Зміст

Розділ 3. МАТЕМАТИЧНА МОДЕЛЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ В УМОВАХ КІБЕРБОРОТЬБИ, ТЕОРЕТИЧНІ ПОЛОЖЕННЯ ЩОДО РОЗВИТКУ СПРОМОЖНОСТЕЙ З ВЕДЕННЯ ПРОТИБОРСТВА У КІБЕРПРОСТОРІ ТА ТЕРМІНОСИСТЕМИ

Перелік умовних позначень

APT – Advanced persistent threat.
SCADA – Supervisory Control And Data Acquisition.
ГРУ ГШ ЗС рф – Головне розвідувальне управління Генерального штабу Збройних Сил російської федерації.
ДЦКЗ ДССЗЗІ України – Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.
ЗС України – Збройні Сили України.
ІКС – інформаційно-комунікаційна система.
МО України – Міністерство оборони України.
ОВТ – Озброєння та військова техніка.
ОВУ – Орган військового управління.
ОП – оборонне планування.
ПЗ – програмне забезпечення.
рф – російська федерація.
СОБ України – Стратегічний оборонний бюлетень України.
ФСБ рф – Федеральна служба безпеки російської федерації.
ШПЗ – Шкідливе програмне забезпечення.

ВСТУП

Сьогодні кіберпростір є одним з театрів (сфер, вимірів, доменів) воєнних дій, офіційного визнання чому надав саміт держав-членів Північноатлантичного альянсу у Варшаві 2016 року. У світі з кожним роком все дужче набирає сили тенденція зі створення державами власних кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної та кібер інфраструктури, а й постійна кіберрозвідка противника на стратегічному та/або оперативному рівнях, здійснення деструктивних кібервпливів на нього як під час наступальних, так і оборонних кібероперацій, що у комплексі, принаймні у першому наближенні, дає уявлення про сутність сучасної кіберборотьби.

Україна підтверджує оборонний мандат на кіберпростір, у якому має ефективно захищати свої інтереси як під час воєнного періоду у теперішній і майбутніх війнах, так і у формально мирний час, враховуючи притаманну воєнним конфліктам сьогодення особливість тривалого підготовчого етапу, котрий має на меті створення сприятливих умов для подальшої активної фази (ураження високоточною зброєю, наземна операція та ін.) шляхом розвідувальної і підривної діяльності, зокрема і у кіберпросторі. Передовий досвід та уроки міждержавних протистоянь останнього десятиліття демонструють підвищення інтенсивності ведення кіберборотьби за геометричною прогресією, урізноманітнюються методи її суб'єктів, розширюється спектр об'єктів кібервпливу, а загалом кіберпростір та операції в ньому набувають ознак асинхронності. Справжнім викликом обороноздатності держави в контексті здобуття та утримання переваги над противником у кіберпросторі є різка необхідність постійного удосконалення форм і способів застосування сил та засобів кіберборотьби, котрі прямопропорційно залежать від рівня розвитку новітніх інформаційних технологій, а також інновацій у науці й техніці.

Актуальність дослідження за тематикою монографії підтверджується положеннями низки цільових програмних документів державного рівня, а саме:

Стратегією воєнної безпеки України одними із завдань щодо досягнення пріоритетних цілей державної політики у воєнній

сфері та сфері оборони визначено: “розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохоплюючої оборони України”, а також “підвищення рівня боєздатності Збройних Сил України з досягненням і підтриманням визначених спроможностей щодо відбиття агресії в кіберпросторі (ведення кібероборони)”;

у Стратегічному оборонному бюлетені України сформульовано перелік спроможностей з ведення протиборства в кіберпросторі, серед яких: “створення системи кібероборони для ведення протиборства в кіберпросторі”, а також “здатність організовувати підготовку та проводити кібердії (кібервпливи, кібератаки) із застосуванням апаратно-програмних комплексів кібербезпеки, засобів з кіберзахисту та усіх видів кіберзброї для вирішення завдань кіберборотьби”;

Стратегією кібербезпеки України визнано “недостатніми організацію і проведення наукових досліджень у сфері кібербезпеки”.

Галузь порушеного наукового питання є новітньою, але з огляду на свою актуальність та інноваційність, досліджується досить активно. Аналіз релевантного наукового доробку за означеним напрямом доводить те, що більшість методологів і теоретиків у сфері кібербезпеки сходяться на визнанні трьох базисних складових системи кіберборотьби, а саме підсистем кіберзахисту, кіберрозвідки та кібервпливу.

