проблеми методології

УДК 002.4

Підходи до формування тезаурусу у сфері кібербезпеки

Дмитро Дубов,
кандидат політичних наук,
завідуючий відділом
досліджень інформаційного суспільства
та інформаційних стратегій
Національного інституту стратегічних досліджень

Стаття присвячена проблемі впорядкування кібербезпекової термінології (кіберпростір, кібербезпека, кібератака, кібертероризм) та огляду підходів, що існують у цій сфері в практиці вітчизняних і західних досліджень.

Ключові слова: *кіберпростір, кібербезпека, кібератака, кібертероризм.*

The article is dedicated to the problem of cybersecurity terminology systematizing (cyberspace, cybersecurity, cyberattack, cyberterrorism) and viewing the approaches which exist in this sphere in native and foreign researches.

Keywords: *cyberspace, cybersecurity, cyberattack, cyberterrorism.*

Актуальність дослідження

Динамічні процеси інформатизації суспільства, що докорінним чином змінюють всі сфери життєдіяльності суспільства (міжособистісного спілкування, державного управління, політичної комунікації, економіки, енергетики, охорони здоров'я тощо), надають їм нових імпульсів розвитку та можливості реалізації в нових умовах. Водночас ці ж процеси є причиною появи і принципово нових викликів для безпекової сфери (як суспільної безпеки, так і суто військової), що обумовлюється глибинним проникненням інформаційних технологій у всі елементи критично важливої для держави інфраструктури, від життєдіяльності якої залежить саме існування суспільства. І якщо на початкових етапах розвитку кіберпростору (переважно - мережі Інтернет) основні проблеми виникали

внаслідок діяльності хакерів-одинаків, то вже на зламі XX і XXI століть можливостями використання інформаційних технологій у зборі інформації та ведення боротьби з супротивником зацікавились і силові відомства (в першу чергу – розвідувальні органи та міністерства оборони) провідних держав світу. За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі 2010 року [18], уже більше двадцяти країн планували здійснювати або реально здійснювали різнопланові інформаційні операції. Формуються спецпідрозділи, які мають на меті ведення розвідувальної роботи в мережах, захист власних мереж, блокування і „обвал" структур супротивника.

Провідні держави світу (США, Велика Британія, Франція, Німеччина) ставляться до таких загроз цілком серйозно, про що свідчать ухвалені ними нормативні документи, що регулюють політику із захисту власного кіберпростору та основних напрямів протидії діяльності ворожих груп.

Незважаючи на те, що такі поняття, як „кіберпростір", „кібервійна", „кібератака" та „кібертероризм", широко використовуються як у науковій, так і в публіцистичній літературі, все ще існує значна невизначеність щодо змістового наповнення цих термінів, що, у свою чергу, значно ускладнює наукове і практичне осмислення проблеми загроз у кіберпросторі.

Ступінь розробленості теми

Термінологічними проблемами у сфері безпеки кіберпростору переймалися такі зарубіжні дослідники, як Дж. Ліпман [11], Д. Фахренкург [7], Ф. Крамер, Л. Вентц [9], Дж. Льюіс [10], а також вітчизняні - О. Порфимович [25], А. Марченко [23], Ю. Федорова [28], М. Погорецький, В. Шеломенцев [24], О. Манжай [22],

Мета статті – дослідити особливості підходів до визначення тезаурусу сфери кібербезпеки серед науковців США та України.

