DOI: https://doi.org/10.32839/2304-5809/2020-5-81-48
УДК 34.343

Лугіна Н.А., Вартовнік А.М.
Університет державної фіскальної служби України

КІБЕРЗЛОЧИННІСТЬ ЯК ІНСТРУМЕНТ ТРАНСНАЦІОНАЛЬНИХ КОРПОРАЦІЙ

Анотація. У статті досліджується особливості негативного впливу діяльності транснаціональних компаній в Україні. Проаналізовано основні характеристики транснаціональної кіберзлочинності. Здійснено порівняння її з транснаціональними компаніями. Виявлено основні наявні форми боротьби, що здійснюються між транснаціональними корпораціями. Наведено приклади негативного досвіду базування транснаціональних компаній в Україні. Проаналізовано основні можливості залучення хакерів та хакерських угрупувань задля послаблення конкурентів та здійснення недобросовісної конкуренції в Україні. Зроблено прогноз та основні припущення щодо впливу транснаціональних організацій на держави та міжнародні органи та основні можливості і інструменти цього впливу. Виявлено негативні сторони збору даних користувачів та клієнтів. Виявлено основні проблемні моменти у боротьбі держави з кіберзлочинністю.

Ключові слова: глобалізація, кіберзлочинність, недобросовісна конкуренція, транснаціональні компанії.

Lygina Natalia, Vartovnik Anastasiia
University of the State Fiscal Service of Ukraine

CYBER CRIME AS AN INSTRUMENT OF TRANSNATIONAL CORPORATIONS

Summary. In the article features the negative effects of activities of transnational companies in Ukraine. Analyzed the main characteristics of transnational cybercrime. Made a comparison of it with multinational companies. Identified the main existing forms of struggle that are conducted between multinational corporations. description of the positive and negative aspects of the activities and influence of transnational companies. Examples of negative experience-based transnational companies in Ukraine. Analyzes the main opportunities for attracting hackers and hacker groups to weaken the competitors and implementation of unfair competition in Ukraine. The allocation of the main characteristics of cybercrime. The forecast and underlying assumptions on the impact of transnational organizations on state and international bodies and the main opportunities and tools of this impact. Conditioning the factors and conditions that determine the criminal behavior of transnational companies. Analyzed possible aspects of the information society and the negative participation of cybercrim in multinational companies. Definition of cybercrime. Description of the use of hacker attacks by transnational companies as a means of unfair competition, haracterized the main conditions for its prosperity are described. The described mechanism of outsourcing as a tool to fight transnational organizations. Characterized by a DoS attack as an instrument of unfair competition. Hazard description victim behavior victims of cybercriminals and further consequences such as misuse of data by users and clients. Described as influenced by the conditions of globalization on the development of electronic Commerce and increase opportunities to carry out illegal business activity. Analyzed the dependence of the existence of "black market" independence and accountability of the Internet. Resolving the issue of legality of data collection by various services and their further use. The main problem of the state that arises in the fight against cybercrime is described, namely the problem of lawful collection of evidence and non-violation of the basic principles of law and law during this fight.

Keywords: globalization, cybercrime, unfair competition, multinational companies.

Глобалізація світу стала одним із чинників надання злочинності ознаки транснаціональної. Найновіші технології стали доступнішими та поширюються у всіх державах. Використання цих технологій викликало глобальну інформатизацію суспільних відносин в різних сферах. Наразі цифрові технології широко використовуються в електронній комерції, з поняттям якої пов'язані поняття електронних грошей, ринків та розрахунків в безготівковій формі.

Постановка проблеми. Перехід суспільства на новий рівень, тобто становлення його, як інформаційного, має і вкрай негативні сторони, оскільки, жодна країна, міжнародні організації, не зможуть втримати контроль за масштабами здійснення кіберзлочинів, як окремих індивідів так і транснаціональних компаній. Для останніх такі можливості дають їм змогу контролювати всі сфери суспільного життя і серйозно впливати на них, зокрема, на політичну, економічну тощо. Ці корпорації можуть диктувати свої правила і нехтувати основними законами держав і міжнародного права.

