УДК 340.12
DOI: https://doi.org/10.21564/2663–5704.55.268524

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

ОСОБЛИВОСТІ СПІВІСНУВАННЯ ЛЮДИНИ ТА ДЕРЖАВИ У СФЕРІ КІБЕРБЕЗПЕКИ: ЄДНІСТЬ ЧИ ПРОТИЛЕЖНІСТЬ?

Публікацію присвячено з'ясуванню питання місця держави та громадянина-користувача в кіберпросторі. Розглядаються два протилежних підходи, кожний з яких базується на позиціях первинності держави або людини в питаннях кібербезпеки. Наводяться аргументи прихильників обох підходів і робиться висновок про ефективність їхньої діалектичної взаємодії з метою покращання ефективності кібербезпекових заходів.

Ключові слова*: кіберпростір, кібербезпека, кіберзлочинність, держава, людина, кіберсуверенітет, користувач.*

Постановка проблеми. Кіберпростір усе більше розширюється та поглинає нові сфери суспільного життя. Якщо раніше до кіберпростору входили переважно суто технічні та інші вузькі і специфічні сфери, то сьогодні це розширення торкнулося таких сфер, які мають украй важливе та критичне значення для життєдіяльності суспільства і життя кожної людини. Серед таких сфер можна побачити ті, захист яких держава самостійно вже неспроможна ефективно здійснити, а в деяких випадках і не повинна. Таким чином, постає питання залучення приватного сектору до реалізації цілей кіберзахисту. Кожна людина, за необхідності, має докласти певних зусиль, щоб захистити себе та коло своїх близьких. Але чи здатний на це сучасний «споживач»? Що він повинен знати? На кого повинен перетворитись цей «споживач» кіберпростору, щоб ефективно співпрацювати з державою з метою реалізації ефективних заходів з кіберзахисту? Яким є співвідношення участі держави та людини у сфері кіберзахисту? Відповідь на ці запитання дозволить створити більш спроможну систему кіберзахисту, яка буде ефективно діяти в усіх напрямках кіберпростору.

Аналіз останніх досліджень та публікацій. Звертаючись до аналізу наукових праць іноземних науковців, варто відмітити відсутність єдиної позиції

у визначенні позицій держави та громадянина у сфері кібербезпеки. Узагалі існує два полярних погляди на цю проблему.

Представники першого напрямку прямо заперечують можливості людини у сфері кібербезпеки. Свою позицію про людину у сфері кібербезпеки висловлює британський дослідник Дж. да Силва [1]. Спираючись на опитування та інтерв'ю керівників структур інформаційної безпеки великих приватних підприємств, він робить висновок, що приватний сектор не в змозі повною мірою протистояти кіберзагрозам. Людина без допомоги великого загального механізму не здатна створити повноцінну систему захисту. Згадуючи «Левіафан» та інші твори Томаса Гоббса, дослідник вважає, що таким механізмом повинна бути держава. Лише вона здатна дати ефективні практики з кібербезпеки. Обмеженість ролі людини у безпековій частині кіберпростору висловлюють індійські вчені М. Кхарі, Дж. Шрівастава, С. Гупта та Р. Гупта [2]. Підкреслюючи надважливість кібербезпеки в цілому, вони зазначають, що в комп'ютерній безпеці чи інформаційній безпеці відношення до людини в основному пов'язано з її обов'язком (-ами) у процесі безпеки. У кібербезпеці цей фактор має додатковий вимір, відносячи людей до мішеней для кібератак або навіть стаючи частиною кібератак неусвідомлено. Таким чином, на основі вищенаведеного можна зробити висновок, що лише загальна структура – держава – здатна протистояти кіберзагрозам. Але не всі науковці стоять на подібній позиції.

Другий – протилежний попередньому – напрямок, навпаки, стверджує, що лише за участі людини можливий ефективний кіберзахист. І перше, про що необхідно подбати – поінформованість людини про кібербезпеку. Цієї думки дотримуються сербські вчені А. Ковачевич, Н. Путнік та О. Тошковіч [3]. Теоретичний та емпіричний аналіз, зазначають вони, показує, що поінформованість про кібербезпеку становить особливий інтерес для кібербезпеки. Люди є центральними фігурами в кібербезпеці, і спосіб знизити ризик у кіберпросторі полягає в тому, щоб зробити людей більш обізнаними з безпекою. Досліджуючи різні аспекти поінформованості про кібербезпеку, дослідники відмічають, що вони суперечливі і залежать від середовища. Потрібно проводити глибокий аналіз поінформованості про кібербезпеку та спробувати з'ясувати, як різні фактори, такі як соціально-демографічні фактори, сприйняття кібербезпеки, попередні порушення кібербезпеки, використання ІТ та знання, можуть окремо або разом впливати на кібербезпеку та безпекову поведінку. Як приклад, науковці провели дослідження серед студентів, оскільки вони є найбільш технологічно активною частиною суспільства. Було виявлено, що знання виявилися домінантним фактором поінформованості про кібербезпеку, і хоча учні є цифровими аборигенами, вони не почуваються в безпеці в кіберсередовищі; вони поводяться небезпечно і не мають достат-

ніх знань, щоб захистити себе в кіберпросторі. Тому поінформованість про кібербезпеку повинна бути системною.