Ключовою проблемою у формуванні тезаурусу сфери „кібербезпеки" є визначення того, що саме належить розуміти під поняттям „кіберпростір". Американський дослідник Дж. Ліпман зазначає, що важливим є „...розуміння того, чим є кіберпростір (і чим він не є), а також того, що означає боротьба у кіберпросторі" [11, с. 74]

Американські дослідники, які працюють у мілітарному дискурсі кібербезпеки [7; 9], вважають, що базовим визначенням поняття „кіберпростір" в американській практиці дослідження проблем кібербезпеки має бути запропоноване у документі „Національна військова стратегія для операцій у кіберпросторі" 2006 року, де кіберпростір визначений як „...сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язану з ними фізичну інфраструктуру" [13, с. 9]. Це ж визначення було покладено

проблеми методології

в основу і розробки документа „Стратегічне бачення. Кіберкомандування повітряних сил" (2008 рік) [1] та „Стратегії національної безпеки США" (2010 року), де зазначається, що „військові повинні і надалі мати можливість захищати інтереси США у всіх основних сферах – на землі, у повітрі, на воді, в космосі та в кіберпросторі" [15, с. 22]. Отже в сучасному офіційному безпековому дискурсі США кіберпростір розглядається саме як „фізичний" простір.

Водночас Дж. Ліпман наполягає [11], що такий підхід характерний саме для фахівців з міністерства оборони США (і ВПС зокрема), однак останнім часом відбувається часткове зміщення точок зору (в тому числі й серед військових спеціалістів) у бік розуміння кіберпростору як теоретичного (чи, швидше, віртуального) поняття. Вартим уваги також є визначення, запропоноване П. Вуллей з Інституту технологій повітряних сил США, яка пропонує розуміти кіберпростір „...як створене людиною цифрове довкілля, що використовується для миттєвого, безкордонного, глобального, без організаційних, культурних, національних чи політичних кордонів збору, зберігання і передачі даних та інформації між електронним обладнанням" [16, с. 8]. Водночас не можна не відзначити, що „Кібербезпековий огляд" США від 2009 року (комплексний документ з оцінки стану кібербезпекового простору США і можливих шляхів його поліпшення) розуміє кібербезпеку відповідно до визначення, запропонованого у Президентській Директиві з національної безпеки 54 / Президентській Директиві з внутрішньої безпеки 23 (NSPD-54/HSPD23), які визначають кіберпростір як „... взаємозалежні мережі, комп'ютерні системи, IT-інфраструктури, що включають Інтернет, телекомунікаційні мережі, комп'ютерні процесори та контролери у критично важливих сферах" [6, с. 1].

У підготовленій фахівцями „Центру стратегічних та міжнародних досліджень" (за загальним керівництвом Дж. Льюіса) доповіді „Безпека кіберпростору для 44-го президентства" кіберпростір тлумачиться як „... дещо більше, ніж просто мережа Інтернет, і включає в себе всі мережеві форми та цифрову активність (діяльність)" [10, с. 11]. Водночас автори документа зазначають, що загрози від кібератак виявились не зовсім такими, якими очікувались: „...ми вважали, що наслідки від кібератаки будуть переважно фізичними (відкриття греблі, падіння авіалайнерів), вони ж в реальності носять яскраво виражений інформаційний характер" [10, с. 12]. При цьому наводяться приклади численних проникнень хакерів у інформаційні системи з метою викрадення певної інформації, перехоплення e-mail листування посадових осіб тощо.

Слід зазначити, що більшість інцидентів, які наводяться для ілюстрування цієї тези, пов'язують з діяльністю хакерів з Китаю. Фахівці з Центру стратегічних та міжнародних досліджень зазначають також, що „...головні загрози критичній інфраструктурі виходять, у першу чергу, від військових та розвідувальних служб інших держав, оскільки саме вони підготовлені необхідним чином, мають необхідні ресурси і ставлять перед

собою чіткі цілі" [10, с. 13]. Цієї ж думки дотримуються й укладачі вже згадуваного „Кібербезпекового огляду" США від 2009 року, зазначаючи, що „...зростання зв'язків між інформаційними системами, Інтернетом, іншими інфраструктурами створює можливості для зловмисників порушити зв'язок, постачання електроенергії, пошкодити трубопроводи, нафтопереробні заводи, фінансові структури та інші критично важливі об'єкти інфраструктури" і що „розвідувальна спільнота вважає, що ряд країн вже має технічні можливості для проведення таких атак" [6, с. 2]. При цьому не зазначається можливість доступу до таких „технічних можливостей" недержавних акторів.