Аналіз останніх досліджень. Деякі вчені розглядали різні аспекти даної проблеми, зокрема, як В.В. Кузнецов, П.Д. Біленчук, С.А. Буяджи, М.А. Дем'янчук, В.М. Дрьомін, О.В. Климчук, А.А. Комаров, В.В. Лунєєв, В.В. Марков, В.А. Номоконов, Ю.М. Онищенко, Н.А. Розенфельд, Т.Л. Тропіна, Д.М. Цехан, В.Т. Шатун, С.О. Орлов та інших.

Виділення не вирішених раніше частин загальної проблеми. Також, виникнення та поширення сучасних технологій дає світовій злочинності можливості та інструменти для ведення свого бізнесу та уникнення відповідальності. Кордони зруйнувалися, виявлення навіть місцезнаходження майже не можливе – це ідеальні умови для транснаціональної організацій та підтримки ними кіберзлочинності. Це є однією із глобальних загроз нашого століття поряд із екологічною та іншими загрозами за своєю небезпечністю.

Мета статті. Порівняння ознак транснаціональних корпорацій із ознаками транснаціональної злочинних організацій, виявлення

проблеми прояву злочинних ознак в діяльності транснаціональних компаній. Визначення проблем їх діяльності та впливу на держави та міжнародні органи, зокрема на Україну. Використання транснаціональними компаніями хакерських атак, як засобів недобросовісної конкуренції.

Виклад основного матеріалу. Термін «транснаціональний» означає переміщення через державні кордони потоків інформації, капіталу, ресурсів, тощо. Міжнародні транснаціональні організації діють отримання надприбутків і в цьому вони схожі з транснаціональними злочинними організаціями. Під виглядом різного роду законної господарської діяльності і різних лозунгів за мир, добробут на землі тощо, які транслюються засобами масової інформації та мережею, транснаціональні компанії порушують закони і якщо раніше це було як винятки, то тепер це перетворюється на правила та норми, що є очевидним, тому що уряди слабких країн є корупованим і зачасту діють заодно. Транснаціональні організації прагнуть отримати максимальну свободу та звільнитись від контролю з боку громадських організацій, держав, міжнародних органів, або ж навіть взяти під їх під свій контроль [12].

Супроводжуючись розвитком фінансових систем останні десятиліття відбувається небувалий зріст світової торгівлі, що зумовило збільшення транснаціональних економічних угод. Їх об'єми та складність роблять надзвичайно важким контроль з боку держав та процес їх регулювання. Такі масштаби електронної торгівлі дозволяють приховувати незаконні угоди та виведення коштів в офшори при різних електронних операціях, в тому числі і за допомогою та залученням до цього хакерів та їх угрупувань [9].

Конвенція ООН проти транснаціональної злочинності від 15 листопада 2000 року регламентує поняття та ознаки транснаціональної злочинної організації, а саме:

– планомірність всіх видів діяльності та операцій;
– ієрархічність структур;
– головна мета – максимальний прибуток;
– ділове чуття;
– ефективна система управління;
– тощо.

Отже, можна сказати, що ці ознаки можуть відповідати і ознакам звичайної транснаціональної компанії, за винятком лише однієї – законності в діяльності [1].

Всі галузі економіки пронизані нитками і ТНК, більшість з яких пов'язана з виробничим сектором. Основними позитивними аспектами для держави є діяльність транснаціональних корпорацій, що полягає у:

– підвищенні рівня зайнятості населення, створення нових робочих місць;
– надходження до бюджетів різних рівнів;
– інвестиції у національні компанії і виробників, що відносяться до середнього бізнесу;
– використання та впровадження найновітніших технологій тощо.

Негативних ознак також вистачає, наприклад:

– монополізація влади;
– негативний вплив на розвиток економіки держави як самостійної;
– приховування прибутків;
– обхід національного законодавства;
– подавлення національних виробників, шляхом монопольного встановлення цін на продукцію;
– першочергове задоволення власних інтересів, не зважаючи на потреби держав та суспільства;
– маніпулювання настроями населення або залякування за допомогою використання впливу ЗМІ на свідомість людей [12].