Більше уваги приділяти людині пропонує і американський вчений В. Даттон [4]. Експерти з кібербезпеки, зазначає він, визнали необхідність приділяти більше уваги поглядам, переконанням і практикам кінцевих користувачів. На жаль, замість того, щоб стимулювати соціологічні дослідження стосовно користувачів, це усвідомлення частіше призводило до їхнього звинувачення у створенні проблем безпеки та спонсорства, заснованих на страху кампаній, спрямованих на кінцевих користувачів. Автор наполягає на вихованні «думки про безпеку». Замість того, щоб просто визначити безпечні практики, пише дослідник, це допоможе сформувати мислення, яке вбудовує міркування кібербезпеки в повсякденний вибір користувачів. Це, у свою чергу, дозволить опрацювати концепцію «менталітету» безпеки та її соціальне значення. На подібних позиціях стоїть і канадський вчений Дж. Плетсіс [5]. Розглядаючи перехресний спектр проблем, на які кібердомен впливає при прийнятті рішень людиною, він стверджує, що технічних зусиль і рішень недостатньо. Поки особиста обізнаність про кіберсферу не покращиться, зазначає він, ми не наблизимося до вирішення цієї великої проблеми нашого часу.

Таким чином, можна констатувати наявність двох напрямків, які пропонують різні підходи до встановлення провідного суб'єкта у сфері кібербезпеки та кіберзахисту.

Формулювання цілей. Основною метою цієї публікації є спроба дати відповідь на питання: хто ж є первинним суб'єктом у сфері кібербезпеки: держава чи людина?

Виклад основного матеріалу. Питання первинності суб'єкта у сфері кібербезпеки є головним, але не єдиним. На його невирішеність, на думку автора, впливає ще одна проблема, що існує в науці. На неї звернули увагу американські вчені Р. Раміpез та Н. Чукрі [6], і це низький рівень міждисциплінарної співпраці. Незважаючи на багато зусиль, вважають вони, міждисциплінарна співпраця у сфері комп'ютерної безпеки все ще недостатня. Дослідники стверджують, що ці обмеження здебільшого зумовлені відсутністю міждисциплінарної співпраці, необхідної для вирішення проблеми, яка є явно багатогранною. Також науковці визначають потребу в подальшому вдосконаленні стандартної термінології кібербезпеки для сприяння міждисциплінарній співпраці та пропонують вказівки для глобальної спільноти багатьох зацікавлених сторін в інтернеті, які слід враховувати під час розроблення таких стандартів. Окремо американські вчені пропонують створити єдиний жаргон у галузі кібербезпеки для широкого вжитку. Таким чином, як можна побачити, велика кількість якісно різних суб'єктів у кібербезпеці приводить до їхнього певного непорозуміння, і в термінології зокрема. Схожа позиція

і в австралійського вченого С. Парсера [7]. Стандартизація процесів і процедур, пише він, має важливе значення для досягнення ефективного співробітництва в транскордонному та міжгромадському середовищі. Кількість організацій, що розробляють стандарти, і кількість опублікованих стандартів інформаційної безпеки зросла в останні роки, створюючи значні проблеми. Країни використовують стандарти для досягнення різноманітних цілей, у деяких випадках нав'язуючи стандарти, які є конкуруючими та суперечливими або надмірно обмежувальними та несумісними. Інші стандарти віддають перевагу компаніям, які вже домінують у своїй галузі. З цього він робить висновок, що розроблення та використання стандартів є необхідним, своєчасним та вимагає залучення суб'єктів державного та приватного секторів, які працюють у тандемі.

Повертаючися до основного питання, перш за все необхідно зрозуміти аргументи прихильників першого підходу, які орієнтуються на первинність держави в питаннях кібербезпеки. Вони стверджують, що фактично наявна правова термінологія може бути накладена на сферу кібербезпеки. Прикладом може слугувати дослідження китайського дослідника К. Венхонга [8], який на перше місце ставить проблему кіберсуверенітету держави. З розвитком інтернету, пише вчений, він поступово став незамінною інфраструктурою для всіх країн світу. Останнім часом у різних країнах виникають проблеми кібербезпеки, і країни по всьому світу починають створювати власні системи кібербезпеки. Походження всієї діяльності з кібербезпеки походить від «кіберсуверенітету». «Суверенітет» означає найвищу та виключну владу управління справами в межах певної юрисдикції. «Кіберсуверенітет», на думку науковця, є природним продовженням національного суверенітету в кіберпросторі. Щодо побудови кібербезпеки, зазначає автор, є різні думки. Коли значення «свободи інтернету» є важливим, вважається, що слова «кіберсуверенітет» є першим і головним у побудові системи кібербезпеки. А сам кіберсуверенітет є основою всієї відповідної діяльності. Теоретично кіберпростір не має кордонів, але юридично він не є поза межами закону. Зараз кібернетичний суверенітет стикається з багатьма проблемами. Щоб відповідати їм, необхідно вивчити майбутній кіберсуверенітет (безпеку) за участю країн, що розвиваються. Жодна країна, зазначає К. Венхонг, не може отримати абсолютну безпеку. Зазвичай велика держава пропагує свободу, тоді як інші наголошують на правилах гри. Підкреслення ролі кіберсуверенітету в розбудові кібербезпеки не означає закриття кібернетики та відокремлення країни від зовнішнього світу. Міжнародне співтовариство, вважає китайський вчений, має створити новий порядок кіберуправління, заснований на взаємній повазі до кіберсуверенітету та суверенної рівності. Спільне управління має стати майбутнім кіберсуверенітету.

