УДК 343.9:004]:[316.3:351.862.4]
2. Конституційне право. Адміністративне право і процес. Фінансове право. Інформаційне право. Міжнародне право.

Анфіса Нашинець-Наумова,
доктор юридичних наук, доцент,
заступник декана з науково-методичної
та навчальної роботи
Факультету права та міжнародних відносин
Київського університету імені Бориса Грінченка

ДО ПИТАННЯ ЩОДО БОРОТЬБИ З КІБЕРШПІОНАЖЕМ: ВИВЧЕННЯ ТА ОСМИСЛЕННЯ

У статті автор розмірковує про загрози інформаційної безпеки та розглядає одну з найбільш актуальних проблем сучасного інформаційного суспільства – кібершпіонаж. Проводить аналіз підходів щодо протидії загрозам, а також форм і методів, необхідних для вирішення цих завдань. Зокрема, відзначається доцільність створення спеціалізованої служби, здатної відповідати мінливим викликам сучасного інформаційного суспільства.

***Ключові слова**: інформаційна безпека, інформаційне суспільство, комп'ютерна злочинність, кібершпіонаж.*

Нашинец-Наумова А.

К вопросу о борьбе с кибершпионажем: изучение и осмысление

В статье автор размышляет об угрозах информационной безопасности и рассматривает одну из наиболее актуальных проблем современного информационного общества – кибершпионаж. Проводит анализ подходов по противодействию данным угрозам, а также форм и методов, необходимых для решения этих задач. В частности, отмечается целесообразность создания специализированной службы, способной соответствовать меняющимся вызовам современного информационного общества.

***Ключевые слова:** информационная безопасность, информационное общество, компьютерная преступность, кибершпионаж.*

Nashynets-Naumova A.

On the issue of the fight against cyber espionage: the study and understanding

This article, the author reflects on the threats to information security and considers one of the most pressing problems of the modern information society – cyber espionage. Conducts an analysis of approaches to counter these threats, as well as the forms and methods necessary to solve these problems. In particular, the

expediency of creating a specialized service capable of meeting the changing challenges of the modern information society is noted.

Keywords: *information security, information society, computer crime, cyber espionage.*

Постановка проблеми. До початку двадцять першого століття людство не змогло повністю впоратися із загальносвітовими проблемами безпеки – природними та техногенними катастрофами, епідеміями та збройними конфліктами. Новий термін «кібербезпека» позначив ще одну проблему інформаційного суспільства – вразливість світу злочинним атакам і зазіханням, метою яких можуть бути як окремі громадяни, приватні компанії, так і цілі держави. Сьогодні Інтернет-середовище активно освоюють провокатори, злочинці і терористи. Крім того, з'явилися і витончені системи тотального електронного стеження. Це створює загрозу безпеці та суверенітету держав, породжує ланцюгову реакцію недовіри і підбурює гонку інформаційних озброєнь [1, с. 96]. Безумовно, у віртуального світу є не тільки позитивні сторони: сфера міжнародної інформаційної безпеки вимагає найпильнішої уваги світової спільноти. В даному аспекті досить чітко висловлюється К.І. Бєляков, який зазначає, що уникнути конфліктів в інформаційній сфері та їхніх наслідків, часом негативних, що можуть привести до юридичної відповідальності в разі перетворення в правопорушення, практично неможливо, тому й постає потреба вивчення їх сутності, динаміки, досвіду вирішення, прогнозування, запобігання та правової охорони [2, с. 40]. «Кожен з напрямків розвитку інформаційного суспільства, – продовжує професор І.Л. Бачило, – стосується реалізації прав та інтересів людини, відповідальності суб'єктів, які порушують встановлений порядок протиправними діями і бездіяльністю, а також діяльності правоохоронних і судових органів в сфері захисту прав людини і громадянина в межах, що реалізують їх компетенцію та правовий статус» [3, с. 169].

Протягом багатьох років в Україні, як і в багатьох країнах світу на державному рівні не приділялося достатньої уваги питанням правового

регулювання порядку використання інформаційних технологій. В силу цього за протиправні дії фактично була відсутня відповідальність. Ще менше уваги приділялося питанням профілактики правопорушень, запобігання злочинам та їх розслідування.

