УДК 340.12
DOI: HTTPS://DOI.ORG/10.21564/2663-5704.57.276665

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

РІЗНОМАНІТНІСТЬ ІСНУВАННЯ ЛЮДИНИ В КІБЕРПРОСТОРІ ЯК ОСНОВА ФОРМУВАННЯ АНТРОПОЛОГІЧНОГО НАПРЯМУ ЙОГО ДОСЛІДЖЕННЯ

У публікації досліджуються різноманітні аспекти існування людини в кіберпросторі. Звертається увага на те, що сьогодні кіберпростір є необхідною умовою нормальної життєдіяльності людини. Він охопив як старі, традиційні сфери людського життя, так і створює нові, потребу в яких викликає сучасний розвиток суспільства. Звертається увага і на проблему кіберзлочинності як явище, що теж отримало розвиток у цифровій реальності. У цілому публікацією доводиться необхідність існування антропологічного напряму дослідження кіберпростору.

Ключові слова: *кіберпростір, законослухняний користувач, кіберзлочинність, кіберзлочинець, антропологічний напрям.*

Постановка проблеми. Кіберпростір усе більше поглинає суспільне життя. Людина набуває все більше життєвої потреби використовувати його можливості. Це спрощує та полегшує її життя, реалізує бажання, економить час. Але кіберпростір потребує певних технічних посередників, опанування яких стає вже сьогодні необхідним і нагальним. Людина в результаті такого опанування стає більш освіченою і краще починає розуміти всі аспекти діяльності в ньому, зокрема і злочинний. Кіберзлочинність сьогодні поширюється як змістовно, так і кількісно. Прикладом може слугувати статистика кібер-злочинності в Україні [1]. Але технічні засоби не можуть провести аналіз того, з якою метою та наміром людина відвідує кіберпростір. Спеціалісти можуть створювати певні технічні заборонні механізми та обмеження, але людський аспект «залізо» все одно не зможе не те що виокремити, а і просто обмежити. З цього важливо сказати наступне. Людина в кіберпросторі є і об'єктом, на який спрямовано певні кібердії та трансакції, і суб'єктом, який користується кіберпростором для задоволення своїх законних та незаконних потреб. Фак-

тично людина є центральною особою в кіберпросторі, що вимагає критичного осмислення її ролі в ньому. Важливо дослідити всі складові людини: фізичні, психологічні, раціоналістичні у призмі застосування їх у кіберсфері. Це допоможе виховати добре підготовленого, законослухняного користувача, створити ефективні механізми його захисту в мережі, притягати кіберзлочинців до відповідальності, запобігати скоєнню злочинів у кібернетичному просторі, проводити ефективну профілактичну діяльність.

Аналіз останніх досліджень та публікацій. Розгалуженість кіберпростору, його постійне розширення, зростання уваги до проблеми кібербезпеки відкрила науковій спільноті нові напрями досліджень.

На зростанні популярності та актуальності дослідження взаємоіснування людини та кіберпростору звернув увагу хорватський вчений Н. Свілічіч [2]. Як різновид антропології, пише він, кіберантропологія вважається найбільш швидкозростаючою підгалуззю в науці. Вона, на його думку, базується на синергічних ефектах мультимедійних систем і гіпермедіа, використовуючи їхні порівняльні переваги. Після цього вчений звужує предмет свого дослідження і вивчає вплив на людину офлайн- та онлайн-носіїв однакового контенту. Але, на думку автора, позиція хорватського науковця дещо звужує коло кіберантропології до взаємодії людини з мультимедійними системами і сприйняття нею медійного контенту. Жалкують про обмеженість використання людського фактору в кіберпросторі нідерландські вчені Х. Юнг, Т. ван Влієт, Дж. ван де Вен, С. Джоль та К. Брокмен [3]. Людський фактор, звертають увагу вони, значною мірою відсутній у широкому діалозі про кібербезпеку, і його сфера часто обмежена. Вчені пропонують розглядати кібербезпеку як стан системи. Зміни в цій системі викликані поведінкою суб'єкта. Втручання – це способи зміни поведінки суб'єктів для запобігання небажаній поведінці та посилення бажаної поведінки. При виборі втручання слід враховувати динамічний характер того, як люди використовують кіберпростір. Люди навряд чи змінять колишню поведінку відразу. Головне, вважають науковці, винайти нові способи зберегти стару поведінку в нових обставинах. Вони розрізняють три основних шляхи поведінки суб'єктів, які впливають на кібербезпеку системи: рефлекс, звичку та продуманий шлях. Урахування цих систем справді полегшує зусилля щодо розроблення успішних втручань. З цієї публікації можна зробити висновок, що людський фактор є центральним елементом системи виховання законослухняного користувача.

На вплив інтернету та кіберпростору на поведінку споживачів звертає увагу колектив учених Дж. Саура, А. Рейєс-Мендес, Н. де Матос, М. Корійя та П. Палос-Санчес [4]. Вони відмічають, що в останні десятиліття інтернет, новітні технології та соціальні медіа привели до еволюції поведінки споживачів. Зміни в поведінці клієнтів, викликані цифровими розробками, створю-

ють багато можливостей і викликів, з якими компаніям також доводиться мати справу в інтернеті. Чим краще компанії знають про поведінку своїх клієнтів, тим легше вони можуть взаємодіяти з ними за допомогою таких стратегій, як користувальницький досвід, впливовий маркетинг, контент, створений користувачами, електронне радіомовлення тощо. Ці стратегії є важливими в тому числі і для збільшення продажів і розвитку онлайн-бізнесу, оскільки такі стратегії збільшують взаємодію з користувачами та впливають на їх поведінку. Тому, вважають науковці, необхідно зосередитись на аналізі поведінки споживачів в епоху цифрових технологій.