Вітчизняні науковці, досліджуючи поняття кіберпростору, працюють переважно у загальнофілософському або ж у юридичному дискурсі. Так, у студіях щодо значення терміна „кіберпростір" О. Манжай пропонує таке визначення: „Це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами" [22, С. 145]. У свою чергу, А. Погорецький та В. Шеломенцев пропонують під „кіберпростором" розуміти „...штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг ведення електронної комерції тощо)" [24, с. 80].

Не повністю визначеним залишається питання стосовно того, що саме слід розуміти під поняттям „кібербезпека" та „війна в кіберпросторі" (кібервійна). Дж. Ліпман пропонує для військової сфери США таке визначення „кібербезпеки": „Забезпечити для США свободу дій, контроль доступу та визначення місцезнаходження супротивника у кіберпросторі" [11, с. 73]. У документі „Стратегічне бачення. Кіберкомандування повітряних сил" зазначається, що кібербезпеку держави слід розуміти як своєрідну сукупність категорій: „використання кіберпростору" (атаки у кіберпросторі та збільшення власних сил), „контролювання кіберпростору" (оборонні дії у кіберпросторі та атакуючі контрдії у кіберпросторі) і „налаштування кіберпростору" (глобальні спостережні операції у кіберпросторі, операції з управління і контролю за мережами та безпекою, операції з цивільної підтримки у кіберпросторі) [1, с. 11].

„Директива президента з національної безпеки 54" поділяє сферу кібербезпеки на три ключові компоненти: атаку комп'ютерних мереж, захист комп'ютерних мереж та управління ними. Крім того, саме на

проблеми методології

Міністерство оборони США (а вже потім на розвідувальні та правоохоронні органи) покладається обов'язок забезпечення кібербезпеки.

Американський дослідник С. Бейделман [3, с. 11] зазначає, що поняття „війна в кіберпросторі" є надто широкою дефініцією у його сучасному трактуванні. Кібервійна не є просто синонімом інформаційних операцій, однак цілком може бути їх компонентою. Інформаційні операції включають в себе психологічні операції, військову хитрість, операції із забезпечення безпеки, електронну війну та операції в комп'ютерних мережах [8]. Операції в комп'ютерних мережах описуються як „використання комп'ютерних мереж" для атаки „...інформації, що міститься на комп'ютерах і комп'ютерних мережах, або самих комп'ютерів і мереж [8, II-5] Під час кібервійни кіберпростір використовується для атаки персоналу, будівель або обладнання на додачу до інформації та комп'ютерів [2], і саме це – чіткий зв'язок між комп'ютерним середовищем та фізичною інфраструктурою і довкіллям – є визначальним для виокремлення кібервійни в окрему сферу військових дій.

В більшості ж менш чітких визначень „кібербезпеки" ключовим стає можливість захиститись (чи ефективно протидіяти) „кібератакам". Водночас цей термін також практично не визначений в більшості критично важливих офіційних документів.

У доповіді Дослідницької служби Конгресу США RL30735 дослідник С. А. Хілдрет відзначав, що кібератаки або кіберзагрози - це несанкціоновані спроби проникнення в комп'ютери, керовані комп'ютерні системи чи мережі [29]. Розроблений 2000 року в США „Національний план захисту інформаційних систем" під кібератакою розуміє „використання вразливостей в програмному забезпеченні компонентів управління, що базуються на інформаційних технологіях" [14, с. 148]. С. Бейделман на основі визначення „операція в кіберпросторі", що наводиться у спеціальному військовому словнику „Словник військових та пов'язаних з ними термінів" Міністерства оборони США [8], пропонує власне визначення терміна „кібератака": „Кібератака може розглядатись як сукупність кібероперацій з використанням ворогом комп'ютерів та інформаційних технологій з метою досягнення певних ефектів чи цілей через кіберпростір" [3, с. 12].