На центральному місці політики та політичних ініціатив, а значить, і держави, у сфері кібербезпеки наполягає німецька вчена Л. Фіхтнер [9]. Коли політика або ініціатива обираються політиками, пише вона, аналіз основного підходу покращує наше розуміння того, як це формує відносини між учасниками, а також сприяє усвідомленню цінностей, які вписано у відповідні технології.

Рушійною силою у сфері кібербезпеки називають політику і швейцарські вчені М. Кавелті та А. Венгер [10]. Такий підхід, на їхню думку, дозволяє спрогнозувати розвиток цієї сфери на майбутнє. Варто також відмітити, що швейцарські вчені також відмічають важливість існування міждисциплінарного підходу до розуміння процесів у сфері кібербезпеки. Важливість політики у сфері кібербезпеки на міжнародному рівні, де суб'єктом є держава, підкреслює індонезійський дослідник Ф. Тімар [11]. За останні десятиліття, відмічає він, інформаційні технології так сильно вплинули на глобальну політику, що експерти з оборони та безпеки стверджують про початок нової ери у війні. Багато іноземних країн почали визначати кіберзагрозу як визначальний фактор у просторі міжнародної безпеки, що також підтверджує важливість кібербезпеки в зовнішній політиці, зазначає вчений.

На централізованому підході у сфері кібербезпеки з державою на чолі наполягають індійські вчені Д. Шрінівас, А. Дас та Н. Кумар [12]. Звертаючи увагу на велику кількість та різноманітність кіберзагроз (віруси, фішинг, троянські коні, хробаки, атаки на відмову в обслуговуванні (DoS), незаконний доступ (наприклад, викрадення інтелектуальної власності чи конфіденційної інформації), атаки на системи керування тощо), вони наполягають на важливості створення різних стандартів у кіберзахисті та побудови архітектурі системи кібербезпеки. Вчені впевнені в необхідності розроблення та прийняття державою національної стратегії кібербезпеки для захисту кіберпростору, а також різних урядових політик щодо захисту кібербезпеки. Мексиканські вчені П. Ороссо та Г. Алехандро [13] взагалі пропонують створити загальну платформу з метою порівняння моделей та стратегій кібербезпеки держав для виділення найбільш вдалих їхніх елементів та побудови комплексної ефективної моделі чи стратегії.

Зважуючи небезпеку кіберзагроз для держави та суспільства, фінські дослідники Л. Лімнел та М. Лехто [14] вважають за необхідне існування стратегічного лідерства у сфері кібербезпеки. Кібербезпека, пишуть вони, стала одним із найбільших пріоритетів для компаній і урядів. Оптимізація та зміцнення стратегічного лідерства є ключовими аспектами забезпечення реалізації бачення кібербезпеки. Стратегічне лідерство в кібербезпеці, на їхню думку, передбачає визначення та встановлення цілей на основі захисту цифрового операційного середовища. Крім того, це передбачає координацію дій

і готовність, а також управління значними збоями. З точки зору ефективного стратегічного керівництва кібербезпекою життєво важливо визначити структури, які можуть відповідати оперативним вимогам середовища. В якості основи для національного розвитку та готовності необхідно мати чітку модель керівництва на рівні стратегії та усвідомлення ситуації, що підтримує управління. Вони також необхідні для управління серйозними, масштабними збоями як у звичайних, так і в надзвичайних умовах кіберопераційного середовища. Проблеми управління кібербезпекою, зазначають науковці, є особливо помітними на рівні стратегічного керівництва. Щоб забезпечити кібербезпеку та досягти поставлених стратегічних цілей, суспільство має мати можливість залучати різних суб'єктів та якомога ефективніше узгоджувати використання різноманітних ресурсів та напрямки дій. Кіберспроможність, роблять висновок дослідники, має розвиватися в усьому суспільстві, що вимагає стратегічної координації, управління та виконавчої спроможності.

Ще одним аргументом на користь держави як первинного суб'єкта вважається можливість створення стратегій з регулювання питань у сфері кібербезпеки. На це звертають увагу і з цим погоджуються дослідники з різних країн [15–17].

Отже, головними є такі аргументи на користь держави:

1. Можливість використовувати вже наявну термінологічну базу з урахуванням особливостей сфери кібербезпеки.

2. Спроба використовувати політичну систему держави для створення єдиної системи цінностей у сфері кібербезпеки.

3. Вступати в міжнародні відносини в питаннях кібербезпеки.

4. Бути стратегічним лідером у досліджуваній сфері.

