УДК 007.51:004.491

Р.В. Грищук,
доктор технічних наук, старший науковий співробітник

КІБЕРНЕТИЧНА ЗБРОЯ: КЛАСИФІКАЦІЯ, БАЗОВІ ПРИНЦИПИ ПОБУДОВИ, МЕТОДИ ТА ЗАСОБИ ЗАСТОСУВАННЯ Й ЗАХИСТУ ВІД НЕЇ

У статті аргументовано доведено, що кібернетична зброя на сьогодні одним із найновіших та найдієвіших зразків сучасної зброї. Розкрито етимологію поняття зброя та показано сучасні підходи до її трансформації в кібернетичну. Запропоновано нову класифікацію кібернетичної зброї, яка позбавлена від більшості недоліків відомих класифікацій. Розкрито характерні ознаки, властиві кібернетичній зброї, та визначено основні завдання, що покладаються на неї її розпорядниками.

Ключові слова: *кібернетична зброя, класифікація, кібервійна, кібербезпека, кібервплив, кіберрозвідка, кіберзахист.*

В статьи аргументированно доказано то, что кибернетическое оружие сегодня выступает одним из новейших и найдействиннейших образцов современного оружия. Также раскрыто этимологию понятия оружие в общем его понимании и применительно к кибернетическому оружию. Получила дальнейшее развитие классификация кибернетического оружия, в которой отсутствуют недостатки известных классификаций. Раскрыты характерные признаки, свойственные кибернетическому оружию, и определены основные задания, возложенные на него его распорядителями.

Ключевые слова: *кибернетическое оружие, классификация, кибервойна, кибербезопасность, кибервоздействие, кибеpразведка, киберзащита.*

It is proved in a well-argued manner in part I of the paper that cyber weapon is one of the most advanced and effective sample of modern weapon nowadays. It is also explained the etymology of the concept of weapon both in general and in respect to cyber weapon. It is suggested a new classification of cyber weapon without drawbacks of previous classifications. It is described the main characteristics relevant to cyber weapon and defined the main tasks designated to it by the owners.

Keywords*: cyber weapon, classification, cyber war, cyber security, cyberattack, cyber intelligence, cyber protection.*

Постановка проблеми в загальному вигляді та її зв'язок з важливими практичними завданнями. Вивчення та аналіз відкритих джерел у галузі військового мистецтва показав, що одним із важливих інструментів гібридних дій збройних сил провідних держав світу є кібернетичні дії [1–4; 5]. Водночас кібернетичні дії, які відбуваються між державами в кіберпросторі без силової (вогневої) підтримки військ (сил) у класичних театрах воєнних дій, можуть переростати в нове явище, яке ще інколи називають кібервійною [1; 2]. Наприклад,

у світі вже де-факто відбулися дві кібервійни, ініціатором яких як у першому, так і в другому випадку була Російська Федерація [6; 7].

Вивчивши досвід ведення перших кібервійн, встановлено, що ключовим інструментом їх реалізації, крім відповідних сил та засобів, є кібернетична зброя (далі – КЗ) [6–8; 9]. Незважаючи на значну кількість досліджень у згаданій царині, на сьогодні й надалі залишаються актуальними питання про те, що слід розуміти під КЗ на сучасному етапі розвитку науки і техніки, якою ця зброя буває, на яких принципах ґрунтується, які існують методи та засоби її застосування й захисту від неї, тощо.

Аналіз останніх досліджень і публікацій показав, що дослідженню питань, пов'язаних із вивченням ролі та місця КЗ в системі забезпечення національної безпеки та оборони в розвинених державах світу, приділяється значна увага наукової спільноти. Останнім часом у відкритому доступі з'явилося кілька десятків наукових публікацій [1–14]. З аналізу цих джерел випливає те, що найбільшої уваги науковці приділяють, головним чином, питанням дефініційного характеру та, власне, класифікації такої зброї та ін [1; 11–13; 16; 17]. Поза увагою, як правило, залишаються найбільш проблемні питання, що потребують глибшого та системного дослідження. Зокрема, це такі питання, як принципи побудови КЗ, способи та методи її застосування, питання захисту тощо. Таким чином, систематизація відомих досліджень, їх упорядкування та подання через призму власного досвіду забезпечення кібербезпеки, повинно забезпечити передумови для створення єдиної наукової платформи при оперуванні таким важливим для оборони держави поняттям, як КЗ.

Метою статті є розкриття невизначеності з питань сутності та змісту кібернетичної зброї, її класифікації, базових принципів побудови, методів та засобів застосування та захисту від неї.