Однак жодне з визначень „кібератак" не дає розуміння того, хто є їх суб'єктом. Крім того, залишається не визначеним, у якому співвідношенні слід розуміти поняття „кібератака" і „кібервійна": чи є кібератака елементом кібервійни, чи сукупність кібератак призводить до кібервійни, чи кібератаки і кібервійни є цілком незалежними поняттями, що перетинаються лише ситуаційно.

З огляду на брак таких пояснень, ми пропонуємо своє визначення „кібератаки": „Кібератака може розглядатись як сукупність дій супротивника чи ворожої групи, що прагне досягти певної негативної для об'єкта атаки цілі чи ефекту з використанням комп'ютерної техніки зокрема чи можливостей кіберпростору в цілому, частіше за все – з

використанням спеціально розроблених для таких завдань засобів". Сукупність кібератак, що перевищують за своїм загальним негативним впливом певне порогове значення, можуть розглядатися як початок кібервійни. Хочемо зазначити, що проблема визначення „порогового значення" та вписування кібератак у контекст міжнародного права (як „акту війни") є важливою проблемою для методологічних досліджень у сфері національної та міжнародної безпеки.

Окремо хотілось би зупинитись на понятті, що активно використовується вітчизняними дослідниками – „кібертероризм". Не можна не зазначити, що значною мірою вітчизняні науковці оперують поняттям кібертероризму, часто розуміючи під ним і „кібервійни", і „кібератаки" тощо, що неправильно як з методологічної точки зору, так і стосовно відображення сучасних реалій цієї безпекової сфери.

Навіть у західній науковій літературі термін „кібертероризм" та опис можливих наслідків актів кібертероризму має переважно ідеологічно-пропагандистську та абстрактно-теоретичну компоненту, що обумовлюється проголошеною за часів президентства Дж. Буша-молодшого „глобальної війни з тероризмом". До останнього ж часу більшість реальних загроз критично важливій інфраструктурі інформаційно розвинених держав (США, Велика Британія, Німеччина) надходили не від поодиноких терористичних груп, що просто змінили безпосередню тактику ведення своєї боротьби, а від спеціально підготовлених інформаційно та матеріально забезпечених спеціалізованих груп, що функціонують в інтересах тих чи інших держав і є фактично продовженням їх „військової машини".

У ґрунтовній праці „Кібервійна та кібертероризм" (за редакцією Л. Жанчевскі і А. Коларіка) дається таке визначення кібертероризму: „Кібертероризм - це політично мотивовані атаки, що здійснюються субнаціональними групами чи таємними агентами або окремими індивідами проти інформаційних та комп'ютерних систем, комп'ютерних програм чи даних, результатом яких є насилля проти нонкомбатантів[1]" [5, с. 13]. На нашу думку, це визначення містить дві ключові компоненти, що мають відокремлювати кібертероризм від всіх інших форм кіберзлочинів: наявність доведеної „політичної мотивації" та бажання здійснити „насилля проти нонкомбатантів".

„Словник тероризму" описує кібертероризм як „злочин, до якого в майбутньому буде вдаватися криміналітет, використовуючи комп'ютери". При цьому зазначається, що „кібертерористи мають політичну мотивацію для їх злочинів" [16, с. 61]. М. Каветлі пропонує таке визначення

[1] „Нонкомбатанти – особи, що входять до складу збройних сил, однак функції яких полягають лише в обслуговуванні та забезпеченні військової діяльності збройних сил, і які мають право використовувати зброю лише у випадку самозахисту". Та в цьому випадку йдеться швидше про цивільне населення в цілому.

проблеми методології

кібертероризму: „Під кібертероризмом розуміємо незаконні напади з боку недержавних суб'єктів стосовно комп'ютерів, мереж та інформації, що міститься в них, які здійснюються з метою залякування уряду (чи населення) чи з метою досягнення певної поведінки суб'єкта, що залякується. Кібератака може розумітись як кібертероризм лише в тому випадку, якщо це призводить до фізичного насилля проти осіб чи власності або виникнення значного страху у зв'язку з можливістю здійснення таких наслідків" [12, с. 1].