5. Розробляти і приймати єдині для всієї держави нормативні акти з питань кібербезпеки та кіберзахисту.

Звернімося до прихильників первинності людини у сфері кібербезпеки. Чим вони аргументують свою позицію? Варто відмітити, що людський фактор у кібербезпеці здатний мати і позитивний, і негативний окрас. Про останній пишуть італійські вчені І. Коррадіні та Е. Нарделлі [18]. Дивлячись на поточний сценарій XXI ст., пишуть вони, люди революціонізували своє повсякденне життя та діяльність за допомогою інтернету та цифровізації. Оскільки цифрова ера просувається вперед і стає все більш технологічною, кіберпростір часто стає об'єктом неетичних атак з метою незаконної вигоди. Раптовий сплеск кібератак призвів до створення кіберправил і норм. Хитрість і ефективна атака зловмисників роблять майже неможливим відстеження зловмисника. Спираючися на думку італійських науковців, можна дійти висновку, що наука повинна допомагати не тільки створювати ефективні правила та норми поведінки в кіберпросторі, а й вивчати особу кіберзлочинця, його мотивацію,

можливості, звички та навички з метою ефективного протистояння йому, тому що людина-злочинець може дуже просто прорахувати недоліки та слабкі сторони людини-потерпілого.

На уразливість людини від кібератак звертають увагу і португальські вчені Ф. Бреда, Х. Барбоса та Т. Моріс [19]. Оскільки цифрова ера розвивається, відзначають вони, кібербезпека розширюється, та вразливість програмного забезпечення зменшується, однак люди як окремі особи сьогодні більше вразливі, ніж будь-коли раніше. В даний час одними з найбільш практикуваних і ефективних атак проникнення є соціальні, а не технічні, настільки ефективні, що ці експлойти відіграють вирішальну роль у підтримці більшості кібератак. У цьому аспекті вони звертають увагу на те, що кіберзлочинність використовує соціальну інженерію. Соціальна інженерія – це мистецтво використання людських недоліків для досягнення зловмисної мети. У контексті інформаційної безпеки фахівці-практики порушують захист, щоб отримати доступ до конфіденційних даних, зловживаючи, зокрема, людською схильністю до довіри. Кіберзлочинці, твердять дослідники, спонукають своїх жертв порушувати протокол безпеки, втрачати конфіденційну інформацію, сприятливу для більш цілеспрямованої атаки. На жаль, у багатьох випадках вони маніпулюють потребами користувачів, щоб мимовільно «заразити» та саботувати систему.

Що наука пропонує для протистояння кіберзлочинності? Перш за все констатується складність вирішення цієї проблеми і важливість людини для її вирішення. На це звертають увагу індійські вчені К. Такар, Р. Джоші і А. Добарія [20]. У кіберсфері, яка постійно розвивається та прогресує, потреба в кібербезпеці зростає, звертають увагу вони. Роль кожного індивідуума дуже важлива в забезпеченні кібербезпеки. Вчені розглядають це як додатковий вимір, а також зосереджують увагу на потенційній меті кіберзлочину. Враховуючи це, дискусія про кібербезпеку стає важливою, і вона має важливе значення, оскільки вона зосереджується на етичній сфері суспільства. Вирішити цю проблему нелегко, оскільки вона стосується широкого спектра проблем – від кіберзлочинності до переслідувань в інтернеті та шахрайства в інтернеті.

Розглядаючи людину як суб'єкта кібербезпеки, пропонується в боротьбі з кіберзлочинністю використовувати елементи її поведінки. Стверджується, що в кіберпросторі людина не зможе швидко та повністю створити нові поведінкові системи, тому потрібно використовувати наявні, які вже склалися. Такої думки дотримуються нідерландські вчені Ю. Хізер, Т. ван Влієт, Дж. Ван де Вен, С. Джоль та К. Брокмен [21]. Людський фактор, зазначають вони, значною мірою відсутній у широкому діалозі про кібербезпеку, і його сфера часто обмежена. Вчені пропонують розглядати кібербезпеку як стан системи. Зміна системи викликана поведінкою суб'єкта. Втручання – це способи зміни поведінки суб'єктів для запобігання небажаній поведінці та по-