Викладення основного матеріалу дослідження. Перш ніж перейти до розгляду питання класифікації КЗ, необхідно розглянути саме поняття "зброя". Так, ретроспективний аналіз розвитку збройної боротьби показує, що будь-яка війна, незалежно від її мети та цілей протиборчих сторін, ведеться з використанням зброї [5]. Водночас зброя є не тільки основною формою боротьби у війні, а й її специфічним змістом. У сучасну епоху повсюдної комп'ютеризації та економічної взаємозалежності держав уже очевидним є факт того, що сучасна війна або локальний збройний конфлікт як на етапі підготовки, так і на етапі проведення не відбувається без дій у кіберпросторі [5]. Саме ця обставина і вимагає кардинального перегляду сфери дії таких усталених у класичному розумінні понять, як "війна" та "зброя".

Систематизувавши найбільш поширені в енциклопедичних виданнях визначення поняття "зброя" й опираючись на останні наукові дослідження, наприклад, можна зробити висновок про те, що не всі засоби ураження або завдання шкоди протиборчій стороні називаються зброєю [16; 17]. Зброєю можуть називатися тільки спеціально створені для збройної боротьби й ті, що застосовуються під час її ведення, засоби ураження противника та його інфраструктури. Водночас наявність у розпорядженні провідних розвинених держав надзвичайно широкого спектра новітніх засобів ураження, зростання розмаїття способів і технологій їх застосування, постійного збільшення кількості цілей ураження – об'єктів критичної кібернетичної інфраструктури (далі – ОККІ) й особливо

кібернетичної в різних сферах, потенційно може призвести до виникнення ефекту ланцюгової реакції, внаслідок якого проявлятимуться не тільки прямі, а й опосередковані наслідки від застосування зброї. Саме тому сьогодні класичне й уже усталене поняття зброя є застарілим та потребує уточнення, незважаючи на те, якого виду зброї воно стосується, – вогнепальної, холодної, ядерної, біологічної, хімічної, геофізичної, інформаційної, кібернетичної тощо. Отже, розглянемо сутність та зміст КЗ як об'єкта цього дослідження.

Кібернетична зброя, як стверджується в статті *"Nation state sponsored attacks: the offensive of Governments in cyberspace"* головного технічного редактора журналу *CyberDefense* П. Паганіні, нині розробляється, досліджується та застосовується урядами близько 140 держав світу. Найбільші успіхи здобули такі держави, як США, РФ, Китай, Великобританія. Незважаючи на це, ні на регіональному, ні на міжнародному рівнях немає однозначного розуміння того, що ж саме слід розуміти під КЗ та як потрібно здійснювати її класифікацію. Термінологічна та правова невизначеність стосовно категорії КЗ, що склалася на сьогодні у світовому масштабі, породжує перед суспільством ряд проблем як організаційного, так і технологічного характеру. З одного боку, це проблеми, пов'язані з питаннями правової та політичної відповідальності тієї чи іншої держави в разі застосування нею КЗ, з іншого, – привід до розвитку нового витку гонки озброєнь – кіберозброєнь.

З моменту першого виявлення 17 червня 2010 року співробітником білоруської компанії *"ВирусБлокАда"* С. Уласенем, а нині співробітником компанії *"Лаборатория Касперского"* хробака *win32/Stuxnet* почався новий етап у розвитку сфери комп'ютерної вірусології – вірусології військового призначення. Пізніше, у липні 2010 року, після ґрунтовного аналізу цього комп'ютерного хробака незалежними представниками компанії *"Лаборатория Касперского"* та корпорації *Symantec* запропоновано *дату 17 червня 2010 року офіційно вважати початком зародження нової віхи в історії зброї.* Уперше у світі для досягнення стратегічних та політичних цілей державою або групою держав проти іншої держави застосовано новітній зразок зброї – комп'ютерний хробак *Stuxnet*, який справедливо можна віднести до зброї нового виду, яка й одержала назву кібернетичної.

Очевидно, причиною, що спонукала експертів до таких висновків, була надзвичайна складність цього зразка зброї. Розробити такий зразок без висококласних професіоналів із різних галузей та без належної державної фінансової підтримки неможливо. Орієнтування цього зразка зброї на конкретну ціль – зрив технологічних процесів в АСУ промисловими об'єктами Ірану також підтверджує справедливість зазначеного висновку [14]. Водночас політичною ціллю, що переслідувалася державою (державами) – розробниками хробака *Stuxnet,* можна вважати дискредитацію правлячого режиму в Ірані, а стратегічною – зрив темпів виконання національної ядерної програми.