Немає однозначності у трактуванні зазначеного поняття і у працях вітчизняних науковців. У більшості випадків дослідники широко використовують терміни „кібертероризм", „кібератака" тощо, не подаючи при цьому жодних визначень чи тлумачень, оперуючи розпливчастими поняттями на кшталт „звичайні кібератаки" (див., наприкл. [25]). Тим часом О. Порфимович пропонує таке визначення кібертероризму: „... це терористичні дії в кіберпросторі та політично активне хакерство, вчинені з метою завдати серйозних збитків життєдіяльності людини та економіці країни" [25, с. 29], а до найбільш вдалих дослідниця відносить визначення, запропоноване американським дослідником К. Вілсоном: „...це використання комп'ютерів як зброї політично мотивованими міжнародними або національними групами чи таємними агентами, котрі завдають або загрожують завдати шкоди чи посіяти паніку з метою вплинути на населення або уряд для зміни політики" [4].

Так само до проблеми „кібертероризму" звертається і А. Марченко [23], розуміючи під ним „...навмисне застосування окремими особами, терористичними групами або організаціями засобів інформаційного насильства з метою руйнації єдиного інформаційного поля, нанесення економічної шкоди країні, створення атмосфери істерії в соціумі, нав'язування конкретної лінії поведінки у вирішенні внутрішніх і зовнішніх суперечок" [23, с. 356]. Однак дослідниця не вказує на різницю між „кібертероризмом" та „комп'ютерним тероризмом", що, на нашу думку, методологічно неправильно, оскільки поняття кіберпростору значно ширше за своїм змістом, ніж просте використання комп'ютерної техніки.

Лінгвіст Ю. Федорова вважає, що такі поняття, як „кібербезпека" (cybersecurity), „кібератака" (cyberattack), „кіберзброя" (cyberweapon), „кіберзахист" (cyberdefence) співвідносяться і протиставляються з ключовими поняттями „кібертероризм" (cyberterrorism) [28].

Вітчизняні офіційні нормативні документи у сфері національної безпеки не дають відповіді щодо того, як саме держава розглядає проблему кібербезпеки і чи існує вибудована стратегія ведення протиборства в кіберпросторі. У „Стратегії національної безпеки України" (від 12 лютого 2007 року) [27] зазначається лише, що Україна має „розробляти та впроваджувати національні стандарти та технічні регламенти застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі

й згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність", однак сама Конвенція про кіберзлочинність (ратифікована українським парламентом ще 2005 року) [20], не має прямого стосунку до власне проблем убезпечення кіберпростору держави від кібератак (які мають переважно військовий характер), а зосереджена на протидії карним діям (шахрайство, підробка, поширення дитячої порнографії, порушення авторських прав тощо) з використанням комп'ютерної техніки та різних мереж.

Більше уваги кібербезпеці та питанням, пов'язаним з нею, приділено у „Доктрині інформаційної безпеки України" [26]. У ній згадуються і поняття „комп'ютерний тероризм", і „кібератаки", однак жодних пояснень цих термінів у преамбулі не знайти. Так само і в Законі України „Про основи національної безпеки" [19] зустрічається лише поняття „комп'ютерний тероризм" та „комп'ютерна злочинність".