силення бажаної поведінки. При виборі втручання слід враховувати динамічний характер того, як люди використовують кіберпростір. Люди навряд чи змінять колишню поведінку відразу, зазначають дослідники. Головне – винайти нові способи зберегти стару поведінку в нових обставинах. Тому, на їхню думку, у кіберсфері необхідно розрізняти три основних шляхи поведінки акторів, які впливають на кібербезпеку системи. Такими є рефлекс, звичка та продуманий шлях. Розуміння різниці між ними та правильне використання, констатують вчені, приведе до розроблення успішних втручань у боротьбі з кіберзлочинністю. До біологічних інновацій у сфері безпеки закликають також американські вчені А. Гачиконда, Е. Аль-Шайєр, А. Фарук, М. Райя [22]. Вони зазаначають, що разом із широким використанням інтернет-технології зростають ризики кібератак і порушень безпеки, які можуть мати катастрофічні наслідки для атакованої системи. За час свого існування, пишуть дослідники, люди та інші живі істоти розробили різні природні форми захисту для виживання, і ці біологічні інстинкти та схильності можна штучно відтворити та застосувати до систем кібербезпеки для підвищення стійкості системи перед обличчям атаки. Американські вчені М. Гретен, С. Бандіа, М. Кукейра, Дж. Дікстраб та А. Гінзера [23], звертаючися до людини, визначають предикатори позитивної поведінки в кіберпросторі. На основі соціологічних досліджень серед студентів та викладачів, вони дійшли висновку, що індивідуальні відмінності спричиняють 5–23% відмінностей у намірах поведінки щодо кібербезпеки. Вони встановили, що такі характеристики, як фінансовий ризик, раціональне прийняття рішень, екстраверсія та стать, є важливими унікальними предикторами хорошої поведінки у сфері безпеки. Також, зазначають вчені, вплив індивідуальних відмінностей на наміри поведінки щодо безпеки може залежати і від середовища. Отже, деякі рішення безпеки також повинні залежати від нього.

На значенні поведінки користувачів для покращання рівня кібербезпеки акцентують увагу й австралійські вчені А. Мустафа, А. Белло та А. Марашет [24]. Інформаційна безпека, відзначають вони, протягом тривалого часу була сферою вивчення інформатики, програмної інженерії та інформаційних комунікаційних технологій. Термін «інформаційна безпека» нещодавно був замінений більш загальним терміном «кібербезпека». Дослідники стверджують, що, окрім досліджень інформатики, поведінкові науки, зосереджені на поведінці користувачів, можуть надати ключові методи, які допоможуть підвищити кібербезпеку та пом'якшити вплив соціальної інженерії зловмисників і методів когнітивного злому (тобто поширення неправдивої інформації). На думку вчених, користувачі комп'ютерної системи володіють різними когнітивними можливостями, які визначають їхню здатність протистояти загрозам інформаційної безпеки. А психологічні методи допоможуть користувачам

комп'ютерної системи дотримуватися політики безпеки і таким чином підвищити безпеку мережі та інформації.

Для підвищення ефективності кібербезпекових заходів, вони повинні реалізовуватись спільно усіма громадянами-користувачами. Такий підхід пропонують науковці з Гонконга та Австралії Л. Чанг, Л. Жонг та П. Грабоскі у своїх спільних дослідженнях [25]. Ураховуючи обмежені ресурси та можливості держав підтримувати кібербезпеку, пишуть вони, окремі особи чи колективи доклали різноманітних зусиль щодо спільного виробництва з різним ступенем організації та координації. Запобіжні заходи та принципи, зазначають вони, пропонуються для сприяння конструктивному спільному створенню кібербезпеки між громадянами та користувачами мережі. Але, відмічають вчені, хоча спільне створення безпеки може сприяти соціальному контролю, слід заохочувати лише ті види діяльності, які перебувають у межах закону.

Наступним важливим елементом, який впливає на підвищення рівня кібербезпеки користувачів, є рівень поінформованості та обізнаності користувачів. Зважаючи на проникнення кіберпростору в життя людини, навіть найбільш досвідчені користувачі не завжди мають необхідний рівень кіберсосвіченості. Здавалося б, молодь, яка «сидить» у гаджетах, має бути самою поінформованою, але і тут є певні прогалини. Тому пропонуються різні програми та схеми навчання користувачів залежно від вікової складової, приналежності до тієї чи іншої соціальної групи тощо. Також обізнаність повинна бути не тільки про технічні сторони, а й про законодавчі акти, але рівень її занадто низький. На це звертають увагу малайзійські вчені М. Пітчан та С. Омар [26]. Право, відзначають вони, – це одна з державних політик, створена для блага держави. Закон контролює та регулює суспільство. Однак в ім'я свободи багатьом це не подобається. У контексті розвитку інтернету кіберзакони створено для забезпечення того, щоб користувачі мережі послуговувались кіберпростором належним чином і обережно. Серед кроків для боротьби з кіберзагрозами є створення кіберправоохоронних органів. Однак, констатують вчені, користувачі мережі все ще не знають про існування кіберзакону та збільшення кількості випадків кіберзлочинності. Тож вони провели дослідження, що мало на меті виявити обізнаність інформатора про існування кіберзаконів і проаналізувало виконання закону про загрози кібербезпеці в Малайзії. Для отримання якісних дослідних даних, автори використали якісну методологію, тобто фокус-групи, глибоке інтерв'ю та аналіз документів. Кількість інформантів фокус-групи – 35 користувачів мережі Інтернет, кількість інтерв'юерів – 6 осіб. Серед основних документів, які вони аналізували в цьому дослідженні, є законодавство, річні звіти, повідомлення для ЗМІ та ін. Отримані ними дані свідчать про те, що інформанти фокус-груп не знають

про існування кіберзаконів, оскільки вважають їх найменш важливими, а також інформанти менш чутливі та не практикують їх.

