УДК 007.51:004.491

В.О. Хорошко,
доктор технічних наук, професор,
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 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 статье представлено новую классификацию 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, киберразведка, киберзащита.*

In the paper it is suggested a new classification of cyber weapon without drawbacks of previous classifications. Main characteristics relevant to cyber weapon are revealed and the main tasks designated to it by the owners are defined.

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. У статті аргументовано доведено та показано те, що кібернетична зброя (далі – КЗб) на сьогодні є одним з найновіших й найдієвіших зразків сучасної зброї [1]. Крім того, в попередніх дослідженнях розкрито етимологію поняття зброя та показано сучасні підходи до її трансформації в кібернетичну. Тому, незважаючи на те, що на сьогодні вже встановлено сутність та зміст КЗб, невирішеною остаточно залишається проблема формалізації простору ознак, належність від яких дозволятиме здійснювати класифікацію кібернетичної зброї.

Аналіз останніх досліджень і публікацій показав, що на сьогодні відомо три основні класифікації КЗб: американська, яка розроблена в 2011 році в Пентагоні та є загальноприйнятою в США для всіх силових структур, та дві класифікації, розроблені незалежно одна від одної експертами П. Пассері та П. Паганіні. Є й інші підходи до класифікації, зокрема В. Каберника [1; 2; 3; 4].

Так, відомості щодо класифікації КЗб в США мають гриф обмеження доступу. Друга класифікація наведена у квітні 2012 року в статті *"What is a Cyber Weapon?"* П. Пассері. Класифікація П. Пассері показує, що КЗб класифікується за чотирма параметрами: точність (націлювання на досягнення конкретної мети та зменшення при цьому побічних збитків); рівень проникнення; скритність; ресурсоємність. Як видно з приведеної класифікації, автор для спрощення її сприйняття застосував метод аналогій. Така класифікація очевидно є неповною.

Альтернативний варіант класифікації КЗб запропоновано П. Паганіні у квітні 2012 року в статті *"Cyber Weapons"*. В основу класифікації покладено спектр її дії. Так, за спектром дії КЗб буває низького, середнього та високого потенціалу. До КЗб низького потенціалу належить зброя, яка є шкідливою, але такою, що не спроможна проникати до конкретної цілі та завдавати їй прямої шкоди. До КЗб середнього потенціалу належить зброя, що може проникати на об'єкт кібернетичного впливу, але не спроможна досягати конкретної мети. При цьому вона за будь-яких умов завдає збитків інфраструктурі та противнику. Кібернетична зброя високого потенціалу здатна до проникнення на об'єкт, долаючи систему захисту, та водночас спроможна завдати катастрофічних збитків. Приведена класифікація також є досить умовною як і попередня, що значно обмежує її застосування на практиці.

У статті В. Каберника теж запропоновано класифікацію КЗб, яка, на нашу думку, є найбільш повною, але відсутність у її описі ознак комплексності суттєво звужує всебічний опис характеристик такої зброї [4; 1].

Метою статті є розроблення принципово нової класифікації кібернетичної зброї, яка позбавлена від недоліків відомих класифікацій та, на відміну від них, спроможна описувати характеристики будь-якого зразка кібернетичної зброї незалежно від його спектра дії.

Викладення основного матеріалу дослідження. Для досягнення поставленої в статті мети було розглянуто та досліджено базові підходи до побудови класифікацій, які ґрунтовно розкрито в [1]. Об'єм статті не дозволяє більш ґрунтовно розглянути зазначене вище питання, а тому далі пропонуємо зупинитися суто на предметі цього дослідження.

Під класифікацією КБз будемо розуміти розподілення усіх можливих її видів на взаємопов'язані класи, визначені на підставі найбільш суттєвих та важливих у практичному відношенні ознак [1].