На нашу думку, труднощі з вивченням явища кібертероризму пов'язані, в першу чергу, з тим, що прикладів кібертерактів чи подій, які могли б бути цілком однозначно віднесені саме до кібертерористичної діяльності, немає. Так, у дослідженні Л. Жанчевські і А. Коларіка зазначається, що „...донині не було серйозних дій кібертерористів, хоча комп'ютерні мережі піддавались атакам в ході конфліктів у Косово та на Близькому Сході" [5, с. 1]. Водночас висловлюється припущення, що „...через те, що терористи мають обмежені фінансові можливості, кібератаки стають більш привабливими, оскільки вони потребують меншої кількості людей та меншої кількості ресурсів" [5, с. 2]. На нашу думку, це твердження досить дискусійне, оскільки, незважаючи на те, що для кібертерактів теоретично і справді потрібно менше людських ресурсів, однак це висуває підвищенні вимоги до їх кваліфікації. Крім того, розробка (чи навіть придбання) спеціального програмного забезпечення, що може використовуватися для подібних дій, теж потребують коштів, а ймовірність бути відстеженим при використанні таких засобів без підтримки (політичної і технічної) певної держави надто велика.

Не можна не відзначити й те, що навіть автори цього дослідження, наводячи приклади терактів з використанням інформаційних технологій, певною мірою суперечать собі, коли пропонують розглядати в якості теракту, наприклад, події в Австралії у березні 2000 року, коли невдоволений працівник, користуючись мережею Інтернет (вдалось йому це з 45 разу – перші 44 атаки просто ніхто не помітив), випустив мільйон літрів стічних вод у ріку й прибережні території Квінсленду. Водночас не важко побачити, що ця дія не була „політично мотивована" і „не мала на меті здійснити насилля проти нонкомбатантів".

Як у вітчизняній, так і в західній літературі з проблем кібертероризму до кібертерактів традиційно відносять акцію 1998 року, здійснену „Тиграми звільнення Таміл Іламу", коли спеціальний підрозділ цієї організації намагався масовою розсилкою електронної пошти на певні адреси

проблеми методології

призупинити діяльність серверів дипломатичних представництв Шрі-Ланки [21]. Однак, оперуючи наведеним вище двокомпонентним поняттям „кібертероризму", можна помітити, що ця акція не мала на меті завдати жодної фізичної шкоди нонкомбатантам, а за своїм характером більше нагадувала спам-розсилку, що активно використовується в протиправній діяльності хакерських організацій. Крім того, симптоматично, що ця акція відноситься до 1998 року, однак більш свіжі приклади такої діяльності не наводяться, що теж може свідчити про значно перебільшений характер загрози від кібертероризму та про можливість його існування взагалі.

М. Каветлі наводить [12, с. 1 - 2] власну типологію кіберконфілктів (за ступенем їх загрози), застосування якої може дати більш адекватну відповідь про місце кібертероризму в структурі кібербезпеки й того, до якої категорії належить більшість прикладів кібертероризму, що наводяться дослідниками:

1) **кібервандалізм** (включає в себе зміни чи знищення змісту, наприклад, веб-сайту, відключення чи перевантаження сервера; це найбільш поширена форма кіберконфлікту, що отримує значний суспільний резонанс, однак наслідки таких інцидентів обмежені у часі та відносно незначні);

2) **інтернет-злочини** (діяльність переважно з метою отримання прямого фінансового зиску від такої діяльності; може включати як злочини з комп'ютерної техніки, так і суто комп'ютерні злочини);

3) **кібершпигунство** (головною жертвою найчастіше стає корпоративний сектор; за деякими підрахунками втрати компаній від такої діяльності становлять до трильйона доларів на рік; урядові мережі, в яких міститься конфіденційна інформація, стають жертвами атак доволі рідко, хоча останнім часом такі атаки стають все частішими);

4) **кібертероризм** (під кібертероризмом розуміють незаконні напади з боку недержавних суб'єктів стосовно комп'ютерів, мереж та інформації, що міститься в них, які здійснюються для залякування уряду (чи населення) чи з метою досягнення певної поведінки суб'єкта, який залякується; кібератаку можна розуміти як кібертероризм лише тоді, коли це призводить до фізичного насилля проти осіб чи власності або виникнення значного страху можливості здійснення таких наслідків; потенційно масштаби збитків від кібертерakту оцінюються дуже високо, однак досі не було жодного реального випадку кібертероризму);

5) **кібервійна**.

