УДК 343.34+ 343.97
DOI https://doi.org/10.32782/2524-0374/2022-4/82

КІБЕРНАЙМАНСТВО: ФЕНОМЕНОЛОГІЧНИЙ АНАЛІЗ ТА ПРОБЛЕМА ПРАВОВОЇ ОЦІНКИ

CYBERMERCENARISM: PHENOMENOLOGICAL ANALYSIS AND THE ISSUE OF LEGAL ASSESSMENT

Юртаєва К.В., к. ю. н., доцент,
доцент кафедри кримінального права і кримінології факультету № 1
Харківський національний університет внутрішніх справ

У статті здійснено феноменологічний аналіз кібернайманства. На основі аналізу наукової літератури, позицій практичних працівників і міжнародних компаній у сфері забезпечення кібербезпеки та релевантної міжнародно-правової бази визначено два основні підходи до розуміння кібернайманства. Відповідно до першого підходу під кібернайманством розуміють вид хакерської діяльності, який посягає у виконанні на замовлення різних видів протиправних діянь переважно загальнокримінальної спрямованості та який поступово може приймати форму або долучатися до організованих форм злочинності. У статті звертається увага на збільшення кількості недружніх актів у кіберпросторі, спрямованих проти урядових установ та об'єктів критичної інфраструктури, який стає якісно новим проявом аутсорсингу на ринку цифрових послуг. Визначено, що відповідно до другого підходу під кібернайманством розуміють спеціалізовану високопрофесійну діяльність приватних компаній (агентів), які надають широкий спектр кіберпослуг захисного та наступального характеру, які виходять або знаходяться на межі легальності. Користувачами послуг кібернайманців є як приватні компанії, так і уряди тих країн, які прагнуть отримати перевагу в кіберпросторі, але не мають для цього відповідних технічних, інтелектуальних або кадрових ресурсів або які намагаються досягти політичних цілей, застосовуючи ризоморфні методи політичного протистояння. Визначено основні детермінанти та прояви такої діяльності, розглянуто приклади здійснення подібних кібератак та визначено правові підходи щодо оцінки зазначених діянь. У статті здійснено аналіз діяльності приватних військових та охоронних компаній, визначено, що переважна більшість з них надають розвідувальні послуги і кіберпослуги. Розглянуто питання щодо легального регулювання й контролю за аутсорсінгом кіберпослуг приватним військовим та охоронним компаніям та ризиків, пов'язаних з подібною діяльністю. Робиться висновок, що правова оцінка феномену кібернайманства є доволі неоднозначною, а застосування кібернайманців у певних випадках можливо віднести до складового елементу сучасних форм агресії. Ставиться питання про можливість застосування *jus in bello* щодо найбільш небезпечних проявів кібернайманства.

Ключові слова: кібернайманство, приватні військові та охоронні компанії, цифрові послуги, аутсорсінг, кіберзлочинність, правове регулювання, агресія, кібервійна.

The article provides phenomenological analysis of cybermercenarism. Based on the analysis of scientific sources, positions of practitioner and international companies in the sphere of cybersecurity and relevant international legal documents the article outlines two main approaches to understanding cybermercenarism. According to the first approach cybermercenarism is understood as a type of hacking activity, which encompasses various types of general criminal actions in cyberspace performed on demand of a third party that eventually evolve or merge with organized crime. The article draws attention to the growth of the number of unfriendly acts in cyberspace, aimed at governmental institutions and objects of critical infrastructure, which represent a qualitatively new form of outsourcing at the market of cyberservices. The article ascertains that according to the second approach cybermercenarism is understood as a specialized high-performance activity of private companies (agents), which provide a wide range of cyberservices of protective and offensive character that lie on the verge of legality. The clients of cybermercenaries are private companies as well as governments of those countries, which pursue to obtain advantage in cyberspace, but do not possess proper technical, intellectual or human resources or those, who apply rhisomorph methods in political confrontation. The article defines main determinants and manifestations of such activities, studies examples of relevant cyberattacks and define legal approaches of their assessment. The article offers analysis of the activities of private military and security companies, defines that the most of them provide intelligence and cyberservices. The work studies an issue of legal regulation and control over outsourcing of cyberservices provided by private military and security companies and relevant risks posed by such activity. The conclusion is drawn that legal assessment of the phenomenon of cybermercenarism is very controversial and in certain instances cybermercenarism can be assessed as an element of contemporary forms of aggression. The article takes up an issue of application of *jus in bello* to the most dangerous forms of cybermercenarism.

