені дають пропозиції щодо мови та поведінки, які слід включити у визначення кіберзалякування, щоб більш чітко донести цю концепцію до майбутніх респондентів та ширшої спільноти.

Питання віктимізації на прикладі Фінляндії порушують дослідники з цієї країни М. Ньосі, П. Даніельсон та М. Каакінен [14]. Вони розглядають поширеність різних типів віктимізації кіберзлочинності та їх спільні фактори ризику серед населення Фінляндії. Автори досліджують, як соціально-економічні зміни в житті респондентів, їхній минулий досвід офлайн-віктимізації, онлайн-активність, навички користувача та заходи захисту впливають на ризик найпоширеніших форм онлайн-віктимізації та онлайн-полівіктимізації. Згідно з їхніми висновками, п'ятьма найпоширенішими формами віктимізації були зловмисне програмне забезпечення, переслідування, сексуальні переслідування, хакерство та шахрайство. Повсякденні дії в інтернеті та контакти з потенційними правопорушниками разом із минулим досвідом віктимізації офлайн слугували помітними факторами ризику для низки різних досвідів віктимізації в інтернеті. Вчені показують дещо різні фактори ризику для віктимізації різних онлайн-правопорушень, тим самим вказуючи на різноманітний характер різних типів онлайн-віктимізації. Як висновок вчені показують, що молодий вік, кращий фінансовий стан, активне використання інтернету та навички користувача, а також минула офлайн-віктимізація майнових злочинів і насильства пов'язані з підвищеним ризиком полівіктимізації в інтернеті. Високий захист користувачів, на їхню думку, зменшує ризик полівіктимізації в Інтернеті.

Цій же проблемі приділяють увагу і нідерландські вчені Р. Нотте, Е. Люкфелдт, М. Мелш [15]. Вони досліджують вплив віктимізації онлайн-злочинів. На їхню думку, більшість наслідків онлайн-порушень відповідають наслідкам традиційних офлайн-порушень, хоча, як вважають автори, існують також відмінності, щодо офлайн-віктимізації. Декілька форм впливу, здається їм, є специфічними для жертв онлайн-злочинів: значний масштаб і видимість віктимності, віктимізація, яка не припиняється вчасно, переплетення онлайн- і офлайн-злочинів і звинувачення жертви. Жертви страждають від подвійних, потрійних і навіть четверних ударів; саме накопичення різних типів впливу,

викликане необмеженістю в часі та просторі, робить віктимізацію онлайн-злочинів настільки інвазивною. Крім того, особливості віктимізації онлайн-злочинів значно ускладнюють боротьбу з онлайн-злочинністю та запобігання їй. Нарешті, роблять висновок вчені, висока поширеність віктимізації від кіберзлочинів у поєднанні з серйозним впливом цих злочинів суперечить громадській думці та пов'язана з моральним судженням щодо жертв. Подальші дослідження, завершують нідерландські дослідники, домінантного суспільного дискурсу щодо віктимізації та того, як це впливає на роботу поліції та підтримку жертв, були б цінними.

Окремою проблемою, яка досліджується в межах кібербулінгу, є проблема свідків у ньому. Це питання розглядає група канадських учених – Д. Пеплер, Ф. Мішна, Дж. Дукет і М. Ламейро [16]. Вони вивчали уявлення молоді про природу та дилеми бути стороннім спостерігачем у кібербулінгу. Незважаючи на те, що взаємодія з однолітками через соціальні мережі має багато переваг, існують ризики, пишуть автори, зокрема, кіберзалякування. Спостерігачі є невід'ємною частиною динаміки та шкоди як під час особистої зустрічі, так і під час кіберзалякування. Використовуючи якісний підхід, вчені діляться думками молоді про досвід свідків кібербулінгу та про дилеми, з якими вони стикаються, вирішуючи, чи підтримати однолітка і як відповісти. Науковці провели тематичний аналіз якісних інтерв'ю з шістнадцятьма підлітками. Молоді люди описували низку почуттів, які відчували як свідки: від дискомфорту та гніву до моральної незаангажованості та виправдання кіберзалякування. Молодь повідомила про три форми ролей сторонніх спостерігачів: аутсайдера, помічника та захисника, що відповідає традиційному булінгу. При цьому канадські дослідники роблять висновок: вирішення проблеми кібербулінгу, на думку молоді, лежить на плечах дорослих.