Аналіз останніх досліджень і публікацій. Питанням щодо вирішення зазначеної проблематики приділялася увага у наукових працях В. М. Бутузова, В. Д. Гавловського, В. М. Горового, В. М. Петрика, М. М. Присяжнюка, В. С. Цимбалюка, О. М. Юрченка та інших. Слід зауважити, що достатньо важливим та конструктивним видається вклад цих та інших вчених у розвиток правової доктрини розвитку інформаційного суспільства, особливо в контексті правового регулювання порядку використання інформаційних технологій. Разом із тим, ураховуючи сучасні тенденції розвитку інформаційного суспільства, необхідність формування його дієвої та ефективної моделі, важливого та ключового значення набувають питання щодо профілактики правопорушень, запобігання злочинам та їх розслідування в зазначеній сфері.

Отже, **метою даного дослідження** є вивчення та осмислення сутності інформаційних правопорушень, які викликані кібершпіонажем, а також комплексний аналіз можливих ефективних шляхів їх нейтралізації.

Виклад основного матеріалу. Якщо говорити про правове регулювання діяльності в українському сегменті глобальної інформаційно-телекомунікаційної мережі «Інтернет», то за багато років слабкого правового режиму виникла середа з дуже низькою правовою культурою і багатьма проявами режиму безвідповідальності. З розвитком інформаційних технологій стали розроблятися інструменти для шпигунства з використанням як спеціалізованих пристроїв, так і програмного забезпечення. На відміну від класичних методів розвідки і шпигунства, нові технології внесли в них суттєві коригування. В даний час іноді неможливо встановити, хто саме розробив те чи інше програмне забезпечення для проведення розвідувальних дій у сфері високих технологій. Розробниками подібного спеціалізованого програмного

забезпечення можуть бути як приватні особи, так і підприємства різної форми власності, з різними джерелами фінансування. Нерідко особи, які розробили програмне забезпечення, не є тими особами, які його використовують для здійснення кібершпіонажу. Це ускладнює, а іноді унеможливлює, ідентифікацію осіб, які здійснюють кібершпіонаж, і як результат – їх залучення до встановленої форми відповідальності. Подібна практика призводить до того, що зацікавлені особи найчастіше самостійно вишукують методи протидії проявам кібершпіонажу в кожному конкретному випадку. Останні включають в себе класичні методи підвищення інформаційної захищеності об'єктів, а також спеціалізовані методи кіберконтррозвідки [4, с. 88].

На відміну від загальної думки, що об'єктами нападу в кібершпіонажі є міжнародні, міждержавні, державні органи, організації та установи, на справді об'єктами нерідко виявляються комерційні компанії та підприємства. Однак, з якихось причин до цих обставин не приділяється належної уваги, особливо якщо це не було пов'язано з розкраданням державної таємниці. Кібершпигуни нерідко мають на меті крадіжку цілого масиву інформації, оскільки такі дії дозволяють отримувати велику кількість персональних даних та/або комерційно значущої інформації. Метою цих дій може бути зміна або видалення певної інформації, що дозволяє усунути компрометуючі відомості, створити позитивну (негативну) історію або, наприклад, створити певні умови для здійснення іншої протиправної дії.

Робота щодо припинення навмисних протиправних дій бачиться неможливою без чіткого розуміння найбільш значущих політичних чинників розвитку комп'ютерної злочинності. Саме в цьому контексті слід відповісти на питання, які процеси демократичного управління та які юридичні норми повинні бути погодженні для прийняття рішення щодо застосування тих чи інших відповідних заходів.

До «найвагоміших політичних чинників, що визначають розвиток комп'ютерної злочинності в Україні, слід віднести:

1) розвиток руху хактивістів як політичної причини комп’ютерної злочинності. Хактивізм (hacktivism, від анг. hack – рубати та activism – активізм [5]) – це суспільний рух, який передбачає боротьбу за права та свободи людини та громадянина за допомогою використання комп’ютерних технологій та інформаційно-телекомунікаційних мереж, включаючи Інтернет;

2) заподіяння шкоди державним інтересам, діяльності механізму державної влади України збройними силами ворожих країн, шляхом використання шкідливих комп'ютерних програм в якості інформаційної зброї;

3) діяльність спецслужб іноземних держав щодо українських органів влади, установ, підприємств для отримання інформації геополітичного, військово-технічного, дипломатичного та іншого стратегічного характеру, тобто «кібершпіонаж» [6, с. 41].