Key words: cybermercenarism, private military and security companies, cyberservices, outsourcing, cybercrime, legal regulation, aggression, cyberwar.

Постановка проблеми. На сьогоднішній день можна із впевненістю констатувати, що в українському суспільстві інформатизація увійшла у життя кожної людини. Розвиток інформаційних технологій змінив парадигму людського спілкування, трудових відносин, режим надання послуг, при чому не лише в приватному секторі, а й в переважній більшості публічних сервісів. Більш того, сучасні реалії визначають, що, якщо людина не володіє хоча б базовими навичками роботи з цифровими пристроями, вона не лише не може претендувати на престижне місце в соціальному устрої, а й фактично втрачає можливість доступу до значної кількості соціальних благ. Початок пандемії вірусу Covid-19 лише прискорив перехід України до цифрового суспільства. І хоча сучасний рівень цифровізації суспільних відносин далеко не завжди знижує корупційні ризики, здатний ефективно забезпечити належний рівень прозорості та економію ресурсів, подальший розвиток людства саме за цифровим напрямом є беззаперечною перспективою найближчих десятиріч.

Водночас дослідницьку увагу привертають супутні негативні і вкрай загрозливі наслідки цифровізації, пов'язані із ризиками порушення основоположних прав людини, забезпечення яких переведено в цифрову сферу, спрощенням доступу до персональних даних, а також перспективою обмеження цифрових прав людини як основи самореалізації у новоствореному цифровому середовищі. Викликають занепокоєння й численні випадки протиправних посягань на цифрові відносини, яким, як промовисто свідчить практика, не здатні ефективно протистояти спеціалізовані агенції. При чому під прямою загрозою опиняються не лише права і свободи окремих громадян, а й об'єкти критичної інфраструктури, система публічного управління та безпека нації загалом. Підвищена вразливість цифрового суспільства до сучасних кіберзагроз обумовлює необхідність оцінки кримінальних ризиків у цій сфері та шляхи їх мінімізації. У цьому контексті хотілося б звернути увагу на розширення практики використання професійних хакерів або навіть цілих спеціалі-

зованих організацій для вчинення масштабних посягань у кіберпросторі. На міжнародному рівні цей феномен отримав назву кібернайманства.

Метою статті є вироблення визначення кібернайманства на основі феноменологічного аналізу цього кримінально протиправного явища та визначення підходів до його правової оцінки.