З одного боку, Україна намагається створити певні стратегії і сприятливу базу для ефективного залучення інвестицій та ефективної діяльності транснаціональних компаній. З іншого боку, створюючи такі плани, перш за все, необхідно враховувати національні інтереси українців та України, які, на нашу думку, зазвичай, зовсім не беруться до уваги.

Наприклад, міжнародні корпорації, що виготовляють автомобілі відкривають в Україні цехи, які спеціалізуються на виготовлені автомобільної проводки. Привабливістю для таких компаній наша держава вирізняється наявністю великої кількості дешевої робочої сили, що займаються основним обсягом ручної праці, автоматизація подальших процесів відбувається в більш розвинених країнах. Україна не експортує результати цієї роботи безпосередньо в ЄС, ця продукція може бути придбана лише через дилера відповідного бренду. Умови праці надзвичайно важкі, про це свідчать колишні працівники таких цехів [13].

Отже, можемо бачити, що позитивних моментів від такої уваги транснаціональних компаній до України майже немає, але це не заважало політикам піаритись та всіляко доводити позитивність такого співробітництва [5].

Варто додати, що оскільки, у свій час, Інтернет був проголошений незалежною, не підконтрольною платформою, то можна зрозуміти, що це призвело до появи нових можливостей вчинення злочинів, зокрема фінансування терористичних організацій, чорний ринок наркотиків та зброї, торгівля людьми та дитячою порнографією, розпалювання національної, релігійної, расової ворожнечі, вербування найманців для злочинних війн та конфліктів, пропаганда фашизму та війни, діяльність проституції тощо. Це все, неминуче, призводить до конфліктів та злочинів в реальності, перед якими правоохоронні органи в силу браку кадрів та нормативного забезпечення, просто безсилі [4].

Кіберзлочинність, як визнано багатьма державами та міжнародним співтовариством – це суспільно-небезпечні діяння, що здійснюються за допомогою функціонування всіх систем комунікації, зв'язку, комп'ютерів, мережі Інтернет, будь-яких автоматизованих пристроїв, а також інформаційних технологій. Поняття кіберзлочинності охоплює сукупність злочинів будь-яких видів, вчинених в інформаційному просторі. Найбільш вдалим нам видається таке визначення: «Кіберзлочинність – сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об'єктів, розташованих на ній за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі і комп'ютерні дані» [10].

Отже, можна виділити такі ознаки кіберзлочинності:

– унікальне, особливе середовище – кіберпростір;

– анонімність;

– надзвичайний психологічний вплив на населення;

– надзвичайна латентність злочинів;

– інформація та інформаційні об'єкти можуть бути як об'єктом, предметом так і засобом вчинення злочинів;

– можливість суспільної небезпеки у будь-якій галузі суспільних відносин, або ж навіть загроза такої небезпеки одночасно всім галузям, тобто національній безпеці;

– використання найновітніших технологій у кіберпросторі, що дозволяє з найбільшою вірогідністю уникнути покарання та діяти «на випередження» правоохоронців з будь-якої країни;

– своєрідна спільнота кіберзлочинців, члени якої хоча безпосередньо і не взаємодіють (за виключенням сформованих організованих груп хакерів), але навчають та спілкуються один з одним. Таке спілкування, підтримка, поради можуть за своєю суттю розглядатися як пособництво або підбурювання;

– величезний технічний потенціал. На даний час хоч і існують певні класифікації кіберзлочинів, але все одно, подекуди, скоюються нові, за своїми ознаками, злочини. Деякі кіберзлочинці – це надзвичайно творчі, оригінальні особистості;

– швидкість злочину, порівняно невеликі зусилля та затрати, наприклад придбання нової та потужної техніки;

– легкість у подальшому відмиванні та приховуванні коштів, здобутих нелегальним шляхом.