Особливого значення зазначені проблеми набувають з урахуванням фактичної відсутності ефективно функціонуючого, закріпленого на законодавчому рівні правового механізму забезпечення інформаційної безпеки, істотного відставання України від більшості розвинених держав і ряду держав з перехідною економікою за рівнем впровадження інформаційно-комунікаційних технологій [7, с. 4]. Як відзначають фахівці, «існує багато випадків кібершпіонажу, які ніколи не будуть відомі, і все-таки шпигунство існує для того, щоб ніколи не бути виявленим. На щастя, було кілька випадків кібершпіонажу, які були не тільки виявлені, але також заявлені, і в деяких випадках проаналізовані» [8, с. 5]. Однак, «існування і розвиток будь-якої галузі права пов'язано з реальним станом суспільства. Це простежується на історії класичних галузей права: цивільного, кримінального, адміністративного, конституційного. Правова система – це жива сфера позитивного права. Вона, будучи регулятором суспільних відносин у своїй сукупності, сама схильна до впливу динаміки економічних, соціальних, політичних умов життя соціуму» [9, с. 26]. За аксіомою, «інформаційне суспільство може бути таким лише за умови, що воно є суспільством громадянським, соціальним, демократичним і

правовим» [4, с. 90]. В силу своєї природи кібертероризм і кібершпіонаж «кидають виклик сферам дослідження частково через великий масштаб дій і подій, що мають місце» [10, с. 42]. Подібна особливість кібершпіонажу, на наш погляд, робить єдино можливим і доцільним консолідацію зусиль щодо забезпечення національної інформаційної безпеки в одній державній службі. Створення подібної служби дозволить організувати єдині підходи щодо забезпечення режиму безпеки та правопорядку на національному рівні, а в разі наявності належної політичної волі і міжнародної кон'юнктури і на міжнародному рівні. В умовах складної економічної ситуації важливими є консолідація матеріальних ресурсів і кадрового складу. Це дозволить за умови створення належних організаційно-правових механізмів забезпечити необхідний режим національної інформаційної безпеки, ефективно використовувати бюджетні кошти та наявний кадровий потенціал, ефективно протидіяти актам кібершпіонажу, а також іншим загрозам національної інформаційної безпеки. На думку автора, така служба повинна бути наділена широкими повноваженнями відповідно до Кодексу України про адміністративні правопорушення та Кримінально-процесуального кодексу України. Подібний підхід дозволить створити «живу» структуру, здатну відповідати мінливим викликам сучасного інформаційного суспільства. Наділена необхідними кадровими і матеріально-технічними ресурсами для оперативної компетентної реалізації своїх вузькоспеціалізованих повноважень в рамках спеціальної підслідності, така служба позитивно вплине на стан інформаційної захищеності, рівень законності і правопорядку в національному сегменті інформаційно-телекомунікаційної мережі «Інтернет».

Проблема боротьби з кібершпіонажем в значній мірі ускладнюється через глобальний масштаб інформаційних мереж. В даному випадку ефективності вжитих зусиль заважають ті ж проблеми, які притаманні будь-якому комерційному проекту міжнародного рівня. Крім того, виникають і додаткові складнощі, пов'язані з участю структур приватного сектора. Якщо якийсь