Підсумовуючи цей невеликій аналіз публікацій, можна констатувати поворот кіберпростору в бік звичайної людини, яка стає його основним користувачем. У свою чергу, це спонукає розширення та збільшення кількості відповідних наукових досліджень.

Формулювання мети. Однією з цілей публікації є показати, як людські навички, звички, розум, емоції тощо можуть впливати на розвиток кіберпростору та сфери кібербезпеки зокрема. Наступною метою цієї статті також є з'ясування антропологічних причин кіберзлочинності. Фінальним завданням роботи є довести необхідність існування антропологічного напряму дослідження кіберпростору.

Викладення основного матеріалу. Кіберпростір створений людиною для самої людини. Але рівень користувача вже з перших кроків у кіберпросторі відкрив людині усі його можливості. У ньому відтворюються практично всі соціальні інститути з притаманними їм позитивними та негативними рисами.

Тому вже сьогодні виділяють:

«– Поверхневий, або видимий, інтернет (з англійської Surface Web): та частина глобальної мережі, яка індексується пошуковими системами на кшталт Google або Bing.

– Глибокий інтернет, або «невидима мережа» (з англійської Deep Web): повна протилежність «поверхневому інтернету». У глибокій павутині знаходяться вебсторінки, не пов'язані з іншими гіперпосиланнями, а також сайти, доступ до яких відкритий тільки для зареєстрованих користувачів, та інтернет-сторінки, доступні тільки за паролем.

– Даркнет, «темний інтернет» (з англійської Darknet): повністю анонімна, нерегульована і нікому не підконтрольна частина інтернету. Він недоступний для звичайних користувачів. Доступ у нього можна отримати тільки за допомогою спеціальних програм…Темна сторона «даркнету» готова запропонувати весь спектр протизаконних послуг: кібершахрайство, виробництво шок-контенту, вимагання, послуги хакерів, продаж наркотиків або зброї, схеми афер і багато іншого» [5].

Як можна побачити, якщо перші два шари кіберпростору використовуються для досягнення законних цілей, то даркнет надає прихисток та необхідні можливості кіберзлочинцям. Таким чином, їм ніхто і ніщо не заважає скоювати свої злочинні дії. Тому необхідно піти шляхом виховання захищеного законослухняного користувача. Складність такої виховної роботи постає в необхідності врахування багатьох сторін життя людини: вік, стать, рівень освіти, забезпеченість приладдям, доступ до інтернету та його швидкість, її бажання і цілі, емоційний стан тощо. І цим вже активно займається наукова спільнота.

Так, змінювати поведінку людини через кіберпростір пропонує група науковців – Ч. Пайндер, Дж. Вермелен, Б. Коуен та Р. Біль [6]. Цифрові втручання, пишуть вони, спрямовано на зміну поведінки, особливо ті, що використовують поширені обчислювальні технології, мають великі надії на підтримку користувачів у зміні їхньої поведінки. Однак більшість втручань не враховують звичну поведінку, обмежуючи їхній потенційний вплив. Ця невдача, відзначають автори, частково спричинена великою кількістю теорій зміни поведінки, що збігаються, і пов'язаних із ними стратегій, які не враховують ролі звичок. Вони підкреслюють потенціал теорії подвійних процесів, сучасної теорії звичок і теорії постановки цілей, які разом моделюють те, як користувачі формують звички та позбавляються їх, щоб стимулювати ефективне цифрове втручання. З цього вони формулюють власну модель зміни звички. Таким чином, науковці доводять можливість кіберпростору впливати в тому числі і на формування законослухняного користувача, позбавлення користувача «поганих» звичок.

Водночас уже висловлюються певні побоювання щодо негативного впливу втручання кіберпростору на поведінку людини та формування цифрової нерівності. Про це пишуть тайванські вчені Т.-К. Ю, М.-Л. Лін, Й.-К. Ляо [7]. Цифрова нерівність, відзначають вони, є однією з найбільш критичних проблем в «інформаційну епоху», небагато досліджень вивчали соціальну нерівність в інформаційних ресурсах і моделях цифрового використання. У сільській місцевості засоби інформаційно-комунікаційних технологій не можуть гарантувати, що користувачі зможуть легко отримати доступ до інформаційних технологій і подолати так званий «цифровий розрив». Автори стверджують, що психологічні чинники впливають на поведінку щодо упровадження інформаційно-комунікаційних технологій, сповільнюючи їхній ефект. Виходом є навчання елементів інформаційної грамотності та формування цифрових навичок через систему освіти. Соціалізація, яка відбувається у процесі освіти, покращує також рівень медіанасиченості, медіадосвіду і медіатехнічного стресу, що, у свою чергу, покращує поведінку щодо упровадження інформаційно-комунікаційних технологій. Такий підхід, підбивають підсумок науков-

ці, повинен стати елементом державної політики. На провідну роль освіти та політики звертає увагу і бразильська вчена К. Ачутті [8]. Цифрова ера, пише вона, породила численні форми грамотності: цифрову грамотність і технологічну грамотність, наприклад. Це означає, що нинішні педагоги повинні переходити від традиційної навчальної програми до більш інноваційної, не маючи належного керівництва. Кожен повинен піклуватись про розвиток цифрової та технологічної грамотності покоління, що навчається. Виходячи з розвитку суспільства, продовжує вчена, необхідно змінювати мислення політиків та освітян. Вони здатні спричинити величезну трансформацію в освітній системі.