Якщо додати до цього сучасні умови глобалізації, то до вище наведених ознак кіберзлочинності можна додати і транснаціональний характер. Можна сказати, що вирішена головна проблема злочинців – проблема безпечної комунікації та координації злочинних діянь, їх планування у будь-якій країні, на будь-якій території [6].

Щодо кіберзлочинів транснаціональних компаній в Україні, то можна з впевненістю порівняти їх діяльність на території нашої держави та інших держав. Україна для них – це родючий чорнозем, в силу, перш за все, корупції. Розберемо самі очевидні, наявні випадки кіберзлочинності транснаціональних організацій в нашій державі.

Економічна глобалізація – це тісна взаємозалежна система економік всього світу, ознаками якої є швидке зростання руху через кордони товарів, послуг, технологій та капіталу. Вона також включає в себе і негативні явища, в тому числі і глобальну конкуренцію, що обумовлює боротьбу транснаціональних корпорацій, які розповсюджують свою діяльність, виробляють товари та надають послуги в багатьох країнах світу. Дані компанії використовують різні механізми та інструменти задля ефективної конкуренції на світовому ринку.

Жорсткі стандарти в умовах капіталізму та загострення політичних конфліктів в різних країнах змушують транснаціональні компанії вдаватись до нелегальних, протизаконних дій та таких, що можуть вважатися недобросовісною конкуренцією. Зокрема, механізм аутсорсингу може слугувати таким компаніям для нападу та послаблення, а то і знищення конкурентів за допомогою послуг кіберзлочинців [7].

Найпоширенішою аутсорсингу є IT-індустрія, що цілком логічно, адже наймати програмістів для своєї компанії вимагає дуже великих витрат, тож частину роботи можна делегувати іншим компаніям, в тому числі і за кордоном. Характер даної роботи може бути і нелегальним, але все одно виконується компаніями, адже їх існування залежне від основної компанії. Наприклад, в Індії аутсорсинг бізнес-процесів, в тому числі і в IT проголошений основним видом діяльності, забезпечуючи ріст ВВП та зайнятість, а також зменшення бідності населення [3].

Різного роду дані, що можуть містити в собі ознаки об'єкту для злочинних посягань, тобто різного роду таємні, конфіденційні дані в тому числі і комерційні, банківські, державні таємниці зберігаються на серверах. Злом, втручання, пошкодження, напади на ці сервери представляють собою різного роду інформаційні атаки та несуть небезпеку як для суб'єктів економіки та господарювання, фізичних осіб так і для держави. А в умовах складності, поєднання цих дій з впливом та масштабами цих транснаціональних компаній є загрозою і для світової безпеки [2].

Так, більшість компаній в Україні, зокрема в сфері IT, піддаються DoS-атакам, що значно зменшує їх стійкість та завдає великих збитків. Ці атаки на сервери, зазвичай робляться у вихідні, не робочі часи, що також зменшує оперативність та ефективність їх відбиття. За цими та рядом інших ознак можна стверджувати, що дані атаки є діями конкурентів, які виграють за цей час кошти, витягують з баз даних комерційні відомості про компанію-конкурента, а також дані клієнтів. Потерпілими і даному випадку є і прості фізичні особи, оскільки існують непоодинокі випадки втрати паролів до акаунтів, що можуть, наприклад, бути паролями і від банківських рахунків і т.д. При цьому користувачів і взагалі населення не попереджують, що їх дані вкрадені і можуть бути використані злочинцями, оскільки компанії схильні до приховування від загалу та правоохоронних органів цієї боротьби задля збереження іміджу компанії. Особливо це стосується банків, оскільки така віктимна поведінка та відповідне локальне реагування, без втручання державних органів, має велику суспільну небезпеку для фізичних осіб [11].

На сьогодні ми користуємося безліччю різноманітних браузерів, платіжних систем, додатків, що розроблені транснаціональними корпораціями та які збирають про нас інформацію різного роду. Задля легальності даного збору це прописується в політиках конфіденційності, що розробляються за відповідними міжнародними стандартами. Мета такого збору, зазвичай суто комерційна – задля індивідуалізації пропозицій товарів та послуг. Але, така інформація, також, легко може стати об'єктом неправомірного використання та шпіонажу за звичайними громадянами, порушення їх основоположних прав [9].