Аналіз останніх досліджень і публікацій. Питання протидії кіберзлочинності з кожним роком привертають все більшу увагу вітчизняних науковців. Значний внесок у вказаному напряму було здійснено завдяки науковим працям Д. С. Азарова, Ю. А. Бельського, А. А. Васильєва, П. А. Воробея, Д. В. Дубова, О. О. Дудорова, О. О. Загуменного, М. В. Карчевського, О. Г. Колба, В. К. Колпакова, Є. В. Лащука, М. І. Мельника, А. А. Музики, Д. В. Пашнєва, Н. А. Савінової, А. В. Савченка, М. І. Хавронюка, В. Г. Хахановского та інших дослідників. Питанням кримінально-правових і міжнародно-правових аспектів найманства у різні роки були присвячені роботи К. В. Громовенка, В. Ю. Кравченка, С. М. Мохончука, О. В. Наден, Т. І. Нікіфорова, О. О. Скрильник, О. Пунди та інших науковців. У той же час слід відзначити, що в українських джерелах згадки про кібернайманство є поодинокими, у жодному з них не розкрито зміст кібернайманства або його конститутивні ознаки. Натомість у зарубіжній науковій літературі кібернайманству та його впливу на права людини й кібербезпеку присвячено значна кількість тематичних наукових робіт, серед яких слід відзначити дослідження Д. Бурланда (Daniel Burland), Н. ван дер Вааг-Коулінга (Noëlle van der Waag-Cowling), Зоу Жангуі (Zhou Zhanggui), Т. Маурера (Tim Maurer), Б. ван Нікерка (Brett van Niekerk), Т. Рамлукан (Trishana Ramluckan), О. Сведа (Ori Swed), М. Н. Шмітта (Michael N. Schmitt) та інших. Відсутність в українському правому просторі сформованої наукової позиції щодо розуміння кібернайманства обумовлює необхідність детального розгляду цього питання.

Виклад основного матеріалу. Аналіз наукових джерел і нормативного матеріалу, в яких згадується кібернайманство, дозволяє визначити два основні підходи до розуміння цього суспільно небезпечного феномену. У першій групі джерел кібернайманство визначається як новий вид злочинного бізнесу, який полягає у наданні професійних кіберпослуг для вчинення кримінально протиправних посягань у кіберпросторі різного ступеню тяжкості. Так, наприклад, К. М. Євдокімов з посиланням на дослідження Центру глобальних досліджень і аналізу загроз «Лабораторії Касперского» (GReAT) визначає кібернайманство як один з видів кіберзлочинності, який полягає у вчиненні кібератак за наймом [1, с. 42]. Васильєва І. М., не розкриваючи поняття, кібернайманства, ставить його в один ряд з іншими загальнокримінальними правопорушеннями, що перейшли до кіберпростору [1, с. 24]. До таких видів кримінально протиправної діяльності фахівці зазвичай відносять різноманітні види кібершахрайства, кіберкрадіжок і кібервимагання, організацію обігу небезпечних речовин і предметів в мережі Інтернет (наркотичних речовин, фальсифікованих лікарських засобів, зброї, порнографії тощо), організацією інших видів незаконної діяльності з використанням Інтернет-ресурсів (азартних ігор, нелегальної міграції, проституції, відмивання доходів, одержаних злочинним шляхом, тощо).

Воронкова В. Г., Андрюкайтне Р. М., Нікітенко В. О. визначають діяльність кібернайманців як прояв організованої кіберзлочинності, який полягає у здійсненні кібератак, розробці і продажі шпигунського програмного забезпечення і хакерських інструментів на спеціалізованих ринках [3, с. 11]. Подібне розуміння кібернайманства можна зустріти і в статті Олександра Гринчака, начальника Департаменту кіберполіції Національної поліції України в період з 29.10.2019 р. по 05.01.2022 р. Він вказує, що українські ІТ-фахівці нерідко стають частиною міжнародних хакерських угрупувань, та надає їм наступну характеристику: «Звичайний портрет українських кібернайманців – середнього віку, має технічну освіту та спеціалізується на комп'ютерній техніці. До кіберугруповань їх залучають на постійній основі й переважно обіцяють велику грошову винагороду, яка формується в залежності від категорії злочину та завдань».

Узагальнюючи позиції вищевказаних дослідників, можна зробити висновок, що під кібернайманством вони розуміють вид хакерської діяльності, який посягає у виконанні на замовлення різних видів протиправних діянь переважно загальнокримінальної спрямованості та який поступово може приймати форму або долучатися до організованих форм злочинності.