Зважаючи на прийняте визначення, класифікація видів КЗб за умови вибору правильних суттєвих ознаках класифікації має забезпечити вирішення таких основних завдань: розкрити основні зв'язки між видами КЗб; допомогти практикам орієнтуватися в найскладніших ситуаціях, правильно класифікувати нові зразки, типи і види КЗб, що будуть виникати в майбутньому; стати основою для формування правильних узагальнюючих висновків та прогнозів як виникнення і розвитку нових видів КЗб, так і відповідних способів ведення збройної боротьби; стати основою для обґрунтування нової та вдосконалення існуючих технологій у галузі нових видів зброї; забезпечити швидкий пошук інформації про види КЗб в сучасних інформаційно-пошукових системах. Крім того, класифікація видів КЗб має забезпечувати ефективну цілеспрямовану роботу з подальшого дослідження впливу вражаючих факторів того чи іншого виду зброї на об'єкти ураження, оскільки більшість наявної в доступній літературі інформації щодо впливу новітніх видів

зброї на ті чи інші об'єкти має уривчастий і, як правило, лише описовий характер. Використання такої інформації є неефективним. На підтвердження цьому можна привести такі аргументи.

По-перше, уражаючі фактори зброї не завжди чітко визначені і класифіковані за ефективністю впливу на об'єкти. По-друге, не зазначаються умови проведення й основні обмеження при проведенні досліджень щодо впливу вражаючих факторів новітніх видів зброї на ті чи інші об'єкти, а якщо і наводяться, то вони, як правило, різні. Різняться також методології і критерії обґрунтування мінімально ефективних рівнів їх впливу. Унаслідок цього вже одержані окремі практичні результати впливу новітніх видів зброї на ті чи інші об'єкти, але їх неможливо звести до однотипних умов та обмежень, а тому і неможливо провести їх порівняльний аналіз і зробити правильні наукові й практичні висновки та прогнози. По-третє, не вирішено остаточно питання оцінювання значимості тих чи інших уражаючих факторів при їхньому впливі на організм людини, військову техніку, навколишнє середовище. Отже, наявність приведених вище аргументів суттєво стримує роботу дослідників, а одержувані окремі висновки і прогнози не завжди адекватно відображають справжній стан справ. Саме тому ще й досі не створено узагальненої, універсальної класифікації КЗб. Розглянемо хоча б загалом, якою повинна бути така класифікація на сучасному рівні розвитку наукових знань.

На основі проведеного аналізу відомих класифікацій пропонується узагальнена класифікація, яка може бути використана для опису широкого спектру зразків КБз. З урахуванням того, що КБз досить різноманітна, то основним принципом, який можна покласти в основу класифікації є ознаковий. Вперше такий підхід було реалізовано для класифікації кібератак у [5].

Пропонується класифікувати КБз за такими базовими ознаками: призначення, масштабність застосування; характер вражаючої дії; спосіб доставки; керованість; деструктивний вплив; оперативність; місце базування; рівень маскування; спосіб виготовлення; спектр дії; об'єкти ураження; рівень впливу на об'єкти ураження; прицільні властивості; інтегральний ефект; тип зв'язків та рівень взаємодії; наслідки; принцип генерування; самоорганізація; тривалість ефекту; латентність. Класифікаційний граф КБз наведено у вигляді рисунку в [1].

За призначенням КБз поділяється на: розвідувальну; захисну; зброю кібернетичного впливу. Розвідувальна зброя призначена для добування інформації з кіберпростору або в кіберпросторі шляхом моніторингу кібернетичних систем та процесів, які в них протікають під час функціонування. Кібернетична зброя захисту призначена для забезпечення та підтримання заданого рівня кібербезпеки. Зброя, що призначена для здійснення кібернетичного впливу на елементи кіберпростору противника з метою порушення процесів управління в кібернетичних системах, називаються зброєю кібернетичного впливу.