Починаючи з 2012 року, відбувається сплеск досліджень з питань формування нового науково-категоріального апарату, присвяченого тлумаченню дефініцій з приставкою *"кібер"*. Майже одночасно видано ряд праць відомими у світовому ІТ-товаристві експертами з кібербезпеки, а саме *"Cyber-weapons",* опублікована в журналі *RUSI JOURNAL* за лютий – березень професором П. Макберні та його колегою доктором Т. Рідом з Лондонського королівського коледжу; *"Cyberweapons aspetti giuridici e strategici"*, опублікована у квітні в працях Італійського інституту

стратегічних досліджень "Нікколо Макіавеллі" доктором С. Меле; *"Cyber-weapons"* – доповідь, зроблена в жовтні головним технічним редактором журналу *CyberDefense* – експертом з питань безпеки П. Паганіні на міжнародному саміті *Cyber Threat Summit 2012* у м. Дубліні (Ірландія); *"Кибервойна и кибероружие"*, опублікована начальником відділу науково-освітніх розробок Управління інноваційного розвитку Московського державного інституту міжнародних відносин Міністерства зовнішніх справ РФ В. Каберніком, та ін.

У статті *"Cyber-weapons"* П. Макберні та Т. Ріда наводяться аргументи того, що КЗ не може належати до класу справжньої зброї, оскільки за позицією авторів вона не спричиняє руйнівних наслідків для об'єктів, на які здійснюється кібервплив. Автори стверджують, що чим складніше вірус (програмний код розуміється ними під прототипом КЗ), тим глибше він спроможний проникнути в систему і тим менші побічні ефекти матимуть об'єкти, які не є ціллю кібервпливу. Спираючись на точковий ефект від застосування подібних інструментів, з-поміж яких використовуються інструменти бот-мережі для організації DDoS-атак та відповідні програмні продукти з метою проведення кібернетичних акцій щодо тимчасового порушення доступності інформаційних ресурсів протиборчої сторони, вони мають найменш небезпечний ефект для об'єктів кібернападу. По суті, співавтори наголошують на тому, що на сьогодні складається парадоксальна ситуація, яка полягає в існуванні протиріччя між величиною вкладення інтелектуальних та фінансових ресурсів та ефектом, який наступає від застосування подібних інструментів. Тобто чим більше ресурсів витрачається на розробку інструменту – тим ефект від його застосування менш помітний.

Згідно з дослідженнями доктора С. Меле, КЗ – це пристрій або комп'ютерна програма, які призначені для незаконного пошкодження комп'ютерних систем та телекомунікаційних мереж, що належать до кібернетичної інфраструктури та часткової або повної зміни усталених режимів їх роботи, що, як наслідок, призводить до припинення їх функціонування.

П. Паганіні в КЗ вбачає пристрій, прилад або набір комп'ютерних команд, що призначені для завдання шкоди людині через кіберпростір. Тобто, якщо виходити з наведених дефініцій, – точки зору експертів розділися.

Найбільш близько визначення КЗ, що відповідає її сутності, виходячи з дефініції "кібернетика", на наш погляд, наведено В. Каберніком у його публікації *"Кибервойна и кибероружие"*. Автор наголошує на типовій помилці, якої припускаються західні експерти при тлумаченні терміну КЗ. Об'єктом, на який здійснюється вплив КЗ, за В. Каберніком, є кібернетична система, як-то комп'ютерна система, АСУ технологічними процесами чи людина як біологічна система, тобто будь-яка система зі зворотним зв'язком. Водночас наявність зворотного зв'язку в системі управління – це лише необхідна умова, а достатньою умовою залишається вимога щодо збереження керованості об'єкта кібервпливу та передбачуваність його реакцій на такий вплив.

Існують й інші підходи до визначення КЗ. Кібернетичну зброю інколи визначають як інструмент кібершпигунства, який побудовано за модульним принципом.