З іншого боку, в зв'язку зі збільшенням кількості недружніх актів у кіберпросторі, спрямованих проти урядових установ та об'єктів критичної інфраструктури, привертає увагу якісно новий прояв аутсорсингу на ринку цифрових послуг. Так, зокрема, у Доповіді Робочої групи з питань використання найманців як засобу порушення прав людини і протидії реалізації прав народів на самовизначення від 15.07.2021 р. (далі – Доповідь) відмічається зростаюча загроза приватизації кібератак, що вчиняються за допомогою нового покоління приватних компаній, яких називають «кібернайманцями». Мова йде про розширення використання урядами країн послуг приватних компаній з надання кіберпослуг захисного та наступального характеру, які здійснюють свою діяльність не лише у власному цифровому домені, а й в іноземних юрисдикціях. Як відмічають ІТ-фахівці, спектр подібних послуг є вельми широким та охоплює різні форми делегованої (англ. *proxy* – проксі) діяльності в кіберпросторі, починаючи із захисту власних мереж та інфраструктури і закінчуючи збором великих даних, кіберрозвідкою та кібершпіонажем, здійсненням кібероперацій з метою послаблення військового потенціалу і можливостей військових сил супротивника або навіть підривом територіальної цілісності інших держав [5].

Т. Маурер визначає декілька основних причин зростання популярності використання кібернайманців урядовими установами різних країн, зокрема: відсутність необхідних можливостей для здійснення діяльності у кіберпросторі або прагнення щодо їх посилення; порівняно менша вартість оплати послуг проксі-компаній або навіть утримання цілих приватних кібербезпекових служб, ніж створення спеціалізованих державних агенцій; відсутність у державному секторі необхідної кількості кваліфікованих кадрів; наявність можливості правдоподібного заперечення участі в кіберопераціях як віддзеркалення бюрократичної культури відповідних державних агенцій [6, p. 38–41]. При чому останній аргумент, на нашу думку, нерідко є найвагомішим, оскільки надає можливість країні-замовниці уникнути відкритого протистояння.

До факторів, що прияють розширенню ринка кібернайманства, можна віднести: відкритий і позатериторіальний характер Інтернету; відсутність прозорості у відносинах між винаймаючими урядовими установами та постачальниками кіберпослуг; більш значна швидкість технологічного прогресу в приватній ІТ-сфері у порівнянні з державним сектором; відносна легкість перепрофілювання ІТ-спеціалістів із захисної до наступальні діяльності у кіберпросторі. Окрім того, як зауважують фахівці, значна кількість цифрових технологій є технологіями подвійного призначення, тобто такими, що можуть бути використані як з метою кіберзахисту, так і для агресивних дій в у кіберпросторі. У зв'язку з цим керівництво однієї з найбільших транснаціональних компаній з виробництва програмного забезпечення Microsoft у відповіді на запит Робочої групи з питань використання найманців закликала компанії-розробників цифрових технологій більш відповідально ставитися до надання доступу до своєї про-

дукції та діяти проактивно у випадку виявлення інцидентів її неправомірного використання [7].

Слід відзначити, що на міжнародному рівні, так само як у науковому й фаховому середовищі відсутня консолідована юридична позиція щодо розуміння кібернайманства та правого режиму функціонування компаній-постачальників потенційно небезпечних кіберпослуг на делегованій основі. Більшість дослідників прирівнюють діяльність аналізованих проксі-установ до діяльності приватних військових та охоронних компаній, використання яких стало розповсюдженим трендом під час здійсненні військових операцій на території зарубіжних країн [див., наприклад, 8]. Як зазначається у Доповіді, ринок наступальних кібертехнологій швидко зростає, і, враховуючи значний попит на вказані послуги, їх пропонують як традиційні військові й охоронні компанії, створюючи в своїй структурі підрозділи з кібербезпеки, так і спеціалізовані кібербезпекові компанії. На думку укладачів Доповіді, коли вказані компанії працюють пліч-о-пліч з урядами країн, їх можна визнати певним продовженням державної влади, і саме в таких випадках їх можливо вважати структурами, що діють як найманці за дорученням іншим осіб. Аналізуючи допустимі правові підходи до оцінки діянь зазначених суб'єктів, у Доповіді пропонується застосовувати міжнародно-правові засоби впливу до держав, які використовують послуги кібернайманців, а до самих проксі-установ та суб'єктів, пов'язаних з кібернайманцями, у певних випадках вважається за можливе застосовувати норми міжнародного гуманітарного права [5]. Щодо останнього пункту деякі країни вже висловили свою відверту незгоду [9].

