**Соловйов Д.О.**
слухач магістратури Одеського державного університету внутрішніх справ.
**Ісмайлов К.Ю.**
кандидат юридичних наук, майор поліції, завідувач кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ

## КІБЕРПРОСТІР ЯК СФЕРА ГЛОБАЛЬНИХ КОНФРОНТАЦІЙ

Більшість потужних держав світу (США, Росія, ЄС, Китай, Індія) перебувають нині на етапі створення і трансформації власних військових кібернетичних підрозділів з огляду на можливості використання мережі інтернет проти їх національних інтересів, а також отримання можливості впливати на інші держави.

За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі ще у 2010 р. [13], вже у 2009–2010 рр. понад 20 країн планували або здійснювали різноманітні інформаційні операції. Скільки країн стурбовано створенням і модернізацією власних ківервійськ станом на 2015–2016 рр. невідомо. Однак, зважаючи на випадки (висвітлені пресою) застосування кіберозброєнь, можна припустити, що кількість таких країн істотно зросла.

Якщо в 2010–2011 рр. розвинуті країни лише наблизилися до розв'язання проблеми формування спецпідрозділів, завданням яких є розвідувальна робота в мережі, захист власних мереж, блокування та «обвал» структур противника з використанням можливостей кіберпростору, то в 2012 році кібервійська почали повноцінно функціонувати, і дедалі більше країн розглядали створення таких спецпідрозділів як об'єктивну необхідність. Станом на кінець 2013 року згідно з офіційними заявами військові кіберпідрозділи з виразно захисними функціями створено у США (U.S. Cyber Command); Великобританії (урядовий Cyber Security Operations Centre); Німеччині (Internet Crime Unit та Federal Office for Information Security); Австралії (The Cyber security operations centre); Індії; Ізраїлі та багатьох інших країнах. Готовність до створення кіберкомандування (інформкомандування) серед сусідів України висловила передусім Російська Федерація. Ще в лютому 2013 року перший заступник голови Комітету Держдуми з оборони В. Заварзін за результатами засідання Комітету за участю глави Генерального штабу В. Герасімова, повідомив, що в Генштабі Збройних сил Росії почав роботу спеціальний підрозділ з кібербезпеки [12]. Також у 2013 році з'явилася інформація про те, що створення кібервійськ починає Білорусь [11]. Активну позицію щодо протидії кіберзагрозам посідають провідні

міжнародні безпекові організації й передусім НАТО (Cooperative Cyber Defence Centre of Excellence) та ОБСЄ.

Таким чином, провідні держави світу дедалі більше уваги приділяють розвитку й захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави. Рівень занепокоєння провідних держав світу щодо сфери кібербезпеки засвідчує бажання врегулювати питання стосовно можливості визнання кібератаки актом війни на міжнародному рівні. Зокрема, вже 30 січня 2010 року під час роботи Всесвітнього економічного форуму в Давосі американський сенатор-республіканець С. Коллінс (Susan Collins) зазначила, що США серйозно розглядають питання щодо проголошення кібератак актами війни. А 12 травня 2010 року помічник заступника міністра оборони США з політичних питань Дж. Міллер (James Miller) заявляв про готовність США завдати воєнного удару у відповідь на кібератаки на американські комп'ютерні мережі. Трактування кібератак як потенційних кібервоєн отримало продовження в 2010 році, коли група експертів під керівництвом М. Олбрайт (Madeleine Korbel Albright) взяла участь у розробці нової Стратегічної концепції НАТО. У 2011 році США оприлюднили Міжнародну стратегію щодо кіберпростору, а у 2013 році з'явилося науково-практичне дослідження групи 20 юристів, які доводили можливість застосування чинного міжнародного законодавства стосовно актів збройної агресії до кібератак.

Усе зазначене спонукає держави світу дедалі активніше позиціюватися з питань внутрішньої та зовнішньої політики в контексті актуальних і потенційних кіберзагроз, розробляти й ухвалювати у цій сфері нормативні документи стратегічного змісту. Станом на кінець 2013 року такі стратегії було напрацьовано більшістю країн ЄС (причому як на національному, так і на загальноєвропейському рівні), США, Канадою, Японією та багатьма іншими країнами. Публічно про розроблення аналогічної стратегії заявила Російська Федерація.