Висновок. Сьогодні вже можна впевнено говорити про те, що кіберзлочинність – це дуже велика сфера кіберпростору. Якщо раніше вона зростала за рахунок економічних злочинів, то сьогодні вона все більше охоплює злочини проти людини, зокрема її психічного здоров'я. Приклад кібербулінгу показує, що все частіше кіберпростір використовується як механізм тиску на людину з метою отримання певної нематеріальної вигоди. Кібербулінг став новим способом заподіяння шкоди особі поряд, наприклад, із фізичною. Таким чином, кіберпростір розширює злочинні можливості шахраїв та злочинців, і це вимагає пошуку ефективних способів захисту. Такому пошуку сприяє те, що людина в кіберпросторі переважно керується тими ж мотивами, що і в матеріальному світі. Це, своєю чергою, дозволяє використовувати вже існуючі механізми захисту. Але зростання технологічного рівня кіберзлочинност-

ті вимагає створення й нових підходів, що базуються на її технічній стороні (розвиток програмного забезпечення тощо).

У цілому необхідно констатувати, що кіберзлочинність стає все більше небезпечною. Винахідливість кіберзлочинців вимагає значної активізації як правоохоронних органів, так і наукової спільноти для подальшої протидії цьому злочинному інституту.

ЛІТЕРАТУРА

1. Grigorescu A., Chitescu R. Cyberspace – a challenge. *6th International Academic Conference on Strategica – Challenging the Status Quo in Management and Economics* : proceedings 6th International Academic Conference on Strategica – Challenging the Status Quo in Management and Economics. Bucharest, 2018. P. 824–838.
2. Adamson G. Cybersecurity as the protection of cyberspace. IEEE International Symposium on Technology and Society (ISTAS-21) – Technological Stewardship and Responsible Innovation: proceedings IEEE International Symposium on Technology and Society (ISTAS-21) – Technological Stewardship and Responsible Innovation. Ontario, 2021. P. 1–8.
3. Zhang Z., Yin R., Ning H. Internet of Brain, Thought, Thinking, and Creation. *Chinese journal of electronics*. 2022. №31 (6). P. 1025–1042. URL: https://www.researchgate.net/publication/369157811_Internet_of_Brain_Thought_Thinking_and_Creation (Last accessed: 15.02.2024).
4. Gálik S. Influence of cyberspace on changes in contemporary education. *Communication today*. 2017. №8 (1). P. 30–38.
5. Mincewicz W. Explication and Classification of Social Deviations on the Internet: Cyberdeviation as a New Social Phenomenon. *Polish sociological review.* 2023. №222. P. 231–247. URL: https://polish-sociological-review.eu/pdf-168949-91811?filename=Explication%20and.pdf (Last accessed: 15.02.2024).
6. Pineda F. Computer crime. *Revista general de derecho procesal*. 2020. №50. P. 202–212.
7. Vera F., Guirao J., Infantes A. Security in cyberspace from a sociocultural perspective. *Methaodos-revista de ciencias sociales.* 2022. №10 (2). P. 243–258. URL: https://www.methaodos.org/revista-methaodos/index.php/methaodos/article/view/577/865 (Last accessed: 15.02.2024)
8. Chen S., Hao M., Ding F., Jiang D., Dong J., Zhang S., Guo Q., Gao C. Exploring the global geography of cybercrime and its driving forces. *Humanities & social sciences communications*. 2023. №10 (1). P. 1–10. URL: https://www.nature.com/articles/s41599-023-01560-x (Last accessed: 16.02.2024).
9. Leukfeldt E., Roks R. Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes. *Deviant behavior*. 2021. №42 (110). P. 1458–1469.

10. Dupont B., Holt T. The Human Factor of Cybercrime. *Social science computer review*. 2022. №4 (40). P. 860–864.
11. Kikerpill K. The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. *Kybernetes*. 2021. №50 (4). P. 1015–1026.
12. Chun J., Lee J., Kim J., Lee S. An international systematic review of cyberbullying measurements. *Computers in human behavior*. 2020. №113. Article 106485. URL: https://www.sciencedirect.com/science/article/abs/pii/S0747563220302375?via%3Dihub (Last accessed: 17.02.2024).
13. Sheanoda V., Bussey K., Jones. T. Sexuality, gender and culturally diverse interpretations of cyberbullying. *New Media & Society*. 2024. Vol. 2 (1). P. 154–171.
14. Näsi M., Danielsson P., Kaakinen, M. Cybercrime Victimisation and Polyvictimisation in Finland-Prevalence and Risk Factors. *European journal on criminal policy and research*. 2023. №29 (2). P. 283–301.
15. Notté R., Leukfeldt E., Malsch M. Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International review of victimology*. 2021. №27 (3). P. 272–294.
16. Pepler D., Mishna F., Doucet J., Lameiro M. Witnesses in Cyberbullying: Roles and Dilemmas. *Children & schools*. 2021. №43 (1). P. 45–53.