Проте дослідженню проблем підготовки (планування) та ведення кіберборотьби, з точки зору розгляду її як процесу виконання збройними силами та іншими складовими сил оборони військових заходів з кібероборони, приділено значно менше уваги. Воєнні конфлікти сучасності реалізують принципи гібридної та мережецентричної війни, а притаманна їм кіберборотьба, стає дедалі більш поширеним явищем через побудову високотехнологічного суспільства, його інформатизації та цифровізації. Наразі в науці відсутня обґрунтована система показників та критеріїв оцінювання ефективності ведення кіберборотьби, а дослідження у цьому напрямі висвітлюють лише часткові показники продуктивності (результативності) окремих її складових – кіберзахисту, кіберрозвідки та кібервпливу. Математичне моделювання кіберборотьби, як досить новітнього та інноваційного напряму діяльності Збройних Сил України (далі – ЗС України), є беззаперечно важливим та таким, що дасть змогу всебічно досліджувати

питання стосовно оцінювання ефективності її ведення, якому наразі не надається достатньої уваги.

Окрім цього, на ефективність ведення кіберборотьби в інтересах застосування збройних сил впливає низка зовнішніх та внутрішніх факторів, які не дають змоги повною мірою реалізовувати наявний потенціал спроможностей з ведення протиборства у кіберпросторі. Враховуючи це, актуальним науковим завданням є дослідження факторів (умов та чинників), які впливають на ефективність ведення кіберборотьби в інтересах застосування збройних сил. Термінологічному апарату в сфері кіберборотьби притаманна низка системних невідповідностей, які не дають змогу однозначно трактувати, описувати та класифікувати дії у кіберпросторі, а як наслідок і оцінювати їх ефективність.

Необхідність формування Кіберсил у системі Міністерства оборони України як окремого роду сил, до компетенції якого має увійти підготовка й ведення кібероборони держави додатково підкреслює важливість вирішення згаданих наукових проблем та завдань.

Розділ 1

КІБЕРБОРОТЬБА У ВОЄННИХ КОНФЛІКТАХ СУЧАСНОСТІ: ПЕРЕДОВИЙ ДОСВІД, ТЕНДЕНЦІЇ ТА ЗАКОНОМІРНОСТІ РОЗВИТКУ

1.1. Кіберборотьба як об'єкт дослідження сучасної воєнної науки

Воєнні конфлікти сучасності реалізують принципи гібридної та мережецентричної війни, а притаманна їм кіберборотьба, стає дедалі більш поширеним явищем через побудову високотехнологічного суспільства, його інформатизації та цифровізації [1]. Як наслідок, спектр об'єктів, що піддаються кібервпливу постійно розширюється, а форми та способи його нанесення – удосконалюються та урізноманітнюються [2].

«Сьогодні буває складно визначити межу, за якою починається і закінчується власне війна» [3]. Таким війнам характерний тривалий підготовчий етап, під час якого забезпечується вразливість держави-об'єкта до нападу на неї. Зокрема, поширеним явищем є комплексне ведення кіберборотьби або окремих її складових елементів (кіберрозвідки, кіберзахисту, кібервпливу) до початку активної фази конфлікту, лише у дещо більш скритній манері аніж безпосередньо під час неї. Інтенсивність нанесення кібератак суттєво зростає напередодні активних конвенційних воєнних (бойових) дій, та досягає свого максимуму з їх початком, в цей період здійснюється вплив на заздалегідь виявлені вразливості у кіберінфраструктурі. Подібний сценарій відбувся з Грузією у 2008 році та з Україною на початку широкомасштабного вторгнення російської федерації (рф) – у 2022 році, за даними ДЦКЗ ДССЗЗІ України було ідентифіковано у 18,3 разів більше

кіберінцидентів категорії «Шкідливий програмний код» порівняно з аналогічним часовим проміжком 2021 року [4]. А враховуючи те, що гібридні війни не оголошуються та, відповідно, не завершуються в класичний спосіб, кіберборотьба триває і після основного загострення подій, коли конфлікт стає тліючим. Така природа сучасних воєнних конфліктів зумовлює дослідження кіберборотьби як процесу постійного виконання заходів із кібероборони держави, а досвіду її ведення – як сукупності різнорідних за метою, завданнями, а також формами та способами імплементації, фактів проведення державами або підконтрольними їм організаціями заходів з кіберзахисту, кіберрозвідки та кібервпливу – основних складових кіберборотьби [5; 6].