У відповіді на запит Робочої групи з питань використання найманців керівництво компанії Microsoft зазначило, що кібернайманство є атрибутом діяльності певних країн, які постійно збільшують аутсорсинг своїх повноважень суб'єктам, які діють на їх замовлення. Термін «кібернайманці» керівництво Microsoft пропонує використовувати щодо приватних військових і охоронних компаній, які виготовляють і використовують кіберзброю, або злочинних суб'єктів, що функціонують у приватному секторі. До зазначеного виду діяльності Microsoft включає злам криптографічного захисту цифрових пристроїв, телефонів або мережевої інфраструктури та наступне стеження за об'єктами критичної важливості [7]. Цікаво відзначити, що Microsoft в своїй щорічній Доповіді щодо цифрової безпеки, опублікованій у жовтні 2021 р., не використовуючи терміну «кібернайманство», прямо визначає перелік з тринадцяти найбільших хакерських угрупувань, які керівництво Microsoft безпосередньо асоціює з діяльністю державних установ конкретних країн. Найбільш масштабною кібератакою останніх років, які були здійснені на замовлення урядових установ (англ. *nation state actors*), Microsoft вважає кібератаку SolarWinds [10]. У контексті аналізованої тематики перебіг реалізації цієї кібератаки заслуговує на окрему увагу.

SolarWinds є одним з провідних розробників і постачальників програмного забезпечення на ринок США, а також інших країн. У вересні 2019 р. хакери використали метод ланцюгової атаки (англ. *supply chain attack*), у процесі якої шляхом штатного оновлення програмного забезпечення системи Оріон було інфіковано комп'ютерні системи понад 17000 клієнтів компанії SolarWinds по всьому світу. На відміну від добре відомої в Україні кібератаки, вчиненої за допомогою вірусу-вимагача Petya.A, кібератака на клієнтів компанії SolarWinds мала прихований характер і створювала так званий «бекдор» (англ. *backdoor* – лазівка), до клієнтських комп'ютерних систем, яка активовувалася приблизно через 95 днів з дня зараження. Таким чином хакери протягом майже року мали доступ до комп'ютерних систем клієнтів компанії SolarWinds, до переліку яких потрапили найважливіші урядові агенції США та великі IT-компанії, включаючи й Microsoft. Кібератаку було виявлено і публічно визнано SolarWinds лише в грудні 2020 р., тобто більше, ніж за рік після дати початкового зараження. Уряд США декілька разів змінював офіційну позицію щодо ймовірного суб'єкта хакерської атаки та уряду країни на користь якої він діяв [11]. Керівництво Microsoft вважає винним хакерське угрупування, яке вони називають NOBELIUM [10], проте очевидно, що переконливі докази цього факту та відношення діяльності зловмисників до уряду певної країни наразі відсутні. Зазначений приклад зайвий раз демонструє надзвичайну складність доведення причинно-наслідкового ланцюга та визначення атрибутивного походження кібератак особливо у випадку використання урядами країн послуг кібернайманців. Це у свою чергу призводить до неможливості застосування ефективних правових санкцій у ситуаціях серйозних кібербезпекових порушень, що мають міжнародний характер.