На негативні психологічні аспекти поведінки споживачів у кіберпросторі звертають увагу і словацькі науковиці Дж. Рібанська, І. Косічарова та Л. Негова [9]. Сьогодні, відмічають вони, людство вже знає, який величезний вплив на його життя має цифровізація суспільства. Існує кілька ключів до виявлення процесів споживчої поведінки та прийняття рішень. Якщо необхідно зрозуміти, як споживачі приймають рішення на цифровому ринку, по-перше, потрібно зрозуміти самого споживача – споживача як емоційну людину зі специфічними емоціями та потребами. Як і на ринку товарів і послуг, зазначають авторки, на цифрових ринках споживачі зустрічаються з тими ж інструментами маркетингової комунікації, але в різних формах, в основному з електронною рекламою в різних формах. Незважаючи на відому високу ефективність електронної комерції, науковиці виявили багато негативів і небезпек цього інструменту в цифровому середовищі. Цифрова реклама, особливо та, що спливає, викликає значні негативні емоції. Вчені стверджують, що особистість споживача є значущим предикатором реакції споживачів на цифровому ринку. Таким чином, цифрове середовище приносить не тільки переваги, але й нові проблеми, недовіру, стрес і відразу споживачів.

На прикладі Ізраїлю ще на одну небезпеку у кіберпросторі – нерівність у цифрових навичках – звертають увагу вчений з Уругваю М. Додел та ізраїльський вчений Дж. Меш [10]. Поведінка з точки зору кібербезпеки, відзначають вони, є важливою для запобігання втраті цифрових активів особи та забезпечення безпеки важливих щоденних дій в інтернеті. Кібербезпека окремих людей також має вирішальне значення для національної кібербезпеки. Це питання дуже актуальне для Ізраїлю, країни, яка покладається на цифрові можливості своїх працівників у своїх основних технологічних галузях, а також часто стає об'єктом кібервійни та атак кіберзлочинців. Для дослідників метою цього дослідження є виявлення детермінантів кібербезпекової поведінки. До таких вони відносять вік, стать, рівень освіти та їхній вплив на цифрові навички, пов'язані з безпекою. Автори виводять чіткий зв'язок між цима детермінантами та якістю доступу до інтернету з рівнем навичок

цифрової безпеки користувачів. Як висновок, вони розширюють розуміння кібербезпеки, показуючи, що соціальна та цифрова диспропорції відтворюються у використанні заходів для запобігання онлайн-загрозам, піддаючи цифрових незаможних осіб більшому ризику стати жертвами онлайн-загроз.

Зважаючи на викладене вище, недарма висловлюється позиція про необхідність розвитку цифрових навичок у користувачів. На важливість та необхідність розвитку цифрових навичок звертають увагу німецькі вчені Е. Остмейєр та М. Стробел [11]. Цифрова трансформація, звертають увагу вони, змінює навички працівників, необхідні організаціям для успіху. У цьому контексті для працівників стає дедалі важливішим активно розвивати свої навички. Автори відмічають, що нові дослідження про проактивний розвиток навичок співробітників значною мірою ігнорували можливу роль сприйняття співробітниками широкомасштабних змін в організаційному середовищі в їхній мотивації брати участь у такій цінній поведінці. Вони усувають цю прогалину за допомогою упровадження теорії когнітивно-афективної системи особистості, щоб пояснити, як розвиток макрорівня впливає на поведінку працівників. Результати підтверджують гіпотезу про позитивний непрямий вплив цифрової зрілості галузі на проактивний розвиток навичок через інтерпретацію співробітниками цифровізації як контрольованої та можливості для їхньої організації.

Усі наведені вище приклади свідчать про необхідність упровадження всеосяжної та всеохопної системи цифрової грамотності. Але вже на рівні її розуміння ставиться питання: вона повинна бути локальною чи універсальною? Це питання ставить колектив науковців Л. Пангазіо, А. Гудх, Л. Ледесма та А. Гонсалез [12]. Багато вчених у всьому світі, пишуть вони, вивчали знання, навички та схильності, необхідні для використання цифрових медіа. Проте, оскільки цифрові тексти поширювалися та розвивалися, було багато припущень щодо того, що означає мати «цифрову грамотність». Як і дослідники грамотності з Австралії, Швеції та Аргентини, автори стурбовані прагненням стандартизувати визначення «цифрової грамотності», незважаючи на помітні відмінності в культурній політиці освіти в кожній країні. Вони аналізують, як термін «цифрова грамотність» був концептуалізований і застосований вченими в цих трьох мовних контекстах. Для цього вони досліджують найбільш цитовані публікації з цифрової грамотності в англомовних, скандинавських та іспаномовних наукових публікаціях. Вчені роблять висновок про різноманітність визначень у кожному контексті та всередині кожного контексту, основні суперечності та проблеми, що виникають, а також наслідки для навчання цифровій грамотності. Вони відзначають, що подібні напруження та виклики існують у всіх трьох контекстах, однак шлях до розв'язання залежить від контекстуальних відмінностей. Як висновок, вчені визнають і об-

стоюють необхідність локальних концептуалізацій цифрової грамотності в освітніх системах, що все більше глобалізуються.