Не можна оминути увагою єдиний у світі документ, що регламентує закони ведення кібервійни – *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, який презентовано 5 березня 2013 року в м. Талліні. Ця інструкція підготовлена міжнародною групою з 20 експертів за редакцією професора

М. Шмідта у співробітництві з НАТО, Кіберкомандуванням США та Міжнародним червоним хрестом. Встановлюючи міжнародні правила ведення кібервійни, в інструкції розроблено 95 правил. Зокрема, у 41 правилі (визначення засобів та методів ведення кібервійни) зазначається те, що КЗ – це засоби ведення кібервійни, які призначені для травмування або знищення противника, а також завдання шкоди функціонуванню його об'єктів, що дозволяє характеризувати заподіяні наслідки як факт кібернападу. У більш вузькому сенсі в Таллінській інструкції стосовно КЗ зазначено таке. Кібернетична зброя – це засоби ведення кібернетичної війни та системи, пов'язані з ними. Засоби ведення кібервійни – це КЗ та системи КЗ (техніка, інструменти, механізми, устаткування, програмне забезпечення тощо – це все те, що розроблено та використовується для здійснення кібератак. Особливий акцент у інструкції зроблено на розділенні дефініцій "комп'ютерна система", яка може кваліфікуватися як засіб ведення кібервійни, та "об'єкт з кібернетичною інфраструктурою", що може бути об'єктом кібервпливу. Особливістю цієї інструкції також є те, що вона має неофіційний характер: не прийнята жодною державою та ніким не затверджена. Але знову ж таки, врахувавши замовника та його виконавців, – висновки очевидні. Тому ця інструкція з часом відіграє значну роль при формуванні основ доктринальної політики стосовно питань кібербезпеки в більшості з розвинених держав світу.

Досить розповсюдженою на сьогодні є помилка, яка властива судженням багатьох експертів щодо розуміння сутності та змісту поняття КЗ. У першу чергу, вона пов'язана з масовим поширенням цифрових пристроїв, мікропроцесорів і програмних продуктів, що призвело до штучного звуження класу озброєнь, які потенційно можна віднести до кібернетичних. Типовою помилкою при визначенні КЗ також є переплутування таких понять, як зброя та знаряддя, оскільки грань, яка визначає належність будь-якого засобу до зброї, є досить умовною. Для КЗ така грань є ще більше нечіткою.

У 2012 році відомий спеціаліст з питань кіберзахисту Ч. Міллер з Агентства національної безпеки США представив розрахунок сил та засобів, потенційно необхідних для розробки кібернетичної операції, реалізація якої призведе до колапсу економіки в США, Європейському союзі та РФ. Так, згідно з оцінками Ч. Міллера, для підготовки такої операції потрібно витратити близько двох років. Водночас для колапсу економіки США необхідно близько 98 млн доларів та 592 спеціалісти, економіки ЄС – 112 млн доларів та 750 спеціалістів. Для РФ такі розрахунки склали 86 млн доларів та 517 спеціалістів. Зрозуміло, що цей розрахунок сил та засобів є досить умовним, але головне в ньому – це те, що на розробку, підготовку та реалізацію подібних заходів витрачається значно менше коштів, порівняно з іншими воєнними операціями.

В одній зі своїх доповідей *"Preparing for a Cyber Attack"* провідний експерт США з кібербезпеки К. Коулман зазначає, що вартість розробки зразка КЗ коливається в діапазоні від 300 дол. до 50 тис. доларів. Елементарні розрахунки з порівняння вартості двох високотехнологічних зразків зброї – високоточної (*Tomahawk*) та кібернетичної показують економічну привабливість останньої. Отже, на сьогодні чітко можна спостерігати три основні підходи до розуміння сутності та змісту КЗ: технологічний, соціальний, кібернетичний.

Перший – це технологічний підхід. Він полягає в тлумаченні КЗ як набору технічних та програмних засобів, спрямованих на використання вразливостей у

системах передачі, обробки й зберігання інформації. Другий – соціальний, що передбачає вплив на соціум через кіберпростір за допомогою приладів, пристроїв або наборів комп'ютерних команд. Тобто у першому випадку акценти розставляються на технологічній складовій, у другому – на соціальній. Третій, останній і, по суті, єдиний правильний підхід до тлумачення КЗ полягає в розумінні її як засобу впливу на кібернетичні системи різної природи.

Відомо, що третій підхід досить інтенсивно підтримується військовими аналітиками розвинених держав. Його дотримуються, в першу чергу, у військовій адміністрації США, про що зазначається в доктринальних документах щодо побудови національної стратегії кібербезпеки та підтверджується заявами американських військових очільників. Отже, можна впевнено стверджувати – американські військові де-факто визнали наявність у своїй державі арсеналів КЗ. За ними "підтягнулися" держави – партнери по НАТО, держави Близького Сходу (Ізраїль), Північна Корея, Японія, Австралія та ін. Таким чином, наведені аргументи дозволяють зробити однозначний висновок: КЗ – це новий феномен у розвитку нових видів зброї, який став реалією сьогодення. Водночас у світі вже існує ряд зразків КЗ. Найперші та найвідоміші з-поміж них це: Stuxnet, Gauss, Duqu, Wiper, Flame, miniFlame, Uroburos (Snake) тощо.