Держави намагаються боротися з зовнішніми і внутрішніми загрозами, зокрема тероризмом, екстремізмом та ін. теж нерідко порушуючи закон, недотримуючись основоположних принципів

верховенства права та невтручання в особисте життя. Особливо це небезпечно, якщо дані неправомірно вилучаються і використовуються з офіційних, державних реєстрів, наприклад, щодо місця навчання, лікування, несення служби, роботи, судимості. Таким чином, тотально порушуються основоположні принципи права самою державою, під час боротьби із злочинністю [8].

Висновки і пропозиції. Кіберзлочинність у сучасних умовах інформаційного суспільства та глобальної комп'ютеризації є однією з найбільших загроз світовій безпеці. На нашу думку, основною проблемою нашої держави є те що, інформаційні технології розвиваються і удосконалюються з надзвичайною швидкістю та є дуже складними, поряд з цим нам бракує досвідчених кадрів в правоохоронних органах, а також дуже тривалий, складний бюрократичний шлях наповнення нормами законів, що покликані регулювати дану сферу, а також проблема наступного ефективного їх застосування. Все це призводить до остаточного відставання нашої держави та абсолютної недієвості заходів щодо відвернення загрозам безпеці особистості, суспільству і державі. Єдиним шляхом є нагальна та особлива увага та концентрація на співробітництво у сфері протидії кібертерзлочинності, яке розвивається також і як транснаціональна злочинність. У зв'язку з цим Україна співробітничає з різними країнами, керуючись міжнародними договорами.

Список літератури:

1. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. : ратифікована Законом України від 07.09.2005 р. Відомості Верховної Ради. 2006. № 5-6. Ст. 71.
2. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза. *Криминология: вчера, сегодня, завтра*. 2012. № 1. С. 45–55.
3. United nations conference on trade and development / World Investment Report / The Shift Towards Services. Washington, 2011.
4. Піскорська Г.А., Яковенко Н.Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *Міжнародні відносини. Серія «Політичні науки»*. 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389/3066 (дата звернення: 24.05.2020).
5. Македон В.В. Формат взаємодії транснаціональних корпорацій та реального сектора національної економіки України. *Бюлетень Міжнародного Нобелівського економічного форуму*. 2012. № 1(1). С. 250–258. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/bmnef/2012_1_1/25.pdf (дата звернення: 24.05.2020).
6. Дрьомін В.М. Злочинність як соціальна практика: інституціональна теорія криміналізації суспільства : монографія. Одеса : Юридична література, 2009. 616 с.
7. Конфлікти між державами та організаціями у 2013 році перейдуть у кіберпростір. URL: http://dt.ua/TECHNOLOGIES/konflikti_mizh_derzhavami_ta_organizatsiyami_u_2013_rotsi_ pereydut_u_kiberprostir.html (дата звернення: 24.05.2020).
8. Кібербезпека: світові тенденції та виклики для України. Аналітична доповідь. URL: http://www.niss.gov.ua/content/articles/files/kyber_bezpekaaab17.pdf (дата звернення: 24.05.2020).
9. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом. URL: http://www.crime-research.ru/library/chetilov.htm (дата звернення: 24.05.2020).
10. Буяджи С.А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук: 12.00.01 – Теорія та історія держави і права; історія політичних і правових учень. Класичний приватний університет, Ун-т Короля Данила. Київ, 2018. 203 с.
11. Марков В.В. Хакерські атаки як один із способів протиправного використання кіберпростору: сутність та види. *Вісн. Харк. Ун ту внутр. справ*. 2014. № 2. С. 139–147.
12. Рокоча В.В. Транснаціональні корпорації : навч. посіб. Київ : Таксон, 2001. 304 с.
13. Порошенко у Давосі розповів, що в Україні за рік відкрито 83 нових заводи. *Газета «Главком». Економіка та фінанси*. URL: https://glavcom.ua/economics/finances/poroshenko-u-davosi-rozpoviv-shcho-v-ukrajini-za-rik-vidkrito-83-novih-zavodi-563739.html (дата звернення: 24.05.2020).