вебсайт з шкідливим контентом має розширення, наприклад, .ch (Швейцарія), але належить Росії і розміщений при цьому в Нідерландах, то хто в такому випадку несе за нього відповідальність, і які правові норми повинні при цьому застосовуватися? Але навіть відповідь на це головне питання, тобто хто конкретно стоїть за тією чи іншою IP-адресою, вимагає участі суб'єктів приватного сектора, багато з яких або взагалі не зберігають подібну інформацію, або не хочуть нею ділитися. Ця проблема ускладнюється ще й тим, що в багатьох країнах законодавство з цього питання або зовсім відсутнє, або має дуже обмежений характер [11, с. 17]. У багатьох випадках, навіть якщо керівництво країни рішуче налаштовано на боротьбу з кіберзлочинністю, у держави немає необхідних технічних можливостей для розробки потрібного законодавства або механізмів його реалізації в разі, якщо таке законодавство вже існує. В умовах відсутності необхідної нормативно-правової бази та технічних можливостей для її реалізації, злочинці можуть увійти в Інтернет анонімно, користуючись мережею на території слабо розвиненої держави (наприклад, за допомогою незареєстрованої SIM-карти) і безкарно здійснювати свої злочини із-за кордону. За словами голови консультативної ради Міжнародного багатостороннього партнерства проти кіберзагроз (міжнародна організація, що діє під егідою ООН) Датук Мухаммеда Нур Аміна, такі країни ризикують перетворитися в «недієздатні держави кіберпростору» (cyber failed states). З огляду на витратність заходів щодо забезпечення безпеки інформаційних мереж (за різними оцінками, від 3 до 10% від загальних витрат на утримання мереж), незрозуміло, як скоро такі держави зможуть оволодіти необхідними ресурсами [11, с. 23].

Тому необхідно створити загальну стратегію і загальні правові норми, які б регулювали правила боротьби з кібершпіонажем на міжнародному рівні. Однак зусилля з розвитку міжнародного співробітництва в цій сфері неминуче вимагатимуть вирішення такої серйозної проблеми, як дотримання оптимального балансу між вимогами про збереження анонімності,

конфіденційності та відкритості, з одного боку, і вимогам кібербезпеки, з іншого боку, зокрема, що стосується інформаційних обмінів і вдосконалення можливостей щодо пошуку кіберзлочинців. У контексті боротьби з кіберзагрозами існує і цілий ряд інших проблем демократичного врядування.

По-перше, це проблема розподілу відповідальності. Іншими словами, досить часто буває важко визначити відповідального за ту чи іншу сферу діяльності, яка виникла в результаті злиття різних функцій. Тому необхідно якимось чином об’єднати різні функції, відомства та механізми реагування на загрози, які функціонували окремо один від одного. Особливо це стосується штучного поділу функцій і обов'язків між відомствами, які займаються питаннями національної безпеки та іншими державними структурами. Це також відноситься до сфери законодавчого забезпечення, де існує комплекс не пов'язаних між собою законів, які приймалися для регулювання різних сфер діяльності. Сьогодні як ніколи важливо чітко розподілити функції та обов'язки як всередині державних і приватних суб'єктів боротьби з кіберзагрозами, так і між ними.

По-друге, суб'єкти цієї діяльності нерідко вкрай неохоче діляться отриманою інформацією. Це викликає все більше занепокоєння політиків, особливо з огляду на велику кількість суб'єктів, в розпорядження яких потрапляє інформація, яка потребує невідкладного прийняття рішень. Наведемо лише один приклад. Для того щоб захистити свої цінні ноу-хау, компанії вважають за краще тримати в секреті інформацію про свої заходи безпеки поки не почнуть їх відкрито застосовувати. Це призводить до того, що всі недоліки таких заходів виявляються тільки після того, коли ці заходи вже прийняті.

У багатьох випадках держава отримує можливість дізнатися про факт кібершпіонажу тільки тоді, коли вона сама стає доведеною метою кіберзлочинців. Так, коментуючи недавні хакерські атаки на пошукову систему Google, один з високопоставлених співробітників розвідки визнав, що «якби