Деякі дослідники вважають неприйнятним використання терміну «кібернайманство» відносно діяльності приватних військових та охоронних компаній. Так, наприклад, науковці з Техаського технічного університету О. Свед і Д. Бурланд вважають, що надання приватних розвідувальних і кіберпослуг є абсолютно легальною підгалуззю індустрії приватних військових та охоронних компаній. На думку дослідників, менеджмент, контроль, виробництво і маніпуляція інформацією завжди були невід'ємною частиною воєнних та захисних функцій і, відповідно, потенційною нішею для ринку приватних військових та охоронних компаній. Сьогодні зазначені компанії заповнюють технологічні прогалини, пропонуючи своїм клієнтам доступ до передових наступальних і комунікативних технологій. «Кібернайманство» дослідники визначають як маргінальний феномен, який стосується лише установ і організацій, що діють поза межами легальності. О. Свед і Д. Бурланд дослідили 1674 легально функціонуючі компанії, що діють на ринку військової та захисної індустрії, і визначили, що 62 % з них надають розвідувальні послуги і кіберпослуги. Дослідники визначають п'ять основних напрямів кіберпослуг, які пропонуються приватними військовими та охоронними компаніями: 1) комунікативна інфраструктура (у вразливих ситуаціях, ворожому середовищі або для забезпечення комунікацій захисної індустрії); 2) IT-сервіси і кіберзахист (забезпечення роботи комунікацій і цифрової інфраструктури); 3) розвідка (гео-розвідувальні послуги, радіолокаційні сигнали, стільникова розвідка тощо); 4) наступальні кіберпослуги (проникнення або подолання кіберзахисту супротивника, що, зокрема, може включати захоплення або порушення роботи Інтернет-сайту супротивника); 5) послуги, пов'язані з великими даними (збір, накопичення та аналіз великих даних з потенційною можливістю їх використання для маніпулювання громадською думкою). Як демонструє дослідження О. Сведа і Д. Бурланда, провідні приватні військові та охоронні компанії, зокрема CACI, Booz Allen Hamilton, Lockheed Martin, Raytheon, BAH, Northrop і Harris, надають не лише захисні, а й наступальні кіберпослуги, і, зокрема, Кіберкомандування США вдається до аутсорсінгу обох указаних видів послуг. Дослідники приходять до висновку про доцільність легального регулювання та контролю за аутсорсінгом кіберпослуг приватним військовим та охоронним компаніям, проте у той же час визнають відсутність практичної можливості вплинути на діяльність урядових установ. Найбільш небезпечною формою діяльності «кібернайманців», на думку О. Сведа і Д. Бурланда, є перетворення інформації на зброю і використання її для порушення прав людини і маніпулювання громадською думкою [12].

Загалом вважаючи позицію вищезазначених дослідників у багатьох аспектах слушною, хотілося б висловити цілком логічний сумнів щодо легальності проведення

кібероперацій приватними військовими та охоронними компаніями в інших юрисдикціях. Вбачається, що побідну активність в кіберпросторі, яка здійснюється урядами країн у випадку навіть не відбиття наявних кіберзагроз, а лише за наявності припущення щодо певних кримінальних ризиків, не можна вважати достатньою підставою для здійснення наступальних дій щодо об'єктів у кіберпросторі, що належать іншій країні. Зазначене можна розглядати як втручання у внутрішні справи країни, за винятком ситуацій загрози миру, порушення миру і актів агресії та відповідно до процедури, визначеної в Главі VII Статуту ООН [13]. Крім того вбачається, що наступальні дії в кіберпросторі, в тому числі з використанням кібернайманців, або суб'єктів, пов'язаних з кібернайманцями, що виражаються у спричиненні шкоди об'єктам критичної інфраструктури країни, її конституційному ладу або територіальній цілісності, можна вважать новітніми формами агресії, вчиненої з використанням сучасних цифрових технологій і здійснюваних у середовищі кіберпростору. Як вже зазначалося вище, це ставить цілком обґрунтоване питання про можливість застосування до таких випадків *jus in bello*.