Незважаючи на концептуальні проблеми в рамках цифрової грамотності, пропонується вирішення певного кола проблем, які виникають у користувачів кіберпростору. Однією з таких проблем є дезінформація, яка поширюється через кіберпростір. Її порушують малазійські вчені Л. Антонісамі та П. Сівакумар [13]. Вони звертають увагу, що останніми роками занепокоєння щодо дезінформації викликало відновлення інтересу до аспекту цифрової грамотності. Багато молодих людей у Малайзії не можуть відрізнити справжні новини від фейкових. Хоча є багато досліджень, які вивчають фейкові новини, дослідження, які вивчають пом'якшення дезінформації крізь призму цифрової грамотності, усе ще є рудиментарними. У призмі впливу дезінформації на користувачів вчені звертаються до розгляду складових цифрової грамотності: технічної, когнітивної грамотності та соціально-емоційної грамотності. Як результат вони стверджують, що дві з трьох сфер компетенції цифрової грамотності, технічна грамотність і когнітивна грамотність, мають позитивний зв'язок у зниженні дезінформації серед студентів університетів; однак соціально-емоційна грамотність має протилежний ефект. Крім того, твердять вчені, гедонічна мотивація допомагає пом'якшити дезінформацію, тоді як звичка – ні. Таким чином, на їхню думку, цифрова грамотність може допомогти у виявленні дезінформації, яка маскується під достовірну інформацію, шляхом належної перевірки та аналізу, особливо в епоху цифрових технологій, коли кожен сприйнятливий до дезінформації. У свою чергу, це потребує розроблення нової основи самої цифрової грамотності.

Взаємовплив цифрової грамотності та психологічної вразливості вивчають англійські вчені Е. Хелспер та Д. Смахел [14]. Вчені поєднують клінічно-психологічну та цифрову грамотність, щоб пролити нове світло на пояснення надмірного використання інтернету (EIU). Поєднання цих протилежних підходів, на їхню думку, призводить до більш повного пояснення інтенсивного використання з негативними наслідками. Автори показують, що між змінними психологічної та цифрової грамотності та EIU існують взаємозалежні та непрямі зв'язки. Психологічно вразливі діти з вищим рівнем цифрової залученості мають найбільш негативні наслідки, тоді як найменш ризиковані невразливі діти з високим рівнем грамотності (взаємовідносини). Насправді, твердять дослідники, ризик негативних наслідків для психологічно вразливих дітей посилюється їхньою схильністю проводити більше часу в інтернеті, але протистоїть їхньому нижчому рівню грамотності (що суперечить прямим і непрямим стосункам). Серед тих, хто не є вразливим, цифрова грамотність слабко пов'язана з негативними результатами. Наслідки цих результатів, на думку англійців, для майбутніх досліджень полягають у тому, що пояснен-

ня щодо EIU мають включати психологічні показники та показники цифрової грамотності. Практичні наслідки полягають у тому, що клінічні психологи, які працюють з EIU, повинні враховувати цифрову грамотність при розробленні втручань, а втручання з цифрового залучення повинні враховувати потенційний негативний вплив збільшення використання інтернету на вразливу молодь.

Включити вивчення психології в освіту з кібербезпеки пропонує англо-австралійська група вчених Дж. Тейлор-Джексон, Дж. Мак Аланей, Дж. Фостер, А. Белло, А. Марушат та Д. Дейл [15]. Роль людини в кібербезпеці, констатують вони, добре визнана. Багато інцидентів кібербезпеки залежать від цілей, які виконують певні поведінкові дії, наприклад відкривають посилання у фішинговому електронному листі. Самими кіберсупротивниками керують такі психологічні процеси, як мотивація, групова динаміка та соціальна ідентичність. Крім того, як навмисні, так і ненавмисні внутрішні загрози пов'язані, на думку авторів, з рядом психологічних факторів, включаючи когнітивне навантаження, психічне благополуччя, довіру та міжособистісні стосунки. Включивши психологію в освіту з кібербезпеки, фахівці-практики отримають навички, необхідні для вирішення проблем кібербезпеки. Однак вчені вважають, що є і певні труднощі. Психологія є широкою дисципліною, і багато теорій, підходів і методів можуть мати незначне практичне значення для кібербезпеки. Необхідно переглянути літературу, щоб визначити, що можна застосувати до кібербезпеки. Вчені відмічають, що існують також педагогічні відмінності в тому, як викладають психологію та кібербезпеку, а також психологічні відмінності в типах студентів, які зазвичай можуть вивчати психологію та кібербезпеку. Щоб спілкуватися зі студентами з кібербезпеки, важливо, щоб ці відмінності були виявлені та позитивно розглянуті. Суттєвим для цих зусиль, як висновок дослідників, є необхідність обговорення та співпраці між двома дисциплінами.

Проблема старіння населення нашої планети стає все серйознішою [16]. Тож не дарма науковці вже звертаються до вивчення ставлення людей похилого віку до кіберпростору. Цю проблему розглядають китайські дослідники К. Лі та І. Лаксімон [17]. У наш час, констатують вони, з суспільством, що старіє, зростає кількість людей похилого віку, які є поточними або потенційними користувачами цифрових технологій. Однак те, як люди похилого віку сприймають і використовують цифрові технології, не привертає достатньої уваги дослідників. Предметом їхнього дослідження є відчуття, сприйняття літніми людьми цифрових технологій і поведінка їх у Гонконзі та досвід щоденного використання цифрових технологій. У результаті автори показали, що люди похилого віку позитивно ставляться до використання цифрових технологій, але менше впевнені у своїх власних можливостях вивчення цих