представники Google не повідомили нам, що їх компанія і інші фірми зазнали кібератаки, то ми б, напевно, ніколи б про них і не дізналися. Така ситуація просто недопустима» [12, с. 17]. З іншого боку, держава може не знати і про те, що її власна територія відводитися під здійснення кібератак фізичних або юридичних осіб. Для вирішення цієї проблеми пропонуються кілька шляхів. Один з них передбачає обов'язкове інформування державних органів про всі факти кібератак, якщо їх кількість перевищує певний визначений поріг. Однак, з огляду на те, що великий сукупний ефект може бути досягнутий і в результаті величезної кількості відносно нешкідливих атак, поки незрозуміло наскільки запропонована міра виявиться ефективною в кінцевому підсумку. У свою чергу, Великобританія запровадила у себе систему заохочення інформаційних обмінів, при якій ніхто, крім початкового власника, не має права розпоряджатися отриманою інформацією. Це означає, що інформація передається не уряду, а уповноваженим структурам щодо захисту інформаційної безпеки, і саме вони здійснюють аналіз і інтеграцію отриманих даних. При цьому для приватних суб'єктів першорядне значення мають питання довіри і прозорості. З іншого боку, вони, так само, як і уряд, не хочуть стати об'єктами кібератак і тому зацікавлені у співпраці з метою розробки ефективних заходів протидії. Крім того, існує і безліч невирішених питань правового характеру. Зокрема, це стосується визначення повноважень уряду в сфері захисту інформації, розміщення програмних засобів контролю та датчиків автоматичного виявлення і попередження про атаку, не оминаються питання обміну даними з третіми особами та відповідальності приватних суб'єктів. Інша пропозиція передбачає створення на рівні держави потужних структур, в яких зосереджувалася вся інформація від різних суб'єктів (таких, як місцеві центри кібербезпеки) з метою розробки цілісної картини кіберзагроз та стану мережі, а також координації дій при організації заходів оперативного реагування. На урядовому рівні координація дій повинна здійснюватися спільно з правоохоронними органами, органами розвідки і контррозвідки, а також

збройними силами і охоплювати весь спектр питань – від зовнішніх атак, дій користувачів мереж і виявлення слабких місць в системах захисту, до планування заходів щодо виявлення, стримування і ліквідації загроз. Ці структури повинні бути інтегровані в єдину комплексну систему, зокрема, в таких аспектах діяльності, як реагування на інциденти і створення систем наскрізного захисту (тобто саме в тих сферах, якими сьогодні ніхто не займається).

Висновки. З наведеного аналізу можна зробити такі висновки. Для організації ефективної боротьби з кібершпіонажем держава повинна вийти за рамки чисто урядового підходу і прийняти новий підхід, на центральне місце якого має бути поставлено дієве державно-приватне партнерство. Так, наприклад, правоохоронні органи не можуть ефективно боротися з кіберзлочинністю в умовах, коли аналогічні функції і обов'язки не зосереджені у них в руках, а розподілені серед цілого ряду міністерств і відомств, а створення офіційних мереж державно-приватного партнерства в цій сфері ускладнюється, або ці мережі функціонують неефективно. Остання обставина має особливе значення, враховуючи, що обидві сторони цього партнерства не схильні ділитися важливою інформацією, особливо у випадках, коли справа стосується міжнародних і зарубіжних компаній. У такому партнерстві повинні бути задіяні не тільки приватні суб'єкти, які беруть участь в так званих «критичних» сферах діяльності, але і фірми, що спеціалізуються в сфері інформаційної безпеки, а також розробники програмного забезпечення, виробники обладнання, оператори сервісів електронних платежів і електронної пошти, хостінг-провайдери, учасники банківського і фінансового секторів, торговельні Інтернет-фірми і фізичні особи.

Список використаних джерел

1. Бачило И.Л. Исчерпаны ли конституционные основы развития информационного общества и информационного права // Государство и право. 2013. № 12. С. 95–108.

2. Бєляков К.І. Інформаційний конфлікт та юридична відповідальність: сутність і співвідношення // Правова інформатика. 2013. № 2(38). С. 38–46.
3. Бачило И.Л. Обеспечение безопасности интернет-среды: правовые методы и толерантность отношений против киберпреступности // Право цифровой администрации в России и во Франции: сб. мат. российско-франц. междунар. конф. (г. Москва, 27-28 февр. 2013). М.: Конон-плюс, 2014. С. 168–177.
4. Галушкин А.А. Кибершпионаж – угроза современному обществу // Вестник МГОУ. Серия: Юриспруденция. 2015. № 2. С. 87–91.
5. Хактивизм [Електронний ресурс]. – Режим доступу: http://www.tadviser.ru /index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A5%.
6. Евдокимов К.Н. Политические факторы компьютерной преступности в России // Информационное право. 2015. № 1. С. 41–47.
7. Тедеев А.А. Ценностные ориентиры государственной инновационной политики в сфере обеспечения устойчивого развития электронного бизнеса в России // Финансы и кредит. 2012. № 14. С. 2–6.
8. Adkins G. Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism // J. of Strategic Security. 2013. Vol. 6 (№ 3, Suppl.). P. 1–9.
9. Бачило И.Л. О законодательстве в информационной сфере отношений // Информационное общество. 2001. № 4. С. 25–32.
10. Luppicini R. Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research // Global Media J. (Canadian Edition). 2014. Vol. 7 (№ 1). P. 35–50.
11. Бенджамин С. Бакленд Демократическое управление и вызовы кибербезопасности. Женева: Женевский центр демократического контроля над вооруженными силами. 2013. 47 с.
12. Иванов М. Кибератаки – глобальная угроза для бизнеса // Бизнес и безопасность. 2018 (126). 4. С. 14–20.