Узагальнюючи позицію щодо другого підходу, можна констатувати, що сьогодні на міжнародному рівні вимальовується нове сучасне розуміння кібернайманства як спеціалізованої високопрофесійної діяльності приватних компаній (агентів), які надають широкий спектр кіберпослуг захисного та наступального характеру, які виходять або знаходяться на межі легальності. Користувачами послуг кібернайманців є як приватні компанії, так і уряди тих країн, які прагнуть отримати перевагу в кіберпросторі, але не мають для цього відповідних технічних, інтелектуальних або кадрових ресурсів або які намагаються досягти політичних цілей, застосовуючи ризоморфні методи політичного протистояння. На сьогодні правова оцінка феномену кібернайманства є доволі неоднозначною, а застосування кібернайманців нерідко відносять до складового елементу кібервійни.

Висновки та перспективи подальших досліджень. Шляхом проведеного феноменологічного аналізу було визначено два основні підходи до розуміння кібернайманства: перший – пов'язаний з загальнокримінальними посяганнями у кіберпросторі, вчиненими на замовлення, другий – полягає у реалізації спеціалізованої високопрофесійної діяльності щодо здійснення кібератак, інших відверто протиправних діянь або скритих посягань на різні об'єкти у кіберпросторі або поза його межами на користь урядів певних країн. Вбачається, що в сучасних суспільно-політичних умовах другий підхід до розуміння кібернайманства найбільш повно розкриває сутність цього злочинного феномену і, відповідно, створює належну основу для його правової оцінки та протидії кібернайманству на міжнародному рівні. Особливе занепокоєння викликають випадки застосування кібернайманців для вчинення недружніх актів у кіберпросторі як складового елементу сучасних форм агресії. Вбачається, що в умовах збройного протистояння на території України саме останній напрямок потребує ґрунтовного дослідження.

ЛІТЕРАТУРА

1. Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика) : дис. ... д-ра юрид. наук: 12.00.08 – уголовное право и криминология; уголовноисполнительное право. М., 2021. 557 с.
2. Васильева И. Н. Расследование инцидентов информационной безопасности : учебное пособие. СПб., 2019. 113 с.
3. Публічне управління та адміністрування у цифровому суспільстві : монографія / Г. В. Ортіна та ін. Мелітополь : ФОП Однорог Т. В., 2020. 194 с.
4. Гринчак О. Міжнародні хакерські угруповання: як працюють і що робить Кіберполіція. URL: https://biz.nv.ua/ukr/experts/hakeri-ta-kiberpoliciya-chi-vdastsya-zahistiti-ukrajinciv-novini-ukrajini-50165630.html (дата звернення: 01.02.2022).
5. The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyberactivities. Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination. A/76/151. 15 July 2021. URL: https://undocs.org/en/A/76/151 (дата звернення: 01.02.2022).
6. Maurer T. Cyber Mercenaries: The State, Hackers, and Power. Cambridge. 2018. 259 p.
7. Microsoft Response to the United Nations Working Group on the Use of Mercenaries. October 2021. URL: https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx (дата звернення: 01.02.2022).
8. Юртаєва К. В. Кваліфікація найманства: національний та міжнародно-правовий аспекти. *Форум права*. 2018. № 3. С. 141–148.
9. Информация Российской Федерации на запрос председателя-докладчика Рабочей группы Совета ООН по правам человека по вопросу об использовании наемников как средства нарушения прав человека и противодействия осуществлению права народов на самоопределение по тематике «кибер-наемничества» и его воздействия на права человека. URL: https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx (дата звернення: 01.02.2022).
10. Microsoft. Digital Defence Report. October 2021. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738 (дата звернення: 01.02.2022).
11. Oladimeji S., Kerner S. M. SolarWinds hack explained: Everything you need to know. URL: https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know (дата звернення: 01.02.2022).
12. Swed O., Burland D. Cyber Mercenaries: Review of the Cyber and Intelligence PMSC Market. A report for the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination. URL: https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx (дата звернення: 01.02.2022).
13. United Nations Charter. URL: https://www.un.org/en/about-us/un-charter/full-text (дата звернення: 01.02.2022).