З огляду на запропоновану класифікацію, „акти кібертероризму", як їх найчастіше розуміють дослідники, застосовуючи цей термін, це, швидше, рівень „кібервандалізму" (злам сайтів з метою порушення їх роботи та/чи зміни їх контенту) або „Інтернет-злочинів" (махінації з метою отримання передусім фінансового зиску від своєї діяльності), однак і та і та діяльність більшою мірою перебуває в межах компетенції правоохоронних органів і

до справжнього тероризму стосунку не має, якщо, звичайно, не намагатись штучно розширювати межі поняття „тероризм".

Висновки

Незважаючи на значну кількість наукових дискусій щодо необхідності забезпечення кібербезпеки держав, тезаурус сфери кібербезпеки все ще залишається вкрай нечітким, що характеризується значною різницею у підходах, а подекуди й публіцистичним (журналістським) викладом проблеми.

Порівнюючи підходи до поняття „кіберпростір" і „кібертероризм", що пропонуються науковцями з США, офіційними документами, вітчизняними науковцями, можна констатувати, що американські підходи більш орієнтовані на можливість використання визначень у суто практичній діяльності (формування ефективних стратегій національної безпеки, доктринальних документів у сфері кібербезпеки для тих родів військ чи силових відомств, на які покладається обов'язок його захисту). Водночас визначення, що пропонуються вітчизняними дослідниками, багато в чому носять загальнотеоретичний характер, а почасти вони перевантажені різними уточненнями.

До останнього часу у вітчизняній науковій літературі не відбувалося фахових дискусій стосовно значної кількості термінологічних проблем у сфері кібербезпеки (брак визначень понять „кібератака", „кібервійна", „кібербезпека"), що ускладнює методологічний та науковий супровід прийняття державних рішень з цієї тематики.

Перспективи подальших розвідок

Суттєвого уточнення потребують такі терміни, як „кібервійна", „кіберпростір", „кіберзахист". До важливих методологічних проблем, що потребують масштабних наукових розвідок, можна віднести й розробку системи порогових значень для кібератак та розгляду кібератак як „акту війни".

Література:

1. Air Force Cyber Command Strategic Vision [Electronic resource] / DTIC Online.- Access mode: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060&Location= U2&doc=GetTRDoc.pdf

2. **Alexander B. Keith.** Warfighting in Cyberspace [Electronic resource] / U.S. Army War College, Joint Force Quarterly.- Access mode: http://www.carlisle.army.mil/DIME/documents/Alexander.pdf

3. **Beidleman W. Scott.** Defining and deterring cyber war [Electronic resource] / U.S. Army War College, Carlisle Barracks. - Access mode: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf &AD=ADA500795

проблеми методології

4. **Clay W.** Computer Attack and Cyberterrorism (Vulnerabilities and Policy Issues for Congress) [Electronic resource] / Federation of American Scientists. - Access mode: http://www.fas.org/sgp/crs/terror/index.htm

5. Cyber Warfare and Cyber Terrorism (edited by Lech J. Janczewski and Andrew M. Colarik). - Hershey, PA: Information Science Reference, 2008. - 532 p.

6. Cyberspace Policy Review [Electronic resource] / White House. - Access mode: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_ Review_final.pdf

7. **Fahrenkrug T. D.** Cyberspace Defined [Electronic resource] / Air University. - Access mode: http://www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm

8. Joint Publication 3 - 13, „Information Operations" [Electronic resource] / United State Army Combined Arms Center.- Access mode: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090228_art013.pdf

9. **Kramer D. F., Wentz L.** Cyber Influence and International Security [Electronic resource] / Defense Horizons.-№61.- P. 1 - 11. - 2008. - – Access mode: http://www.carlisle.army.mil/DIME/documents/Kramer%20and%20Wentz%20Cyber%20Influence%20and%20International%20Security%5D.pdf