Зважаючи на зазначене вище, в рамках третього кібернетичного підходу, дамо своє визначення категорії КЗ [5]. *Кібернетична зброя – це набір технічних, програмних та інших засобів, спрямованих на порушення процесів управління в кіберпросторі, включаючи соціум, соціотехнічні системи, технічні системи (комп'ютерні системи та мережі, системи зв'язку та АСУ, управляючі елементи систем озброєння та військової техніки та небезпечних об'єктів і ОККІ, програмне забезпечення, бази даних тощо), у вигляді кібернетичних, інформаційних, психологічних та інших деструктивних впливів різноманітної природи.*

Ґрунтуючись на аналізі доступних наукових видань, присвячених проблематиці кібербезпеки, в найзагальнішому вигляді визначимо: по-перше, перелік ознак, властивих КЗ; по-друге, сформулюємо основні завдання, що покладаються на КЗ; по-третє, розкриємо перелік можливих об'єктів ураження.

До характерних ознак КЗ віднесемо: спрямованість КЗ на ураження конкретних ОККІ, а також визначених заздалегідь суб'єктів, в управлінській компетенції яких такі об'єкти знаходяться, або які мають доступ до них; КЗ застосовується приховано. У більшості випадків уражаючі фактори від застосування КЗ проявляються значно пізніше факту її застосування; КЗ застосовується як доповнення до інших форм воєнних дій і, як правило, заздалегідь до їх проведення; КЗ характерні процеси мутації в часі, що забезпечують їй зміну цілей та задач у процесі бойового застосування, що тягне за собою зміну її структури аж до повної її самоліквідації; процес розроблення, впровадження та застосування КЗ здійснюється за рахунок фінансів державного походження; громадянське суспільство, як правило, не інформується про порядок здійснення процедур кіберзахисту в разі спрацювання "ефекту бумеранга" тощо.

Основні завдання, що покладаються на КЗ, можуть полягати в такому: тимчасове ускладнення чи вибіркове призупинення шляхом відключення або блокування критично важливих вузлів ОККІ; порушення роботи та виведення з ладу АСУ різного призначення та систем зв'язку; фальсифікація, дезінформація

управлінської інформації в усіх сферах, у тому числі й критичних для національної безпеки; дезорганізація роботи кібернетичних систем тощо.

До можливих об'єктів ураження КЗ можна віднести: державні ОККІ, що задіяні в забезпеченні функціонування інфраструктури та життєзабезпечення (атомні електростанції, підприємства хімічної, нафтової, газопереробної галузей, водо-, теплопостачання, АСУ технологічними процесами на стратегічно важливих підприємствах, усі види транспортних мереж тощо); інформаційні та комунікаційні ресурси держави (ЗМІ, оператори стільникового зв'язку, провайдери Інтернет, відомчі локальні обчислювальні мережі, глобальна мережа Інтернет, децентралізовані анонімні мережі (ANts P2P, BitBlinder, Filetopia, Freenet та ін.), гібридні анонімні мережі (Psiphon, Tor, Virtual Private Network тощо), вузькоспеціалізовані анонімні мережі (Java Anonymous Proxy, Mixminion, Veiled тощо); поштова кореспонденція вищих посадових осіб держави та власне такі особи; бази даних спецслужб, силових міністерств та відомств, державних та регіональних органів влади, банківських та фінансових установ, які містять інформацію з обмеженим доступом; соціум та соціотехнічні системи; технічні системи (комп'ютерні системи та мережі; системи урядового зв'язку міліції, збройних сил; АСУ та управляючі елементи систем озброєння та військової техніки об'єктів різного призначення, програмне забезпечення тощо).

Наведені вище переліки постійно доповнюються. У широкому сенсі вони повинні охоплювати всі без винятку кібернетичні системи держави, незалежно від їх цільового призначення та форми власності. Отже, незважаючи на активізацію гонки кіберозброєнь недооцінювання небезпеки від КЗ може мати фатальні для планети наслідки – це в більш широкому сенсі, та непередбачувані наслідки для цивільної та військової критичної кібернетичної інфраструктури будь-якої держави – у більш вузькому.