Особливі умови інформування про питання кібербезпеки та кіберзлочинності пропонують створити для покоління Х південноафриканські вчені В. дер Маймер та П. Макдональд [27]. Одне з найбільш вразливих поколінь, зазначають вони, – це покоління Х, яке народилося між 1960 і 1985 рр. Це покоління людей, які змушені використовувати комп'ютер у повсякденному житті, але не виросли в технологічно розвиненому середовищі, як наступне покоління. Своєю метою вони бачать виявлення тих факторів обізнаності про кібербезпеку, яких бракує в знаннях покоління Х, а потім покращити їхні знання. На стать та поточний рівень освіти при інформуванні стосовно кібербезпеки пропонують звернути увагу боснійські дослідники С. Бараковіч та Дж. Хазіч [28]. Вони показують наявність певних зв'язків між статтю та поточним рівнем освіти та знаннями про кібергігієну, обізнаністю та поведінкою, а також взаємодію та зв'язки між цими результатами кібергігієни.

У цілому наукова спільнота вже дійшла висновку, що людина може бути повноправним суб'єктом кібербезпеки. На її користь говорить можливість застосовувати у заходах безпеки звички, навички та можливості, притаманні лише людині, навіть на інстинктивному рівні. Єдине, на що пропонується звернути більшу увагу, – це поінформованість та підвищення рівня освіченості у сфері кібербезпеки користувачів кіберпростору. У цьому аспекті можна звернути увагу на те, що констатується в цілому доволі низький рівень поінформованості людей, незалежно від покоління. Пропонується, залежно від покоління, звертати увагу користувачів на різні аспекти існування кіберпростору та кібербезпеки.

Висновки. Проведений аналіз показує, що прибічники обох проаналізованих напрямків мають сильні аргументи на свою користь. Але все ж їх можна назвати однобічними. Прихильники первинності держави будують свої аргументи на зовнішніх можливостях держави: побудова єдиної державної політики і стратегії кібербезпеки, можливості законодавчого регулювання наявних проблем, міжнародні можливості, створення системи інформування для громадян тощо. Прихильники первинності людини-користувача до свого позитиву включають антропологічні особливості людини, здатність швидше пристосовуватись до нових кіберобставин та сприймати (вивчати) нове. До плюсів навіть відносять і те, що кіберзлочинець – це така ж людина, і інша людина її швидше збагне, знаходячись у схожих обставинах та умовах. Це скоріше допоможе виявити мотив кіберзлочину. Таким чином, на думку автора, для досягнення цілей кібербезпеки доцільно розглядати ці два напрямки в діалектичні взаємодії. Держава створює зовнішні механізми боротьби з кіберзлочинністю, а людина-користувач зможе їх ефективно використати, навіть

у тих сферах, де держава не може ефективно діяти у зв'язку з тим, що не повинна проникати у приватну сферу людини.

ЛІТЕРАТУРА

1. De Silva J. Cyber security and the Leviathan. Computers & security. 2022. Vol. 116. URL: https://www.sciencedirect.com/science/article/pii/S0167404822000724?via%3Dihub (дата звернення 25.09.2022 р.).
2. Khari M., Shrivastava G., Gupta S., Gupta R. Role of Cyber Security in Today's Scenario. *Detecting and mitigating robotic cyber security risks*. Hersey : Igi Global, 2017. P. 177–191.
3. Kovačević A., Putnik N., Tošković O. Factors Related to Cyber Security Behavior. *IEEE Access.* 2020. Vol. 8. P. 125140–125148.
4. Dutton W. Fostering a cyber security mindset. *Internet Policy Review.* 2017. No 6 (1). URL: https://policyreview.info/articles/analysis/fostering-cyber-security-mindset (дата звернення 25.09.2022 р.).
5. Platsis G. The Human Factor: Cyber Security's Greatest Challenge. *International journal of public administration in the digital age*. 2018. No 5 (2). P. 23–39.
6. Ramirez R., Choucri N. Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*. 2016. Vol. 4. P. 2216–2243.
7. Purser S. Standards for Cyber Security. *Best practices in computer network defense: incident detection and response.* 2014. Vol. 35. P. 97–106.
8. Wenhong X. Challenges to cyber sovereignty and response measures. *Mirovaya ekonomika i mezhdunarodnye otnosheniya*. 2020. No 64 (2). P. 89–99.
9. Fichtne L. What kind of cyber security? Theorising cyber security and mapping approaches. *Internet policy review*. 2018. No 7 (2). URL: https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches (дата звернення 30.09.2022 р.).
10. Cavelty M., Wenger A. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*. 2020. No 41. P. 5–32.
11. Timur F. The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. *KnE Social Sciences*. 2017. No 2 (4). P. 244–250.
12. Srinivas J., Das A., Kumar N. Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems-the international journal of escience*. 2019. No 92. P. 178–188.
13. Orozco P., Alejandro G. Chinese and American cyber security models: a comparative. *Oasis-observatorio de analisis de los sistemas internacionales*. 2021. No 34. P. 107–126.
14. Limnell J., Lehto M. The Importance of Strategic Leadership in Cyber Security: Case of Finland. *18th European Conference on Cyber Warfare and Security (ECCWS).* Proceedings of the 18th european conference on cyber warfare and security (ECCWS 2019). Coimbra, 2019. P. 288–296.