Найпотужнішими та найактивнішими більшість експертів із проблем кібербезпеки вважають військові кіберпідрозділи КНР і США. Дані про потенціал, чисельність і завдання китайських кібервійськ практично відсутні. Однак у доктринальних безпекових документах КНР зростання ролі інформатизації у військовій справі зазначається принаймні від середини 90-х років XX сторіччя. Розширено це питання розглядається в Білій книзі з питань оборони за 2004 рік, де констатується необхідність КНР бути готовою до ведення «локальних війн в умовах інформатизації» [2]. У датованій 2008 роком Білій книзі з питань оборони вказується на бажання досягти до 2020 року значного результату з питань інформатизації армії [6]. Питанню розбудови інформаційного потенціалу збройних сил КНР присвячено також цілий пункт у Білій книзі з питань оборони за 2010 рік. 4 серпня 2010 року очікувалося на оприлюднення даних дослідження компанії Armorize стосовно реального потенціалу китайських і тайванських кібервійськ, однак на вимогу керівництва Тайваню доповідь було виключено із програми конференції Black Hat [10]. Не

містила даних про потенціал кібервійськ Китаю й опублікована усередині серпня 2010 року доповідь Міністерства оборони США про військову міць Китаю, однак у цій доповіді робилося припущення, що значна кількість атак проти мереж, що належать уряду США, могла здійснюватися за підтримки або за безпосередньою участю Народно-визвольної армії Китаю чи уряду Китаю.

Уперше в загальній структурі загроз США кіберзагрозам відведено окреме місце у вже згадуваній Стратегії національної безпеки 2010 року. Цілісним баченням урядом США найближчого майбутнього в розвитку кіберпростору стала Міжнародна стратегія для кіберпростору (International Strategy for Cyberspace). Протягом 2011–2012 рр. було ухвалено ще цілу низку документів практичного значення, спрямованих на мінімізацію кіберзагроз, зокрема щодо протидії роботі бот-мереж і кібершпигунству. 5 січня 2012 року президент США Б . Обама проголосив зміни в оборонній стратегії США, що було зафіксовано в доповіді «Підтримуючи глобальне лідерство Сполучених Штатів: оборонні пріоритети для XXI сторіччя» [9]. У цьому документі на тлі зменшення видатків на оборону було чітко зазначено, що на кібербезпекову сферу видатки не лише не зменшуватимуться, а навпаки, зростатимуть. Зокрема на інші новітні озброєння (літаки «безпілотники» тощо), оскільки нова стратегія вбачає в цьому запоруку «критичної спроможності до майбутніх успіхів» США.

Варто зазначити, що точну оцінку залучення коштів до цієї сфери складно дізнатися не лише через засекречення подібної інформації, а й через особливості бюджетного фінансування у США. Однак один із випадків військового бюджетного планування у США є показовим: у квітні 2013 року Міністерство оборони США подало бюджетний запит на 2014 рік на суму у 4,7 млрд дол. США на поліпшення «операцій у кіберпросторі», в тому числі на спеціальні «атакуючі команди» [14].

Наймасштабніше, на нашу думку, значущість питань кібербезпеки для США загалом та Адміністрації Б. Обами зокрема ілюструє протистояння щодо прийняття комплексних нормативно-правових документів, спрямованих на повноцінне функціонування системи кібербезпеки США, яке розгорнулося протягом 2009–2013 рр. у Конгресі.

У 2012 році найбільш дискусійним і медійно-резонансним був законопроект Cybersecurity Act of 2012 , поданий сенатором Дж. Ліберманом (Joseph Lieberman) у співавторстві з головою комерційного Комітету сенатором С. Коллінс, головою Комітету з розвідки сенатором Д. Рокфеллером і сенатором Д. Файнстайн (Dianne Feinstein). «Законопроект Либермана» лобіював особисто президент Б . Обама. А 16 квітня 2012 року на шпальтах The Washington Post із закликом до пришвидшеного прийняття Законопроекту до конгресменів звернувся старший радник президента США з питань контртероризму та внутрішньої безпеки Д. Бреннан (John O. Brennan) [8].