References

1. Bachilo, I.L. (2013). Ischerpanyi li konstitutsionnyie osnovyi razvitiya informatsionnogo obschestva i informatsionnogo prava [Are the constitutional foundations for the development of the information society and information law exhausted?]. Gosudarstvo i pravo – State and law, 12. 95–108 [in Russian].
2. Bieliakov, K.I. (2013). Informatsiinyi konflikt ta yurydychna vidpovidalnist: sutnist i spivvidnoshennia [Information conflict and legal responsibility: essence and relationship]. Pravova informatyka – Legal informatics, 2(38). 38–46 [in Ukrainian].
3. Bachilo, I.L. (2014). Obespechenie bezopasnosti internet-sredyi: pravovyie metodyi i tolerantnost otnosheniy protiv kiberprestupnosti [Securing the Internet environment: legal practices and tolerance against cybercrime]. Pravo tsifrovoy administratsii v Rossii i vo Frantsii: sb. mat. rossiysko-frants. mezhdunar. konf. (g. Moskva, 27-28 fevr. 2013) – The right of digital administration in Russia and in

France: Sat. mat. Russian-French international conf. (Moscow, February 27-28. 2013). M.: Konon-plyus [in Russian].
4. Galushkin, A.A. (2015). Kibershpionazh – ugroza sovremennomu obschestvu [Cyber espionage – a threat to modern society]. Vestnik MGOU. Seriya: Yurisprudentsiya – Bulletin of MGOU. Series: Jurisprudence, 2. 87–91 [in Russian].
5. Haktivizm [Hacktivism]. Available at: http://www.tadviser.ru /index.php/Statya:H% [in Russian].
6. Evdokimov, K.N. (2015). Politicheskie faktoryi kompyuternoy prestupnosti v Rossii [Political factors of computer crime in Russia]. Informatsionnoe pravo –Information law, 1. 41–47 [in Russian].
7. Tedeev, A.A. (2012). Tsennostnyie orientiryi gosudarstvennoy innovatsionnoy politiki v sfere obespecheniya ustoychivogo razvitiya elektronnogo biznesa v Rossii [Values of state innovation policy in the field of ensuring the sustainable development of e-business in Russia]. Finansyi i kredit – Finance and credit, 14. 2–6 [in Russian].
8. Adkins, G. (2013). Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism. J. of Strategic Security, 6. 1–9 [in England].
9. Bachilo, I.L. (2001). O zakonodatelstve v informatsionnoy sfere otnosheniy [On legislation in the information sphere of relations] // Informatsionnoe obschestvo – Information society, 4. 25–32 [in Russian].
10. Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. Global Media J. (Canadian Edition). 7. 35–50. [in England].
11. Bendzhamin, S. Baklend (2013). Demokraticheskoe upravlenie i vyizovyi kiberbezopasnosti. [Democratic Governance and Challenges to Cybersecurity]. Zheneva: Zhenevskiy tsentr demokraticheskogo kontrolya nad vooruzhennyimi salami [Geneva: Geneva Center for the Democratic Control of Armed Forces]. 47 [in Russian].
12. Ivanov, M. (2018). Kiberataki – globalnaya ugroza dlya biznesa [Cyber-attacks – a global threat to business]. Biznes i bezopasnost – Business and security, 4. 14–20 [in Russian].