

Таким чином, основна мета соціальної протидії корупції цілком кореспондує загальнонаціональним інтересам у формуванні потужного середнього класу – фінансово та політично незалежного прошарку населення. Досягнення цієї мети в нашій державі можливе лише за умови успішної реалізації повноцінного вітчизняного ліберального проекту.

УДК 341.3 + 341.4

Ксенія Володимирівна ЮРТАЄВА,

кандидат юридичних наук, доцент,

доцент кафедри кримінального права і кримінології факультету № 1

Харківського національного університету внутрішніх справ

ORCID: <http://orcid.org/0000-0002-6096-2020>

КІБЕРНАЙМАНСТВО ЯК ЕЛЕМЕНТ СУЧАСНИХ ФОРМ АГРЕСІЇ

В останній час все більшу увагу привертає новий суспільно небезпечний феномен, пов'язаний з данням кримінально протиправних послуг у кіберпросторі. Їх форма і рівень суспільної небезпечності є доволі різноманітними. Нерідко таку кримінально протиправну діяльність називають кібернайманством. Наразі кібернайманство не має одностайної оцінки як серед представників правоохоронної сфери, так і в науковому середовищі.

Аналіз наукових джерел і нормативного матеріалу дозволяє визначити два основні підходи до розуміння кібернайманства. Відповідно до першого під кібернайманством розуміють вид хакерської діяльності, який посягає у виконанні на замовлення різних видів протиправних діянь переважно загальнокримінальної спрямованості та який може мати форму організованої злочинності. Дослідники нерідко ставлять кібернайманство 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 або інших видів незаконної діяльності з використанням Інтернет-ресурсів.

Водночас у зв'язку з порушеною темою привертають увагу новітні тенденції 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. відмічається зростаюча загроза приватизації кібератак, що вчиняються за допомогою нового покоління приватних компаній, яких називають «кібернайманцями». Це стосується розширення використання урядами країн послуг приватних компаній з надання кіберпослуг захисного та наступального характеру. Як відмічають ІТ-фахівці, спектр подібних послуг є вельми широким та охоплює різні форми делегованої 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 [2].

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) [3]. Таким чином приватні військові та охоронні компанії надають не лише захисні, а й наступальні кіберпослуги.

Оскільки наступальні дії в кіберпросторі, в тому числі з використанням кібернайманців, можуть стосуватися втручання в роботу або руйнування об'єктів критичної інфраструктури, конституційного ладу певної країни або порушення її територіальної цілісності, вбачається, що зазначені діяння можуть вважатися новітніми формами агресії, вчиненої з використанням сучасних цифрових технологій та середовища кіберпростору. Таким чином слід резюмувати, що відповідно до другого підходу під кібернайманством розуміють діяльність приватних компаній, які надають широкий спектр кіберпослуг захисного та наступального характеру, які виходять або знаходяться на межі легальності. На сьогодні правова оцінка феномену кібернайманства є доволі неоднозначною, а застосування кібернайманців нерідко відносять до складового елементу кібервійни.

Поняття кібервійни (або кіберагресії чи мережевої війни) дослідниками відносять до якісно нового рівня розуміння цілей та завдань сучасної війни й збройних конфліктів. За своєю сутністю кібервійну можна віднести до віддалених способів ведення військових дій, до яких, зокрема, також зараховують використання посередників, сил спеціальних операцій, приватних військових та охоронних компаній і дронів «для протидії загрозам з відстані» [4]. Як цілком слушно зазначає О. П. Дзьобань, мережева війна має два аспекти: технологічний – використання використовуються інформаційно-телекомунікаційних технологій, і соціальний, який полягає у формуванні «нових груп, кібернайманців, які здійснюють напади – організовані групи хакерів з дуже високим рівнем підготовки, які можуть бути найняті урядами та приватними компаніями для організації і проведення складних ефективних цільових атак на державні структури та установи, приватні компанії з метою втручання в інформаційні бази даних, крадіжки інформації, знищення даних або інфраструктури тощо» [5, с. 37].