Головною «родзинкою» Законопроекту стало передбачене ним державно-приватне партнерство з питань забезпечення тих систем, пошкодження чи знищення яких може призвести до масової загибелі, евакуації, проблем у життєзабезпеченні громадян чи катастрофічним наслідкам для економіки й

національної безпеки. Це партнерство мало бути формалізоване у вигляді «кібербезпекового обміну» (cybersecurity exchanges). Зокрема, у Законопроекті зазначалося, що існуватиме принаймні один центр «федерального кібербезпекового обміну», що сприятиме обміну відповідною інформацією про кіберзагрози й небезпеки як між приватними структурами, так і між приватними структурами та державними установами.

Важливим моментом також стало законодавче «убезпечення» кібербезпекового обміну від негативного впливу інформаційної відкритості уряду, передбаченої FOIA (Freedom of Information Act). Метою такого кроку є підсилення впевненості приватних компаній, які обмінюються відповідною безпековою інформацією з державою, що ці дані не стануть надбанням усього суспільства (а отже, і кримінальних елементів), адже це може негативно вплинути не лише на імідж компаній, а й на їхню безпекову ситуацію в цілому.

Суттєво, що документ покладав функцію оцінювання ризиків та уразливостей критично важливих систем інфраструктури й визначення необхідних стандартів безпеки, яким ці системи мають відповідати, на Міністерство внутрішньої безпеки. З огляду на те, що більшість подібних безпекових систем у США (до 90 %) є у приватній власності, це положення Законопроекту із зрозумілих причин викликало й викликає чимало запитань у приватного сектору. Водночас у Законопроекті закладено й певний компроміс: можливість оскаржувати рішення ДВБ власниками інфраструктурних систем, які вважатимуть, що їхні системи неправильно визначено як об’єкти критичної інфраструктури [5,179].

Наразі власники таких систем висловлюють невдоволення і, щонайшвидше, вживатимуть заходів щодо недопущення прийняття Законопроекту (або принаймні пом’якшення відповідного пункту). На їхню думку, уряд має достатньо важелів впливу на забезпечення кібербезпеки приватних організацій, здійснюючи державний контроль над закупівлями. А якщо при цьому необхідно посилити кібербезпеку, то це має здійснюватися передусім через вдосконалену систему реагування на інциденти [1].

Потенційним наслідком упровадження Законопроекту може стати бажання власників систем критичної інфраструктури применшити важливість належних їм безпекових систем, мінімізуючи таким чином державний контроль і відрахування на безпеку, що у стратегічній перспективі знизить рівень захищеності таких систем [4].

За матеріалами відкритої дискусії можна дійти висновку, що з питань необхідності ухвалення кібербезпекового законодавства досягнуто певного консенсусу, проте відразу після презентації зазначеного «пропрезидентського» Законопроекту до документа виникли запитання навіть з боку представників «пропрезидентської» Демократичної партії. Цікавим елементом протистояння («війни») вказаних законопроектів є те, що Законопроект Дж. Маккейна більшою мірою передбачає зростання ролі Агентства національної безпеки та Кіберкомандування США (хоча Дж. Маккейн у своїх численних заявах це спростовує) на противагу ДВБ, представників якого сенатор називає «некомпетентними бюрократами».

Безумовно, США як одна із країн з найбільшим рівнем інтернетпроникнення в усі сфери життя суспільства чи не найбільше опікується проблемами кібербезпеки, зокрема її військовим аспектом. Хоча країни ЄС і виявляють певну активність у цьому напрямі, але на тлі запеклих протистоянь щодо тих чи інших нормативно-правових документів, що матимуть вплив на забезпечення кібербезпеки США, активність ЄС є набагато скромнішою.

**Використані джерела:**


1. Якунин В. И. Механизм разработки геостратегий в сов ременном российском государстве: На примере транспортно-железнодорож ной сферы : автореф. дис. к.політ.н. : 23.00.02 / В. И. Якунин [Елект ронний ресурс]. –Режим доступу: http://www.dissercat.com/content/mekhanizm-razrabotki-geostrategii-v-sovremennom-rossiiskom-gosudarstve-na-primere-transportn

2. Шенгенская интернет-зона: немцы предложили ввести «национальную маршрутизацию» интернета [Електронний ресурс]. – Режим доступу: http://focus.ua/tech/287113/295

3. Шевчук О. В. Зовнішньополітична стратегія США та РФ щодо КНР : автореф. дис. д.політ.н. : 23.00.04 / О. В. Шевчук; Ін-т світ. економіки і міжнар. відносин НАН України. – К., 2009. – 33 с.