References:

1. Konventsiya Rady Yevropy pro kiberzlochynnist': Zakon Ukrainy vid 7 veresnya, 2005 r. [Council of Europe Convention on Cybercrime of 23 November 2001: Law Of Ukraine of 2006]. (in Ukrainian)
2. Nomokonov, V.A., & Tropyna, T.L. (2012). Cybercrime as a new criminal threat. *Krymynolohyia: vchera, sehodnia, zavtra,* no. 1. pp. 45–55.
3. United nations conference on trade and development / World Investment Report / The Shift Towards Services. Washington, 2011.
4. Piskorska, H.A., & Yakovenko, N.L. (2018). Suchasni vyklyky i zahrozy v kiberprostori: formuvannya mekhanizmu mizhnarodnoyi informatsiynoyi bezpeky [Modern challenges and threats in cyberspace: formation of the mechanism of international information security]. *Mizhnarodni vidnosyny. Seriia «Politychni nauky», (*electronic journal), no. 18-19. Available at: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389/3066 (accessed 24.05.2020).
5. Makedon, V.V. (2012). Format vzaiemodii transnatsionalnykh korporatsii ta realnoho sektora natsionalnoi ekonomiky Ukrainy [The format of interaction of transnational corporations and the real sector of the national economy of Ukraine]. *Byuleten' Mizhnarodnoho Nobelivs'koho ekonomichnoho forumu [Bulletin of the International Nobel Economic Forum]* (electronic journal), vol. no. 1(1), pp. 250–258. Available at: http://www.nbuv.gov.ua/portal/Soc_Gum/bmnef/2012_1_1/25.pdf (accessed 24.05.2020).
6. Dromin, V.M. (2009). Zlochynnist yak sotsialna praktyka: instytutsionalna teoriia kryminalizatsii suspilstva: monohrafiia [Crime as a social practice: institutional theory of criminalization of society: monograph]. Odessa: Yurydychna literatura. (in Ukrainian)
7. Conflicts between states and organizations in 2013 move into cyberspace [Electronic resource]. Available at: http://dt.ua/TECHNOLOGIES/konflikti_mizh_derzhavami_ta_organizatsiyami_u_2013_rotsi_pereydut_u_kiberprostir.html (accessed 24.05.2020).
8. Cybersecurity: global trends and challenges for Ukraine. Analytical report: [Electronic resource]. Available at: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf (accessed 24.05.2020).

9. Shchetylov, A. Some problems of struggle with cybercrime and cyberterrorism: [Electronic resource]. Available at: http://www.crime-research.ru/library/chetilov.htm (accessed 24.05.2020).
10. Buiadzhy, S.A. (2018). Pravove rehulyuvannya borot'by iz kiberzlochynnistyu: teoretyko-pravovyy aspekt [Legal regulation of the fight against cybercrime: theoretical and legal aspect]. Teoriia ta istoriia derzhavy i prava; istoriia politychnykh i pravovykh uchen [Theory and history of state and law; history of political and legal doctrines]. Kyiv: Klasychnyi pryvatnyi universytet, Un-t Korolia Danyla. (in Ukrainian)
11. Markov, V.V. (2014). Khakerski ataky yak odyn iz sposobiv protypravnoho vykorystannia kiberprostoru: sutnist ta vydy [Hacker attacks as one of the ways of illegal use of cyberspace: essence and types]. *Visn. Khark. Un-tu vnutr. sprav*, no. 2, pp. 139–147.
12. Rokocha, V.V. (2001). Transnatsionalni korporatsii [Transnational corporations]. Kyiv: Takson. (in Ukrainian)
13. Poroshenko said in Davos that 83 new plants had been opened in Ukraine during the year. Available at: https://glavcom.ua/economics/finances/poroshenko-u-davosi-rozpoviv-shcho-v-ukrajini-za-rik-vidkrito-83-novih-zavodi-563739.html (accessed 24.05.2020).