10. **Lewis A. J.** Securing Cyberspace for the 44th Presidency [Electronic resource] / Centre for Strategic and International Studies. - 2008. - Access mode: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44 .pdf

11. Liepman M. James, Jr. Cyberspace: The Third Domain [Electronic resource] / Homeland security digital library.- Access mode: https://www.hsdl.org/?view&doc=89385&coll=public

12. **Myriam Dunn Cavelty.** Cyberwar: concept, status quo, and limitations [Electronic resource] / Center for Security Studies (CSS), ETH Zurich. - Access mode: www.sta.ethz.ch

13. National Military Strategy for Cyberspace Operations [Electronic resource] / Department of Defense – Access mode: - http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf

14. National Plan for Information Systems Protection [Electronic resource] / Federation of American Scientists.- Access mode: www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

15. National Security Strategy / White House. - http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

16. **Thackrah J. R.** Dictionary of Terrorism. - NY.: Taylor & Francis, 2004. - 318 p.

17. **Woolley P.** Defining Cyberspace as a United States Air Force Mission / Pamela Woolley [Electronic resource] / Air Force Institute of technology. - Access mode: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA453972&Location=U2&doc=GetTRDoc.pdf

18. В мире два десятка стран занимаются кибероружием – McAfee [Электронный ресурс] // Cybersecurity.ru. – Режим доступа: http://www.cybersecurity.ru/armament/86546.html

19. Закон України „Про основи національної безпеки України" // Відомості Верховної Ради України. – 2003. – №39. – Ст. 351.

20. Конвенція про кіберзлочинність // Офіційний вісник України від 10.09.2007. - 2007. - №65. - С. 107.

21. **Луценко А. В.** Оцінка впливу кібертероризму на зовнішню політику держав: нові підходи до стратегії „м'якої сили" у геополітиці США / А. Луценко // Акутальні проблеми міжнародних відносин. - Вип. 85 (Ч. 2). - 2009. - С. 78 – 82.

22. **Манжай О. В.** Використання кіберпростору в оперативно-розшуковій діяльності / О. Манжай // Право і безпека. Науковий журнал. - 2009. - №4. - С. 142 – 149.

23. **Марченко А. В.** Соціальні наслідки кібертерористичної небезпеки в епоху інформаційних технологій / Анна Марченко // Методологія, теорія та практика соціологічного аналізу сучасного суспільства. Збірник наукових праць Харківського національного університету імені В. Н. Каразіна. - 2008. - №1. - С. 355 – 360.

24. **Погорецький М., Шеломенцев В.** Поняття кіберпростору як середовища вчинення злочинів / Микола Погорецький, Володимир Шеломенцев // Інформаційна безпека людини, суспільства, держави. - 2009. - №2. - С. 77 – 81.

25. **Порфимович О.** Віртуальний криміналітет: від хакера до терориста (портрет явища) / Ольга Порфимович // Актуальні питання масової комуінкації. - Вип. 9 (електронна версія). - 2008. - С. 25 – 34.

26. Про Доктрину інформаційної безпеки України // Офіційний вісник Президента України від 20.07.2009. - 2009. - №20. - С. 18.

27. Про Стратегію національної безпеки України // Офіційний вісник України від 23.02.2007. - 2007. - №11. - С. 7.

28. **Федорова Ю.** Структурування та інноваційна вербалізація понятєвих вузлів англомовної картини світу у галузі комп'ютерних технологій / Юлія Федорова // Наукові записки Кіровоградського державного педагогічного університету імені Володимира Винниченка. Серія: Філологічні науки. - Вип. 81(4). - 2009. - С. 56 – 59.

29. **Хилдрет С. А.** Кибертерроризм. Материалы Исследовательской службы Конгресса. Доклад Исследовательской службы Конгресса RL30735, Кибервойна. [Электронный ресурс] / InfoUSA.ru.– Режим доступа: http://www.infousa.ru/information/bt-1028.htm.