Підсумовуючи зазначимо, що, враховуючи сучасний рівень діджиталізації суспільних процесів та залежність сучасної критичної інфраструктури від комунікативних технологій, використання кібернайманців становить пряму загрозу не лише політичному ладу країни, а національній безпеці загалом, враховуючи й фізичну безпеку її населення. У цьому зв'язку вбачається, що за наявності відповідних підстав кібернайманство слід вважати сучасною формою агресії та здійснювати правову оцінку подібних діянь за нормами міжнародного гуманітарного права.

Список бібліографічних посилань:

1. Васильева И. Н. Расследование инцидентов информационной безопасности: учебное пособие. СПб., 2019. 113 с.
2. 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).
3. 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).

4. Riemann M., Rossi N. Outsourcing Death, Sacrifice and Remembrance: The Socio-Political Effects of Remote Warfare. URL: <https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx> (дата звернення: 01.02.2022).

5. Дзьобань О.П. Концептуалізація поняття «мережева війна» у проблемному полі вітчизняного безпекознавства. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). [Електронне видання]. Київ, 2021. С 36-38.

УДК 343.221.51

Андрій Миколайович ЯЩЕНКО,

доктор юридичних наук, професор,

професор кафедри кримінального права і кримінології факультету № 1

Харківського національного університету внутрішніх справ

ORCID: <http://orcid.org/0000-0003-3956-3487>

ДЕЯКІ МІРКУВАННЯ З ПРИВОДУ НОРМАТИВНОЇ ВИЗНАЧЕНОСТІ ЗАГАЛЬНИХ ТА СПЕЦІАЛЬНИХ ПРАВИЛ ЗАСТОСУВАННЯ ЩОДО ЮРИДИЧНИХ ОСІБ ПРИМУСОВИХ ЗАХОДІВ КРИМІНАЛЬНО-ПРАВОВОГО ХАРАКТЕРУ

Порушення кримінально-правових заборон, передбачених Особливою частиною Кримінального кодексу України (далі – КК), зумовлює реалізацію низки різних за ступенем своєї суворості заходів кримінально-правового характеру. Провідне місце серед них посідає покарання. Водночас воно сьогодні вже не розглядається з позиції виключного пріоритетного заходу державного реагування у сфері протидії будь-якому прояву злочинності. Нормативні приписи чинного КК засвідчують, що порушення окремих заборон в Особливій частині КК, може призвести до застосування не лише покарання щодо винних фізичних осіб, але і до реалізації інших заходів кримінально-правового характеру, які можуть бути застосовані як до фізичних, так й до юридичних осіб. Останні заходи представлені заходами кримінально-правового характеру у вигляді штрафу (ст. 96-7 КК), ліквідації та конфіскації майна (ст. 96-9, 96-8 КК).

Застосування цих примусових заходів кримінально-правового характеру щодо юридичних осіб зумовлює певну діяльність суду, що полягає в ухваленні рішення про обрання щодо юридичної особи конкретного заходу кримінально-правового характеру, визначення розміру окремих його видів (зокрема штрафу) та закріплення його в обвинувальному вирoku суду щодо уповноваженої особи юридичної особи, з дотриманням визначених законом правил. Отже, під час такої діяльності суд змушений вирішувати низку питань, у тому числі пов'язаних з індивідуалізацією цих засобів кримінально-правового впливу.

Ознайомлення зі змістом ст. 96-10 КК дає підстави стверджувати, що саме в цих положеннях законодавства знаходить свій вияв принцип індивідуалізації примусових заходів кримінально-правового характеру щодо юридичних осіб процесі їх застосування. Але тут доречно зазначити, що приписи цієї статті стосуються індивідуалізації лише штрафу як різновиду примусових заходів кримінально-правового характеру щодо юридичних осіб і не мають ні якого відношення до інших таких заходів, зокрема ліквідації та конфіскації майна. Вказане дає підстави стверджувати, що поряд з індивідуалізацією примусових заходів кримінально-правового характеру щодо юридичних осіб, а точніше індивідуалізацією штрафу як різновиду таких заходів, доцільно окремо вести мову про виокремлення загальних та спеціальних засад (правил)