технологій. Більшість таких людей мають труднощі під час використання та вивчення цифрових технологій, особливо проблеми з навігацією. Крім того, серед літніх людей спостерігається тенденція використання мобільних комп'ютерів замість комп'ютерів. Тому вони пропонують: враховуючи особливі потреби та обмеження людей похилого віку в майбутньому проєктуванні цифрових технологій, можна забезпечити кращий досвід користувача. Ще на одну цікаву демографічну проблему – залежність щастя сільського населення з низьким забезпеченням від цифрової грамотності – звертають увагу інші китайські вчені: Дж. Ванг, Л. Чанг та Ж. Каі [18]. Підвищення рівня щастя сільського населення, стверджують вони, є важливою ознакою ефективності управління відносною бідністю. У контексті сучасної цифрової економіки оцінка зв'язку між цифровою грамотністю та суб'єктивним щастям малозабезпечених сільських груп є дуже практичною. Вченими був виявлений значний ефект щастя цифрової грамотності для сільських груп із низьким доходом. Цифрова грамотність, на їхню думку, сприяє суб'єктивному щастю груп із низькими доходами в сільській місцевості через збільшення доходу та зростання споживання. Спостережуваний ефект щастя неоднорідний серед різних характерних груп, і цифрова грамотність значно позитивно впливає на суб'єктивне щастя груп із низькими доходами в сільській місцевості. Декомпозиція суб'єктивного щастя на задоволеність життям і задоволеність роботою, доводять автори, показує, що цифрова грамотність суттєво позитивно впливає на роботу та задоволеність життям у сільській місцевості з низькими доходами. Для подальшого посилення суб'єктивного впливу цифрової грамотності на добробут у будівництві цифрових сіл вчені пропонують уряду зосередитися на розвитку цифрової грамотності серед груп із низькими доходами з боку попиту. Побудова цифрової інфраструктури повинна активно спиратися на пропозицію.

Але навчання цифрової грамотності, вирішення окремих проблем користувачів у кіберпросторі, з кібербезпеки зокрема, не є кінцевими. Для їхнього ефективного використання користувачі повинні займатись кібергігієною. Але і самої кібергігієни потрібно навчатись. Свій підхід до цього процесу пропонує група американських вчених – А. Нейгел, В. Клейпул, Г. Велдфогл, С. Ахрайя, Г. Хенкок [19]. Кібербезпека, пишуть вчені, має першорядне значення в сучасному кіберзахисті. Одним із важливих факторів, пов'язаних зі зменшенням порушень кібербезпеки, спричинених людьми, є кібергігієна. Кібергігієна, за їхнім баченням, – це адаптивні знання та поведінка для пом'якшення ризикованої онлайн-діяльності, яка ставить під загрозу соціальну, фінансову та особисту інформацію людини, – небезпека, яка значно посилюється, коли обговорюється ризик для цілих країн, а не для окремої людини. Цікаво, що, навіть незважаючи на те, що людина є найбільшою загрозою для кібербезпеки,

дуже мало досліджень вивчали приховані індивідуальні відмінності, пов'язані з розвитком знань, ставлень і поведінки, пов'язаних із кібергігієною. Індивідуальні відмінності, такі як довіра до технологій і внутрішня мотивація, вказували на покращання кібергігієни, але залежали від значних статевих відмінностей. Також з'явилися відмінності між академічними спеціальностями, такими як науково-технічні спеціальності. Нарешті, автори визнають важливість розуміння ролі людського фактору в сучасній кібербезпеці та потенційні практичні наслідки, пов'язані з удосконаленням поточних навчальних програм курсів з комп'ютерних та інформаційних наук.

Але кіберпростір є полем життєдіяльності не тільки законослухняних користувачів. Його можливості, особливо відносно анонімності існування, створюють сприятливі умови для злочинної діяльності. Усі наукові дослідження сьогодні обертаються навколо одного з головних питань: у чому схожість звичайного «офлайн»-злочинця та кіберзлочинця?

На згадану проблему звертає свою увагу нідерландський вчений М. Краненберг [20]. Дослідження кіберзлочинів, пише вчений, зазвичай зосереджуються або на організаційній структурі організованої кіберзлочинності, або на процесах соціального навчання серед окремих осіб. Він пропонує новий погляд на співзлочинство, досліджуючи, наскільки окремі особи є співзлочинцями різних типів кіберзлочинів порівняно з традиційними злочинами. Крім того, він звертає увагу на відмінності в типі співзлочинців (друзі, сім'я чи ін.) і зв'язки між ІТ-знанням і кіберспівзлочинством. Нідерландський дослідник робить висновок, що кіберзлочинність і традиційна злочинність демонструють подібні моделі співзлочинства. Більшість правопорушників, вказує він, вважають за краще вчиняти свої злочини поодинці, але деякі види злочинів частіше вчиняються разом із співвиконавцями, ніж інші види злочинів. Що стосується кіберзлочинності, результати свідчать про те, що обмеження в знаннях правопорушника у сфері ІТ можуть бути причиною шукати співзлочинців із сильними навичками у сфері ІТ.

Цю ж проблему вивчає група науковців з Нідерландів та Німеччини М. Краненберг, Ж.-Л. Ван Гельдер, А. Барендс, Р. де Врайс [21]. Кіберпростір, стверджують вони, створює можливості для нових форм злочинності, які можуть бути пов'язані з конкретними характеристиками особистості правопорушників. Особливості особистості кіберзлочинців, за їхніми спостереженнями, досліджувались недостатньо. Вчені усувають цю прогалину, порівнюючи судову вибірку з 261 підозрюваного в кіберзлочинності, 260 підозрюваних у офлайн-злочинності. Це дає їм змогу створити детальну картину особистості кіберзлочинця: порівняно з підозрюваними в офлайн-злочинах, відмічають науковці, підозрювані кіберзлочинці мають значно нижчі оцінки за екстраверсію та значно вищі за сумлінність і відкритість до досвіду. Кіберзло-

чинці більше схожі на учасників спільноти в цих основних сферах особистості. Що стосується основних аспектів, на думку авторів, підозрювані кіберзлочинці видаються унікальними завдяки відносно високому рівню обачності. Вони більше схожі на підозрюваних офлайн-правопорушників за рисами, які можуть допомогти їм здійснювати злочинну діяльність, наприклад менший рівень скромності, лякливості та гнучкості. Однак вони більш схожі на вибірку спільноти за рисами, які можуть посилити їхню здатність або схильність вчиняти кіберзлочини, наприклад, вищий рівень терпіння, перфекціонізму та розсудливості.