За масштабами застосування КБз може бути: глобальна, стратегічна, тактична. Застосування КБз несе глобальний характер, коли масштаб від її застосування потенційно може поширюватися на всі держави, в яких функціонують об'єкти з критичною кібернетичною інфраструктурою. Стратегічний масштаб застосування КБз поширюється на міждержавний (регіональний) рівень. Тактична КБз за масштабом застосування орієнтована переважно на застосування на національному рівні.

За характером уражаючої дії КБз поділяється на: зброю масового ураження, зброю функціонального ураження, функціонального придушення, функціонального

виведення з ладу. Кібернетична зброя масового ураження має такий характер вражаючої дії, який співвимірний з наслідками, що виникають унаслідок застосування зброї масового ураження (ядерної, хімічно, біологічної). Застосування КБз функціонального ураження призводить до ураження окремих функцій, що виконуються об'єктом, внаслідок чого він втрачає здатність до виконання цільової задачі. Кібернетична зброя функціонального придушення передбачає функціональне придушення, що призводить до комплексної дії на об'єкт з критичною кібернетичною інфраструктурою внаслідок чого він втрачає здатність до виконання цільової задачі протягом заданого інтервалу часу. Результатом функціонального виведення з ладу є генерація необоротних процесів, що призводять до виведення з ладу об'єктів впливу.

За способом доставки КБз поділяється на таку, що може доставлятися: природними носіями або штучними носіями. Природним носієм доставки КБз є людина. Наприклад, інсайдер. Штучними носіями є всі інші засоби, що не є об'єктами біологічного походження.

За керованістю КБз поділяється на: керовану і некеровану. Керована КБз передбачає постійне або періодичне управління процесом її бойового застосування. Некерована КБз – це зброя яка не потребує зовнішнього втручання в процесі її цільового застосування.

За деструктивним впливом КБз може бути: безпечна, небезпечна. Ця класифікаційна ознака є специфічною. Вона властива тільки КБз, оскільки "зброя" в принципі не буває "безпечною" або "небезпечною". До безпечної, з точки зору руйнівних властивостей, можна віднести зброю, яка не призводить до фізичних руйнувань інфраструктури об'єкта, а порушує властивості безпеки інформації на ньому. Наприклад, розвідувальна КБз призводить до порушення конфіденційності інформації на об'єкті, що розвідується, але жодним чином не руйнує його інфраструктуру. Небезпечна – зброя, деструктивний вплив від якої має прояви як для інфраструктури об'єкта, так і для безпеки інформації, яка на ньому циркулює.

За оперативністю КБз може бути: миттєвої дії; повільної дії з накопиченням; тимчасової дії; довгострокової дії. Миттєва дія КБз співвимірна з масштабом часу, протягом якого вона проявляє деструктивний вплив на об'єкт або суб'єкт впливу. Кібернетична зброя повільної дії з накопиченням – це зразок зброї, корисний ефект від застосування якої поступово накопичується і при досягненні заданого рівня насичення проявляє свої деструктивні властивості. За оперативністю КБз тимчасової дії орієнтована на виконання своїх деструктивних функцій протягом деякого відносно нетривалого інтервалу часу. Довгострокова дія КБз характеризується відносно тривалим інтервалом часу, протягом якого вона використовується за призначенням.

За місцем базування КБз буває: космічного базування, повітряного базування, наземного базування, морського базування, підземного базування, змішаного базування. Місце базування КБз визначається, виходячи, в першу чергу, із того кола задач, які на неї покладаються. Переважно КБз має змішане базування.

За рівнем маскування КБз може бути: замаскованою; незамаскованою. Замаскована КБз передбачає застосування елементів маскування. Незамаскована – навпаки, такі елементи не використовує.