15. Tatar U., Calik O., Celik M., Karabacak B. A Comparative Analysis of the National Cyber Security Strategies of Leading Nations. *9th International Conference on Cyber Warfare and Security (ICCWS). Proceedings of the 9th international conference on cyber warfare and security (ICCWS-2014)*. West Lafayette, 2014. P. 211–218.
16. Stitilis D., Pakutinskas P., Malinauskaite I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. Ш. 2017. No 30 (4). P. 1151–1168.
17. Srinivas J., Das A., Kumar N. Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems-the international journal of escience*. 2019. No 92. P. 178–188.
18. Corradini I., Nardelli E. Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. *9th International Conference on Applied Human Factors and Ergonomics (AHFE-2018)* : proceeding of the 9th International Conference on Applied Human Factors and Ergonomics (AHFE-2018). Orlando, 2019. Vol. 782. P. 193–202.
19. Breda F., Barbosa H., Morais T. Social engineering and cyber security. *11th International Conference on Technology, Education and Development (INTED-2017)* : proceedings of the 11th International Conference on Technology, Education and Development (INTED-2017).Valencia, 2017. P. 4204–4211.
20. Thakar H., Joshi R., Dobariya A. An Analysis on Scope of Cyber Security. *6th International Conference on Computing for Sustainable Global Development (INDIACom-2019)* : proceedings of the 6th international conference on computing for sustainable global development (INDIACom-2019). New Delhi, 2019. P. 612–615.
21. 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-*2018)* : proceedings of the International Conference on Human Factors in Cybersecurity (AHFE-2018). Los Angeles, 2018. Vol. 593. P. 244–254.
22. Guthikonda A., Al-Shaer E., Farooq A., Raja M. Bio-Inspired Innovations in Cyber Security. *14th IEEE International Conference on Smart Cities – Improving Quality of Life Using ICT and IoT (HONET-ICT-2017)* : proceedings of the14th IEEE International Conference on Smart Cities – Improving Quality of Life Using ICT and IoT (HONET-ICT-2017). Irbid, 2017. P. 105–109.
23. Gratian V., Bandi S., Cukier M., Dykstra J., Ginther A. Correlating human traits and cyber security behavior intentions. *Computers & Security*. 2018. Vol. 73. P. 345–358.
24. Moustafa A., Bello A., Maurushat A. The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology.* 2021. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011/full (дата звернення 15.10.2022 р.).
25. Chang L., Zhong L., Grabosky P. Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*. 2018. No 12 (1). P. 101–114.
26. Pitchan M., Omar S. Cyber Security Policy: Review on Netizen Awareness and Laws. *Jurnal komunikasi-malaysian journal of communication.* 2019. №35 (1). P. 103–119. URL: https://ejournal.ukm.my/mjc/article/view/30796 (дата звернення 17.10.2022 р.).

27. Van der Vyver C., Mcdonald P. Improving Cyber Security Awareness among Generation X. *32nd Conference of the International-Business-Information-Management-Association (IBIMA-2018)* : proceedings of the 32nd Conference of the International-Business-Information-Management-Association (IBIMA-2018). Seville, 2018. P. 170–181.
28. Barakovic S., Husic J. Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information security journal*. 2022. No article 2088428. URL: https://www.tandfonline.com/doi/abs/10.1080/19393555.2022.2088428?journalCode=uiss20 (дата звернення 17.10.2022 р.).

REFERENCES

1. De Silva, J. (2022). Cyber security and the Leviathan. Computers & security. *Vol. 116.* URL: https://www.sciencedirect.com/science/article/pii/S0167404822000724?via%3Dihub.
2. Khari, M., Shrivastava, G., Gupta S., Gupta, R. (2017). Role of Cyber Security in Today's Scenario. *Detecting and mitigating robotic cyber security risks*. Hersey: Igi Global*, 177–191.*
3. Kovačević, A., Putnik, N., Tošković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Acces, 8, 125140–125148.*
4. Dutton, W. (2017). Fostering a cyber security mindset. *Internet Policy Review, 6 (1).* URL: https://policyreview.info/articles/analysis/fostering-cyber-security-mindset.
5. Platsis, G. (2018). The Human Factor: Cyber Security's Greatest Challenge. International journal of public administration in the digital age, *5 (2)*, *23–39.*
6. Ramirez, R., Choucri, N. (2016). Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. *IEEE Access*, *4, 2216–2243*.
7. Purser, S. (2014). Standards for Cyber Security. *Best practices in computer network defense: incident detection and response, 35, 97–106.*
8. Wenhong, X. (2020). Challenges to cyber sovereignty and response measures. *Mirovaya ekonomika i mezhdunarodnye otnosheniya, 64 (2), 89–99.*
9. Fichtne, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet policy review, 7 (2).* URL: https://policyreview.info/articles/analysis/what-kind-cyber-security-theorising-cyber-security-and-mapping-approaches.
10. Cavelty, M., Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41, 5–32.*
11. Timur, F. (2017). The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. *KnE Social Sciences*, *2 (4), 244–250.*
12. Srinivas, J., Das, A., Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems-the international journal of escience, 92, 178–188.*
13. Orozco, P., Alejandro, G. (2021). Chinese and American cyber security models: a comparative. *Oasis-observatorio de analisis de los sistemas internacionales, 34, 107–126*.