Цікавий підхід у з'ясуванні схожості-несхожості офлайн- та онлайн-злочинності запропонували нідерландські вчені Е. Льокфелд та Р. Рокс [22]. Вони досліджують перетин вуличних злочинів і кіберзлочинів. По-перше, вчені перевірили, чи залучені мережі в цих випадках також до іншої кримінальної діяльності, крім кіберзлочинів. По-друге, вони проаналізували походження та розвиток цих мереж, приділяючи особливу увагу ролі або офлайн-взаємодіям на реальних вулицях. По-третє, вони дослідили, чи містяться у справах відомості, які б свідчили про наявність вуличної культури, що інформує про діяльність правопорушників. Їхній аналіз як кримінальної діяльності, так і походження та розвитку мереж кіберзлочинців показав постійну важливість офлайнового світу. Проте, зазначають нідерландські вчені, результати проливають світло не лише на «приховане обличчя кіберзлочинності». Базуючись на їхніх мовних практиках, мотивах і нейтралізаціях, вони побачили приклади того, як основні члени, рекрутери та грошові мули в різних випадках вбудовані в голландську вуличну культуру. Таким чином, як висновок, завершують вчені, випадки кіберзлочинності також можна інтерпретувати як цифрову диверсифікацію традиційних вуличних (економічних) злочинів і, таким чином, як емпіричні приклади вуличних правопорушників, які адаптуються до розвитку технологій.

На питання, що впливає на кількість кіберзлочинців, намагаються дати відповідь вчені з США, Китаю та Південної Кореї [23]. Дж. Парк, Д. Чо, Дж. Лі та Б. Лі ставлять питання: за яких умов існує більша ймовірність використання інтернету з метою злочинної діяльності? Використовуючи вичерпні дані на рівні штатів у Сполучених Штатах за 2004–2010 рр., вони доходять висновку: немає чітких емпіричних доказів того, що рівень проникнення інтернету пов'язано з кількістю злочинців в інтернеті. Однак, продовжують автори, діяльність кіберзлочинців залежить від соціально-економічних факторів і швидкості з'єднання. Зокрема, вищий дохід, більша освіта, нижчий рівень бідності та вища нерівність, швидше за все, сприятимуть більш позитивному зв'язку проникнення інтернету з кіберзлочинцями, які справді відрізняються від умов наземних злочинів у реальному світі. Крім того, зазначають вчені, на відміну

від вузькосмугового, широкосмугові з'єднання суттєво і позитивно пов'язані з кількістю злочинців в інтернеті, і це посилює вищезгаданий вплив соціально-економічного статусу на злочини в інтернеті. Загалом, закінчують дослідники, для кіберзлочинності потрібен не лише кваліфікований злочинець, а й інфраструктура, яка сприятиме отриманню прибутку від злочину.

Зважаючи на викладене, можна зазначити, що проблема кіберзлочинності та кіберзлочинців набирає обертів. Це пояснюється і зростанням обсягу самого кіберпростору, і зростанням злочинності в ньому.

Висновки. Це дослідження показує, що людина охоплюється кіберпростором з усіх боків. Його вплив на неї вже може розглядатись як основа стабільної та нормальної життєдіяльності користувача. Користувачеві пропонується вже не тільки цифровізація старих, уже наявних інститутів, а й створення нових, без яких людина вже не бачить свого нормального існування. З іншого боку, електронні ресурси кіберпростору створюють можливості для кіберзлочинної діяльності, яка теж потребує вивчення з метою подолання та профілактики. У цілому варто відмітити, що місце людини в кіберпросторі дозволяє говорити про необхідність окремого – антропологічного – напряму дослідження цього цифрового явища. Подвійний статус людини як об'єкта та суб'єкта кіберпростору вказує на великий потенціал наукових досліджень цього напряму в подальшому.

ЛІТЕРАТУРА

1. Звіт про результати роботи Департаменту кіберполіції у 2022 році. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u-roczi-969/ (дата звернення: 17.02.2023).
2. Svilicic N. Cyber Anthropology or Anthropology in Cyberspace. *Collegium antropologicum*. 2012. №36 (1). P. 271–280.
3. Young H., Van Vliet T., Van de Ven J., Jol S., Broekman C. Understanding Human Factors in Cyber Security as a Dynamic System. *International Conference on Human Factors in Cybersecurity (AHFE)*. Proceedings of the International Conference on Human Factors in Cybersecurity (AHFE). Los Angeles, 2018. P. 244–254.
4. Saura J., Reyes-Menendez A., de Matos N., Correia M., Palos-Sanchez P. Consumer behavior in the digital age. *Journal of spatial and organizational dynamics.* 2020. №8 (3). P. 190–196.
5. Що таке даркнет і чи насправді він такий небезпечний. URL: https://suspilne.media/170190-so-take-darknet-i-ci-spravdi-vin-takij-nebezpecnij/ (дата звернення: 17.02.2023).
6. Pinder C., Vermeulen J., Cowan B., Beale R. Digital Behaviour Change Interventions to Break and Form Habits. *ACM transactions on computer-human interaction*. 2018. Vol 25 (3). P. 1–66.