За способом виготовлення КБз поділяється на: кустарну, промислову, змішану. Кустарне виробництво передбачає виготовлення зразка несерійного характеру, як

правило, особою або групою осіб та не передбачає залучення державного фінансування. Кібернетична зброя промислового виготовлення – це зброя, яка виготовляється, зазвичай, на замовлення держави або групи держав із залученням її промислових потужностей. Кібернетична зброя за змішаним способом виготовлення поєднує в собі елементи кустарного та промислового виробництва. *За спектром дії* КБз можна поділяти на зброю: низького потенціалу; середнього потенціалу; високого потенціалу. Кібернетична зброя низького потенціалу призводить до деструктивного впливу, що не чинить об'єкту впливу безпосередньої шкоди. Прикладом такої зброї є спеціалізоване програмне забезпечення для генерації потужного потоку трафіку з метою тимчасового перевантаження ресурсів системи, що призводить до заподіяння тимчасової шкоди об'єкту впливу без нанесення йому будь-яких фізичних пошкоджень. Кібернетична зброя середнього потенціалу – це зброя, застосування якої призводить до функціонального ураження або придушення, але не до функціонального виведення з ладу об'єкта впливу. Кібернетична зброя високого потенціалу – це зброя, що здатна досягати об'єкта впливу шляхом обходу його систем захисту й здатна до його функціонального виведення з ладу.

Цілями ураження КБз можуть бути: об'єкти з критичною кібернетичною інфраструктурою; суб'єкти управління. Об'єкти з критичною кібернетичною інфраструктурою – це матеріальні чи віртуальні об'єкти й системи, порушення або припинення функціонування яких призводить до втрати управління, руйнування інфраструктури, незворотних негативних змін або руйнувань економіки країни, суб'єкта або адміністративно-територіальної одиниці, або до впливу на безпеку населення, яке мешкає на цих територіях. Суб'єкт управління як ціль ураження – це особа, група людей або організація, що приймає управлінські рішення та керує об'єктами з критичною кібернетичною інфраструктурою шляхом впливу на них.

За рівнем впливу на об'єкти ураження: об'єкти, що підлягають відновленню; об'єкти, що не підлягають відновленню. Вплив КБз на об'єкти ураження може мати дуальний характер: об'єкти можуть підлягати відновленню за деякий часовий термін або ж такому відновленню не підлягають.

За рівнем впливу на суб'єкти ураження КБз може бути: смертельної дії; несмертельної дії; настроювальної дії. Кібернетична зброя смертельної дії передбачає завдання смертельних збитків протиборчій стороні в живій силі. Кібернетична зброя несмертельної дії не призводить до загибелі живої сили протиборчої сторони. Кібернетична зброя з настроювальною дією – це зброя, властивості якої щодо впливу на живу силу протиборчої сторони налаштовуються у процесі її застосування шляхом виставлення порогу кібернетичного впливу.

За прицільними властивостями КБз буває двох видів: високоточною та неприцільною. Високоточна КБз призначена для нанесення високоточних ударів по визначеним цілям кібернетичного впливу. Неприцільна – це зброя, яка не володіє прицільними властивостями щодо конкретних цілей.

За типом зв'язків та рівнем взаємодії: поодинока; групова. Кібернетична зброя, що належить до класу поодинокої, передбачає застосування її без залучення додаткових допоміжних модулів. До групової відносять КБз, яка для досягнення своєї мети використовує додаткові модулі, що у своїй сукупності дозволяють досягнути поставленої перед нею цілі.

Кібернетична зброя *за наслідками* поділяється на: глобальну, регіональну, локальну. Застосування КБз несе глобальний характер, коли масштаб від її застосування потенційно може призвести до загибелі людської цивілізації. Стратегічний масштаб застосування кібернетичної зброї означає її здатність до зміни ролі й призначення кібернетичних систем на міждержавному (регіональному) рівні. Тактична КБз за масштабом застосування призначена для вирішення задач тактичного рівня у визначеному регіоні.

За генеруванням КБз може бути: самогенеруюча; з часовим механізмом; за настанням визначеної події. Самогенеруюча КБз – це зброя, яка не потребує зовнішнього втручання для приведення її в готовність до виконання задач. Генерування за часовим механізмом передбачає приведення в готовність зброї у визначений момент часу. Настання визначеної події інколи також виступає підставою для виконання КБз своїх функцій.