Невирішеною остаточно до сьогодні залишалася проблема формалізації простору ознак, належність до яких дозволятиме здійснювати класифікацію КЗ. Так, на сьогодні відомо три класифікації КЗ: американська, яка розроблена в 2011 р. в Пентагоні та є загальноприйнятою в США для всіх силових структур, й дві класифікації, розроблені незалежно одна від одної експертами П. Пассері та П. Паганіні.

У наступній частині статті наведемо відомі класифікації, визначимемо їх переваги та недоліки, а також висвітлемо авторське бачення цієї проблеми.

Висновки

У результаті проведеного дослідження доведено, що КЗ – це новий еволюційний крок на шляху розвитку новітніх зразків зброї на нетрадиційних принципах. Показано, що така зброя має специфічні та характерні тільки їй ознаки. Встановлено, що на неї покладаються особливі завдання, які розкрито в першій частині статті, а також показано, що КЗ має власні об'єкти ураження. Крім того, спираючись на кібернетичний підхід, у результаті дослідження запропоновано власне тлумачення дефініції кібернетична зброя та закладено підґрунтя для її подальшої класифікації[1].

[1] Закінчення в наступному номері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Wilson C.* Information Operations and Cyberwar: Capabilities and Related Policy Issues. CRS Report for Congress / C. Wilson [Electronic resource]. – Mode of access : http://www.fas.org/irp/crs/RL31787.pdf.

2. *Паршин С. А.* Кибервойны – реальная угроза национальной безопасности / С А. Паршин, Ю.Е. Горабчев, Ю.А. Кожанов – М. : КРАС АНД, 2011. – 96 с.

3. Боротьба в кіберпросторі: підходи американських військових [Електронний ресурс]. – Режим доступу : http://ia-prometei.org.ua/technologies/borotba-v-kiberprostori-pidhody-amerykanskyh-vijskovyh.

4. *Даник Ю.Г.* Основні аспекти парадигми кібернетичної безпеки / Ю.Г. Даник [Електронний ресурс]. – Режим доступу: http://jrnl.nau.edu.ua/index.php/IMV/article/view/3171.

5. *Грищук Р.В.* Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 634 с.

6. *Kaiser R.* The birth of cyberwar / *R. Kaiser* // Political Geography. – 2015. № 43. – P. 11–20.

7. The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict [Electronic resource]. – Available from : http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf.

8. *Geers K.* Cyber War in Perspective : Russian Aggression against Ukraine / K. Geers. – Tallinn : CCDCOE, 2015. – 176 p.

9. *Thomas R.* Cyber-Weapons / R. Thomas, P. MCBurney // The RUSI Journal. – Vol. 157. – Iss. 1. – 2012. – P. 1–13.

10. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та ін.; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

11. *Тропина Т.Л.* Киберпреступность и кибертерроризм: поговорим о понятийном аппарате / Т.Л. Тропина // Сб. научн. тр. междунар. конф. “ИТ и безопасность”. Вып. 3. – К. : НАН України. – 2003. – С. 173–181.

12. *Шеломенцев В.П.* Поняття та сутність кібернетичної атаки / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2011. – № 2–3 (25–26). – С. 337–344.

13. *Мельник С.В.* До проблеми формування понятійно-термінологічного апарату кібербезпеки / СВ. Мельник, ОО. Тихомиров, О.С Лєнков // Зб. наук. пр. ВІКНУ ім. Т. Шевченка. – К. : ВІКНУ, 2011. – №30. – С. 165–171.

14. *Milevski L.* Stuxnet and Strategy: A Special Operation in Cyberspace? [Electronic resource] / L. Milevski. – Available from : http://www.academia.edu/872101/Stuxnet_and_Strategy_A_Special_Operation_in_Cyberspace.

15. *Каберник В. В.* Проблемы классификации кибероружия / В. В. Каберник // Вестн. МГИМО. – 2013. – № 2 (29) – С. 72–73.

16. *Даник Ю.Г.* Військові аспекти класифікації високотехнологічних систем / Ю.Г. Даник, Д.А. Іщенко, О.В. Манько // Збірник наукових праць ЖВІ НАУ. – Житомир : ЖВІ НАУ. – 2013. – № 8. – С. 5–13.

17. *Новак Я.В.* Сучасний стан та перспективи розвитку криміналістичного дослідження вогнепальної зброї : дис... канд. юрид. наук: 12.00.09 / *Я.В. Новак* ; Київський національний ун-т внутрішніх справ. – К., 2007. – 201 с.

Отримано 15.06.2016
Рецензент Рибальський О.В., д.т.н.