7. Yu T.-K., Lin M.-L., Liao Y.-K. Understanding factors influencing information communication technology adoption behavior: The moderators of information literacy and digital skills. *Computers in Human Behavior,* 2017. Vol. 71. P. 196–208.
8. Achutti C. Learning digital and technology literacy in the era of exponential rate of changes. *9 th International conference on education and new learning technologies (edulearn17).* Proceedings 9 th International conference on education and new learning technologies (edulearn 17). Barcelona, 2017. P. 4778–4785.
9. Rybanska J., Kosiciarova I., Nagyova L. Negative psychological aspects of consumer behaviour in the digital age. *International Scientific Conference on Marketing Identity – Digital Life.* Proceedings of the International Scientific Conference on Marketing Identity – Digital Life. Smolenice, 2015. P. 220–232.
10. Dodel M., Mesch G. Inequality in digital skills and the adoption of online safety behaviors. *Information communication & society.* 2018. Vol. 21 (5). P. 712–728.
11. Ostmeier E., Strobel M. Building skills in the context of digital transformation: How industry digital maturity drives proactive skill development. *Journal of business research.* 2022. № 139. P. 718–730.
12. Pangrazio L., Godhe A.-L., Ledesma L., Gonzalez A. What is digital literacy? A comparative review of publications across three language contexts. *E-learning and digital media*. 2020. Vol. 17 (6). P. 442–459.
13. Anthonysamy L., Sivakumar P. A new digital literacy framework to mitigate misinformation in social media infodemic. *Global knowledge memory and communication*. 2022. URL: https://www.emerald.com/insight/content/doi/10.1108/GKMC-06-2022-0142/full/html (дата звернення: 17.02.2023).
14. Helsper E. J., Smahel D. Excessive internet use by young Europeans: psychological vulnerability and digital literacy? *Information communication & society*. 2020. Vol. 23 (9). P. 1255–273.
15. Taylor-Jackson J., McAlaney J.,Foster J., Bello A., Maurushat A., Dale J. Incorporating Psychology into Cyber Security Education: A Pedagogical Approach. *24 th International Conference on Financial Cryptography and Data Security (FC)*. Proceedings of the 24 th International Conference on Financial Cryptography and Data Security (FC). Kota Kinabalu, 2020. P. 207–217.
16. Населення Землі швидко старіє, не вистачає працівників. Чи готова до цього світова економіка і що чекає на Україну? URL: https://www.epravda.com.ua/publications/2022/01/26/681778/ (дата звернення: 17.02.2023).
17. Li Q., Luximon Y. Older Adults and Digital Technology: A Study of User Perception and Usage Behavior. *International Conference on Physical Ergonomics and Human Factors.* Proceedings of the International Conference on Physical Ergonomics and Human Factors. FL, 2016. P. 155–163.
18. Wang J., Liu C., Cai Z. Digital literacy and subjective happiness of low-income groups: Evidence from rural China. *Frontiers in psychology.* 2022. № 13. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2022.1045187/full (дата звернення: 17.02.2023).
19. Neigel A., Claypoole V., Waldfogle G., Acharya S., Hancock G. Holistic cyber hygie ne education: Accounting for the human factors. *Computers & security*. 2020. Vol. 92. Article 101731.

20. Kranenbarg M. When do they offend together? Comparing co-offending between different types of cyber-offenses and traditional offenses. *Computers in human behavior.* 2022. Vol. 130. URL: https://reader.elsevier.com/reader/sd/pii/S0747563222000085?token=68BE22037551F2B3CC5F521E2EF512A52A56025518A27276B3A8E3F16FC62B7BC72323CC2289CB40657C7608137424C3&originRegion=eu-west-1&originCreation=20230311112032 (дата звернення: 17.02.2023).
21. Kranenbarg M., Van Gelder J., Barends, A., de Vries, R. Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in human behavior*. 2023. № 140. URL: https://reader.elsevier.com/reader/sd/pii/S074756322200396X?token=C9F3890E0ABEF9E274DB15A6994911920CC80FF285240583DA1D8088DCB356C061E56BEA3E5E136F0EA60C99A99221B5&originRegion=eu-west-1&originCreation=20230311100956 (дата звернення: 17.02.2023).
22. Leukfeldt E., Roks R. Cybercrimes on the Streets of the Netherlands? An Exploration of the Intersection of Cybercrimes and Street Crimes. *Deviant behavior.* 2021. Vol. 42 (11). P. 1458–1469.
23. Park J., Cho D., Lee J., Lee B. The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status. *ACM Transactions on Management Information Systems.* 2019. Vol. 10, Issue 4. Article No.: 13. P. 1–23.

REFERENCES

1. Zvit pro rezul′taty roboty Departamentu kiberpolitsiyi u 2022 rotsi. (2022). Retrieved from https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u-roczi-969/ [in Ukrainian].
2. Svilicic, N. (2012). Cyber Anthropology or Anthropology in Cyberspace. *Collegium antropologicum*, *36* (1), 271–280.
3. Young, H., Van Vliet, T., Van de Ven, J., Jol, S., Broekman C. (2018). Understanding Human Factors in Cyber Security as a Dynamic System. *International Conference on Human Factors in Cybersecurity (AHFE):* proceedings of the International Conference on Human Factors in Cybersecurity (AHFE). Los Angeles. *244–254.*
4. Saura, J., Reyes-Menendez, A., de Matos, N., Correia, M., Palos-Sanchez, P. (2020). Consumer behavior in the digital age. *Journal of spatial and organizational dynamics, 8* (3), 190–196.
5. Shcho take darknet i chy naspravdi vin takyy nebezpechnyy. (2021). Retrieved from https://suspilne.media/170190-so-take-darknet-i-ci-spravdi-vin-takij-nebezpecnij/ [in Ukrainian].
6. Pinder, C., Vermeulen, J., Cowan, B., Beale, R. (2018). Digital Behaviour Change Interventions to Break and Form Habits. *ACM transactions on computer-human interaction*, *25* (3), 1–66.
7. Yu, T.-K., Lin, M.-L., Liao, Y.-K. (2017). Understanding factors influencing information communication technology adoption behavior: The moderators of information literacy and digital skills. *Computers in Human Behavior,* 71, 196–208.