14. Limnell, J., Lehto, M. (2019). The Importance of Strategic Leadership in Cyber Security: Case of Finland. *18th European Conference on Cyber Warfare and Security (ECCWS):* proceedings of the 18th european conference on cyber warfare and security (ECCWS 2019). Coimbra, *288–296.*
15. Tatar, U., Calik, O., Celik, M., Karabacak, B. A (2014). Comparative Analysis of the National Cyber Security Strategies of Leading Nations. *9th International Conference on Cyber Warfare and Security (ICCWS):* proceedings of the 9th international conference on cyber warfare and security (ICCWS-2014). West Lafayette*, 211–218.*
16. Stitilis, D., Pakutinskas, P., Malinauskaite, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security journal. 30 (4), 1151–1168.*
17. Srinivas, J., Das, A., Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems-the international journal of escience, 92, 178–188.*
18. Corradini I., Nardelli E. (2019). Building Organizational Risk Culture in Cyber Security: The Role of Human Factors. *9th International Conference on Applied Human Factors and Ergonomics (AHFE-2018):* proceeding of the 9th International Conference on Applied Human Factors and Ergonomics (AHFE-2018). Orlando, *782, 193–202.*
19. Breda, F., Barbosa, H., Morais, T. (2017). Social engineering and cyber security. *11th International Conference on Technology, Education and Development (INTED-2017):* proceedings of the 11th International Conference on Technology, Education and Development (INTED-2017). Valencia, *4204–4211.*
20. Thakar, H., Joshi, R., Dobariya, A. (2019). An Analysis on Scope of Cyber Security. *6th International Conference on Computing for Sustainable Global Development (INDIACom-2019):* proceedings of the 6th international conference on computing for sustainable global development (INDIACom-2019). New Delhi, *612–615.*
21. 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-*2018)*: proceedings of the International Conference on Human Factors in Cybersecurity (AHFE-2018). Los Angeles, *593, 244–254.*
22. Guthikonda, A., Al-Shaer, E., Farooq, A., Raja, M. (2017). Bio-Inspired Innovations in Cyber Security. *14th IEEE International Conference on Smart Cities – Improving Quality of Life Using ICT and IoT (HONET-ICT-2017):* proceedings of the 14th IEEE International Conference on Smart Cities – Improving Quality of Life Using ICT and IoT (HONET-ICT-2017). Irbid, 105–109.
23. Gratian, V., Bandi S., Cukier ,M., Dykstra, J., Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73, 345–358.*
24. Moustafa, A., Bello, A., Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology.* URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011/full.
25. Chang, L., Zhong, L., Grabosky, P. (2018). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12 (1), 101–114.*

26. Pitchan, M., Omar, S. (2019). Cyber Security Policy: Review on Netizen Awareness and Laws. *Jurnal komunikasi-malaysian journal of communication, 35 (1), 103–119*. URL: https://ejournal.ukm.my/mjc/article/view/30796
27. Van der Vyver, C., Mcdonald, P. (2018). Improving Cyber Security Awareness among Generation X. *32nd Conference of the International-Business-Information-Management-Association (IBIMA-2018):* proceedings of the 32nd Conference of the International-Business-Information-Management-Association (IBIMA-2018). Seville, *170–181.*
28. Barakovic, S., Husic, J. (2022). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information security journal, article 2088428.* URL: https://www.tandfonline.com/doi/abs/10.1080/19393555.2022.2088428?journalCode=uiss20

Трофименко Владимир Анатольевич, кандидат юридических наук, доцент, доцент кафедры философии Национальный юридический университет имени Ярослава Мудрого, г. Харьков, Украина

ОСОБЕННОСТИ СОСУЩЕСТВОВАНИЯ ЧЕЛОВЕКА И ГОСУДАРСТВА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ: ЕДИНСТВО ИЛИ ПРОТИВОРЕЧИЕ?

Публикация посвящена вопросу места государства и гражданина-пользователя в киберпространстве. Рассматриваются два противоположных подхода, каждый из которых основывается на позициях первичности государства или человека в вопросе кибербезопасности. Приводятся аргументы сторонников обоих подходов и делается вывод об эффективности их диалектического взаимодействия с целью повышения эффективности мер кибербезопасности.

Ключевые слова*: киберпространство, кибербезопасность, киберпреступность, государство, человек, киберсуверенитет, пользователь.*

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

CHARACTERISTICS OF INTERACTION BETWEEN MAN AND STATE IN THE FIELD OF CYBER SECURITY: UNITY OR OPPOSITION?

The publication is devoted to the question of the place of the state and citizen-user in cyberspace. Two opposite approaches are considered, each of which is based on the

positions of the primacy of a state or a person in the issue of cybersecurity. The arguments of the supporters of both approaches are given and the conclusion is made about the effectiveness of their dialectical interaction in order to increase the effectiveness of cybersecurity measures.

***Keywords**: cyberspace, cybersecurity, cybercrime, states, person, cybersovereignty, user.*