4. Хилдрет С. А. Кибертерроризм : материалы Исследовательской службы Конгресса // Кибервойна : доклад Исследовательской службы Конгресса RL30735 / С. А. Хилдрет [Електронний ресурс]. – Режим доступу: http://www.infousa.ru/information/bt-1028.htm.

5. Халецька Л. Еволюція поняття «могутність» у політичній думці Франції кінця XX – початку XHI століття / Л. Халецька // Кіберпростір як новий вимір геополітичного суперництва Дослідження світової політики : зб. наук. праць. – 2011. – Вип. 2. – С. 177–188.

6. Феоктистов В. М. Культурно-цивилизационные ценности концепции национальной безопасности КНР в условиях глобализации : автореф. дис. к.філос.н. : 09.00.13 / В. М. Феоктистов [Електронний ресурс]. – Режим доступу: http://www.dissercat.com/content/kulturno-tsivilizatsionnye-tsennosti-kontseptsii-natsionalnoi-bezopasnosti-knr-v-usloviyakh-

7. Федорук П. Культурно-цивілізаційний контекст геополітичних пріоритетів України / П. Федорук // Нова парадигма. – 2012. – Вип. 107. – С. 181–191.

8. Управління боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/main/uk/pu-b lish/article/544754293

9. Україна у світі, що змінюється : стратегія національної безпеки України // Офіційний вісник України. – 2007. – № 11. – С. 7.

10. На Black Hat запретили рассказывать о возможностях китайской киберармии [Електронний ресурс]. – Режим доступу: http:// www.securitylab.ru/news/396433.php

11. Минобороны Беларуси создает элитное подразделение к ибервойск [Електронний ресурс]. – Режим доступу: http://www.bezpeka. com/ru/news/2013/09/18/belarus-cyberforce.html

12. Кибервойска РФ рождаются в Генштабе [Електронний ресурс]. – Режим доступу: http://file–rf.ru/news/12209

13. В мире два десятка стран занимаются кибероружием – McAfee [Електронний ресурс]. – Режим доступу: http://www.cybersecurity.ru/armament/86546.html

14. Война в киберпространстве – вопрос времени? [Електронний ресурс]. – Режим доступу: http://www.golos-ameriki.ru/content/cyber-wars-in-future/1681528.html

**Тишлек Д.П.**
здобувач Донецького юридичного інституту МВС України

## КОМП'ЮТЕРНА РОЗВІДКА ЯК ОДИН ІЗ ПРІОРИТЕТНИХ НАПРЯМІВ ПРОТИДІЇ ЕКОНОМІЧНИМ ЗЛОЧИНАМ

На сьогодні злочинці все частіше використовують інформаційно-телекомунікаційні технології під час вчинення злочинів, і в першу чергу це стосується економічних злочинів. При цьому ними застосовуються сучасні досягнення суспільства, зокрема стільникові телефони та мережа Інтернет.

Інтернет, як специфічне соціальне середовище, має низку особливостей, які значно ускладнюють контроль з боку правоохоронних структур. До таких особливостей можна віднести відсутність географічних обмежень, відсутність системи автентифікації користувачів, що надає змогу в більшості випадків діяти анонімно. Такі особливості, все частіше спокушають зловмисників до опанування можливостей мережі Інтернет з метою вчинення злочинів, у тому числі й економічних злочинів.

Організація дієвої протидії злочинній діяльності в економічній сфері з використанням інформаційно-телекомунікаційних технологій є недостатньо ефективною. Цьому сприяють наступні фактори:

1) прогалини у законодавчому забезпеченні правоохоронних органів з протидії використання Інтернет-мережі у протиправних цілях;

2) недостатня організація міжвідомчої взаємодії зі встановлення конкретних користувачів;

3) недостатня кількість відповідних методик протидіїокремимвидам економічних злочинів;

4) наявністьнедостатньої кількості відповідних фахівців та високотехнологічного програмно-пошукового забезпечення в мережі;

5) висока латентність економічних злочинів.

Одним із пріоритетних напрямів пошуку та фіксації інформації з використанням інформаційно-телекомунікаційних технологій є комп'ютерна розвідка, сутність якої полягає у пошуку та отриманні оперативної інформації з комп'ютерних систем та мереж. Необхідність проведення цього заходу обумовлена особливостями сучасної злочинності. Комп'ютерні мережі, насамперед Інтернет, все більш активно використовується зловмисниками не