8. Achutti, C. (2017). Learning digital and technology literacy in the era of exponential rate of changes. *9 th International conference on education and new learning technologies (edulearn 17):* proceedings 9 th International conference on education and new learning technologies (edulearn17). Barcelona, *4778–4785.*
9. Rybanska, J., Kosiciarova, I., Nagyova, L. (2015). Negative psychological aspects of consumer behaviour in the digital age. *International Scientific Conference on Marketing Identity – Digital Life:* proceedings of the International Scientific Conference on Marketing Identity – Digital Life. Smolenice, *220–232.*
10. Dodel, M., Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information communication & society, 21* (5), 712–728.
11. Ostmeier, E., Strobel, M. (2022). Building skills in the context of digital transformation: How industry digital maturity drives proactive skill development. *Journal of business research,* 139, 718–730.
12. Pangrazio, L., Godhe, A.-L., Ledesma, L., Gonzalez, A. (2020). What is digital literacy? A comparative review of publications across three language contexts. *E-learning and digital media*, *17* (6), 442–459.
13. Anthonysamy, L., Sivakuma,r P. (2022). A new digital literacy framework to mitigate misinformation in social media infodemic. *Global knowledge memory and communication*. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/GKMC-06-2022-0142/full/html.
14. Helsper, E. J., Smahel, D. (2020). Excessive internet use by young Europeans: psychological vulnerability and digital literacy? *Information communication & society*, *23* (9), 1255–273.
15. Taylor-Jackson, J., McAlaney, J.,Foster J., Bello, A., Maurushat, A., Dale, J. (2020). Incorporating Psychology into Cyber Security Education: A Pedagogical Approach. *24 th International Conference on Financial Cryptography and Data Security (FC):* proceedings of the 24 th International Conference on Financial Cryptography and Data Security (FC). Kota Kinabalu, *207–217.*
16. Naselennya Zemli shvydko stariye, ne vystachaye pratsivnykiv. Chy hotova do ts′oho svitova ekonomika i shcho chekaye na Ukrayinu? (2022). Retrieved from https://www.epravda.com.ua/publications/2022/01/26/681778/ [in Ukrainian].
17. Li, Q., Luximon, Y. (2016). Older Adults and Digital Technology: A Study of User Perception and Usage Behavior. *International Conference on Physical Ergonomics and Human Factors*: proceedings of the International Conference on Physical Ergonomics and Human Factors. FL, *155–163.*
18. Wang, J., Liu, C., Cai, Z. (2022). Digital literacy and subjective happiness of low-income groups: Evidence from rural China. *Frontiers in psychology, 13.* Retrieved from https://www.frontiersin.org/articles/10.3389/fpsyg.2022.1045187/full.
19. Neigel, A., Claypoole, V., Waldfogle, G., Acharya, S., Hancock, G. (2020). Holistic c yber hygiene education: Accounting for the human factors. *Computers & security*, 92, 101731.
20. Kranenbarg, M. (2022). When do they offend together? Comparing co-offending between different types of cyber-offenses and traditional offenses. *Computers in human*

behavior, 130. Retrieved from https://reader.elsevier.com/reader/sd/pii/S0747563222000085?token=68BE22037551F2B3CC5F521E2EF512A52A56025518A27276B3A8E3F16FC62B7BC72323CC2289CB40657C7608137424C3&originRegion=eu-west-1&originCreation=20230311112032.

21. Kranenbarg, M., Van Gelder, J., Barends, A., de Vries, R. (2023). Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets. *Computers in human behavior*, *140*. Retrieved from https://reader.elsevier.com/reader/sd/pii/S074756322200396X?token=C9F3890E0ABEF9E274DB15A6994911920CC80FF285240583DA1D8088DCB356C061E56BEA3E5E136F0EA60C99A99221B5&originRegion=eu-west-1&originCreation=20230311100956.
22. 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* (11), 1458–1469.
23. Park, J., Cho, D., Lee, J., Lee, B. (2019). The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status. *ACM Transactions on Management Information Systems, 10*, *4, 13, 1–23.*

Trofymenko Volodymyr Anatoliiovych, Candidate of Legal Sciences, Assistant Professor, Assistant Professor of Philosophy Department, Yaroslav Mudryi National Law University, Kharkiv, Ukraine

THE DIVERSITY OF HUMAN EXISTENCE IN CYBERSPACE AS THE BASIS FOR THE FORMATION OF THE ANTHROPOLOGICAL DIRECTION OF ITS RESEARCH

The publication explores various aspects of human existence in cyberspace. Attention is drawn to the fact that today cyberspace is a necessary condition for normal human activity. It covered both old, traditional spheres of human life, and creates new ones, the need for which is caused by the modern development of society. Attention is also drawn to the problem of cybercrime, as a phenomenon that has also developed in digital reality. In general, the publication proves the necessity of the existence of an anthropological direction of cyberspace research.

Keywords: *cyberspace, law-abiding user, cybercrime, cybercriminal, anthropological direction.*