За рівнем інтегрального ефекту КБз поділяється на: зброю часткового ефекту, зброю з повним ефектом. Інтегральний ефект від застосування КБз має дві форми прояву: часткову, коли ефект має лише локальні частинні наслідки, та повну форму прояву, коли ефект носить глобальний характер.

За самоорганізацією КБз буває: самоорганізованою; за окремою командою. Самоорганізованість КБз – це процес упорядкування елементів одного рівня в системі за рахунок внутрішніх закладених функцій, без зовнішнього специфічного впливу. Самоорганізація КБз за окремою командою передбачає реалізацію визначеного вище процесу при надходженні відповідного зовнішнього специфічного впливу – команди.

За часом тривалості ефекту КБз буває: миттєвого ефекту, відкладеного ефекту. Миттєвий ефект від застосування КБз проявляється в масштабі часу, співвимірному з часом її цільового застосування. Якщо ефект від застосування КБз проявляється дещо пізніше від моменту початку її застосування за цільовим призначенням, то така зброя є зброєю з відкладеним ефектом.

За латентністю КБз буває: негайного прояву, відкладеного прояву. Кібернетична зброя, яка проявляє себе належним чином у процесі застосування, є зброєю негайного прояву. У протилежному випадку, коли латентний період є досить тривалим, – КБз може бути кібернетичною зброю з відкладеним проявом.

Перевагою запропонованої класифікації, порівняно з відомими є те, що КБз, яка класифікується за ознаковим принципом, може в кожному конкретному випадку при визначенні загального класу містити не тільки одну, але й більше компонент будь-якої з ознак. Крім того, покладений в основу класифікації ознаковий принцип забезпечує розширення множини ознак, за якими можна здійснювати класифікацію.

Покажемо приклад застосування розробленої класифікації на практиці. Такий зразок КБз, як *Stuxnet* може бути класифікований таким чином. *Stuxnet* – це КБз, яка призначена для здійснення керованого небезпечного кібервпливу стратегічного характеру, спрямованого на функціональне виведення з ладу об'єктів з критичною кібернетичною інфраструктурою. Зразок має довгострокову дію. Характеризується наземним базуванням та доставляється природним носієм. Рівень маскування характеризує його як невидимий зразок промислового походження, спрямований для нанесення кібервпливу з метою невідновлення об'єктів впливу. *Stuxnet* є високоточним зразком з повним рівнем інтегрального ефекту групового

характеру, що має глобальні наслідки й самогенерується. Зброя є самоорганізованою з відкладеним часом тривалості ефекту й відкладеним проявом.

Висновки. Запропонована класифікація на відміну від відомих забезпечує формалізацію вимог до новостворюваних зразків КБз. Вона не претендує на закінченість, не є остаточною, а тому буде доповнюватися, уточнюватися і розвиватися в майбутньому з вдосконаленням цієї зброї і способів її застосування. Водночас така класифікація дає можливість більш чітко уявити особливості механізму дії КБз на всі можливі об'єкти ураження, спрогнозувати тенденції її розвитку, а також передбачити заходи щодо захисту від факторів її ураження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Г*рищук Р.В.* Основи кібернетичної безпеки : монографія / Р.В. Грищук, Ю.Г. Даник ; за заг. ред. проф. Ю.Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. *Passeri P.* What is a Cyber Weapon? / P. Passeri. [Electronic resource]. - Access mode : http://www.hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/#comments.

3. *Paganini P.* Cyber Weapons. / *P. Paganini*. [Electronic resource]. - Access mode : http:// securityaffairs.co/wordpress/3896/intelligence/cyber-weapons.html.

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

5. *Корченко О.Г.* Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк та ін. // Вісник Східноукраїнського національного університету імені Володимира Даля – № 4 (146) – Ч. 1, 2010. – С. 184–193.

Отримано 01.11.2016
Рецензент Рибальський О.В., д.т.н