REFERENCES

1. Grigorescu, A., Chitescu, R. (2018). Cyberspace – a challenge. 6th International Academic Conference on Strategica – Challenging the Status Quo in Management and Economics: proceedings 6th International Academic Conference on Strategica – Challenging the Status Quo in Management and Economics. Bucharest, *824–838.*
2. Adamson, G. (2021). Cybersecurity as the protection of cyberspace. IEEE International Symposium on Technology and Society (ISTAS – 21) – Technological Stewardship and Responsible Innovation: proceedings IEEE International Symposium on Technology and Society (ISTAS – 21) – Technological Stewardship and Responsible Innovation. Ontario, *1–8.*
3. Zhang, Z., Yin, R., Ning, H. (2022). Internet of Brain, Thought, Thinking, and Creation. *Chinese journal of electronics, 31 (6), 1025–1042.* URL: https://www.researchgate.net/publication/369157811_Internet_of_Brain_Thought_Thinking_and_Creation.
4. Gálik, S. (2017). Influence of cyberspace on changes in contemporary education. *Communication today, 8 (1), 30–38.*
5. Mincewicz, W. (2023). Explication and Classification of Social Deviations on the Internet: Cyberdeviation as a New Social Phenomenon. *Polish sociological review, 222, 231–247.* URL: https://polish-sociological-review.eu/pdf-168949-91811?filename=Explication%20and.pdf.

6. Pineda, F. (2020). Computer crime. *Revista general de derecho procesal, 2020, 50, 202–212.*
7. Vera, F., Guirao, J., Infantes, A. (2022). Security in cyberspace from a sociocultural perspective. *Methaodos-revista de ciencias sociales, 10 (2), 243–258.* URL: https://www.methaodos.org/revista-methaodos/index.php/methaodos/article/view/577/865.
8. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities & social sciences communications, 1 (1), 1–10.* URL: https://www.nature.com/articles/s41599-023-01560-x
9. Leukfeldt, E., Roks, R. (2021). Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes. *Deviant behavior, 42 (110), 1458–1469.*
10. *Dupont, B*., Holt, T. (2022). The Human Factor of Cybercrime. Social science computer review, 4 (40), 860–864.
11. Kikerpill, K. (2021). The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. *Kybernetes, 50 (4), 1015–1026.*
12. Chun, J., Lee, J., Kim, J., Lee, S. (2020). An international systematic review of cyberbullying measurements. *Computers in human behavior, 113, 106485*. URL: https://www.sciencedirect.com/science/article/abs/pii/S0747563220302375?via%3Dihub
13. Sheanoda, V., Bussey, K., Jones, T. (2024). Sexuality, gender and culturally diverse interpretations of cyberbullying. *New Media & Society, 26 (1), 154–171.*
14. Näsi, M., Danielsson, P., Kaakinen, M. (2023). Cybercrime Victimisation and Polyvictimisation in Finland-Prevalence and Risk Factors. *European journal on criminal policy and research, 2 (2), 283–301.*
15. Notté, R., Leukfeldt, E., Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International review of victimology, 27 (3), 272–294.*
16. Pepler, D., Mishna, F., Doucet, J., Lameiro, M. (2021). Witnesses in Cyberbullying: Roles and Dilemmas. *Children & schools, 43 (1), 45–53.*

Trofymenko Volodymyr Anatolevich, candidate of Legal Sciences, assistant professor, Department of Philosophy, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.

HUMAN AS OBJECT OF CYBERCRIME

Every sphere of social existence has two sides: positive and negative. This did not escape cyberspace either. Cybercrime, as a sphere of cyberspace, is constantly growing,

being content-wise and technologically updated. One of the rapidly developing areas of cybercrime is cyberbullying, the purpose of which is to influence the human psyche. Thus, cybercriminals master new ways of influencing people. In turn, I demand the intensification of scientific developments in this field

Keywords: *cyberspace, cybercrime, bullying, cyberbullying, technological progress, mental damage.*