На сучасному етапі процесам планування та ведення кіберборотьби все ще притаманна певна невизначеність. Проте, об'єктивна дійсність свідчить про постання кібердомену як сегменту кіберпростору і середовища ведення воєнних дій. У збройних силах провідних країн світу створюються військові формування безпосередньо призначені для ведення операцій (воєнних дій) у цьому середовищі [7]. Водночас, проведений науковий пошук хоч і показав наявність теоретично виведених часткових показників ефективності деяких складових кіберборотьби, наприклад, система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки та модель оцінювання рівня збитків від кібератак, втім системність їм не властива, а тому комплексне оцінювання ефективності воєнних дій у кіберпросторі наразі не є можливим. Термінологічний апарат у сфері кіберборотьби не має однозначності, що призводить до підміни понять як у наукових дослідженнях, так і у військових стандартах та доктринах. Зокрема, на сьогодні не існує чіткої дефініції терміну «кібердомен», а його межі у кіберпросторі не окреслені [8; 9; 10].

Інтерес до вивчення кіберборотьби зростає прямо пропорційно з підвищенням інтенсивності її ведення у воєнних конфліктах сучасності. Більшою мірою, актуальні публікації за темою висвітлюють результати дослідження однієї або декількох окремих кібератак (кіберінцидентів), досвіду кіберборотьби під час певного воєнного конфлікту, кібероперацій та спроможностей у кібердомені однієї з держав, або ж технічних характеристик і можливостей деякого програмного (програмно-апаратного) засобу призначеного для ведення

кіберборотьби. Наприклад, детальний аналіз причин, перебігу та наслідків серії кібератак на інформаційну інфраструктуру Естонії у 2007 році надано в [11]. Автор праці також узагальнив ключові фактори, завдяки яким було досягнуто такого значного на той час ефекту, основним серед яких був високий рівень дигіталізації суспільства без належної кіберзахищеності. Колектив науковців із Федеральної вищої технічної школи Цюриха продемонстрував результати дослідження характеристик, особливостей, способу «доставки», кількісних показників деструктивного впливу та часу, який пішов на відновлення інфраструктури іранського заводу ядерної промисловості від атаки комп'ютерного хробака Stuxnet у однойменній статті [12]. Результати дослідження [13], де розглянуто перебіг та особливості російсько-українського інформаційної і кіберборотьби, засвідчили, що Україна досить вдало проводить кіберзахист своєї інфраструктури, маючи суперником такі кіберзлочинні групи типу розвиненої сталої загрози APT, як Sandworm та FancyBear. Більш ніж ймовірно, ці групи діють під егідою ГРУ ГШ ЗС рф. Корисними є дослідження прикладного спрямування державних установ та агентств призначених для кіберзахисту та реагування на загрози кібербезпеці, а також приватних кібербезпекових компаній. Так, наприклад, дослідження Агентства національної безпеки США [14] висвітлює технічні характеристики, архітектуру побудови та особливості процесу «зараження» комп'ютерних пристроїв ШПЗ Drovorub, яке, за даними агентства, розроблено зазначеним вище APT FancyBear.

Викладене вище свідчить про те, що сьогодні відкриті джерела переповнені інформацією про окремі події у кіберпросторі (кіберінциденти), різноманітність подання якої прямо залежить від її обсягу. Тоді як питання дослідження передового досвіду ведення кіберборотьби, яке дало б змогу розкрити існуючі тенденції та визначити закономірності її подальшого розвитку, залишається невирішеним.

Кіберборотьба – феномен XXI століття. Від звичайних кібератак, які беруть свій початок зі становлення комп'ютингу і, здебільшого, спрямовані на досягнення приватних цілей, її відрізняє обов'язкова приналежність до держави та стратегічний (оперативно-стратегічний) характер наслідків. Кіберборотьба може вестися регулярними силами та засобами (кібервійськами), неурядовими організаціями за державного спонсорування під військовим керівництвом (state-sponsored cyberattack), або, як найчастіше

відбувається в країнах, що займаються кібертероризмом – кібервійськами під виглядом неурядових організацій із повним запереченням причетності до подій держави-агресора, що надає конфлікту ще більшої гібридності та унеможливлює притягнення суб'єкта до відповідальності за міжнародним гуманітарним правом. Сьогодні ДЦКЗ ДССЗЗІ України, на основі рекомендацій Європейської агенції з кібербезпеки та Європейського центру боротьби з кіберзлочинністю Європейської поліції, розроблено та введено в дію класифікацію категорій кіберінцидентів – результатів кіберборотьби, форми та способи ведення якої у воєнних конфліктах сучасності еволюціонували (розвивалися) у декілька періодів, що зумовлені геополітичною ситуацією у світі та рівнем розвитку інформаційно-комунікаційних технологій.

Отже, постає питання невідповідності теорії практиці, створити підґрунтя для вирішення якого можливо шляхом вивчення (аналізу, узагальнення, систематизації) передового досвіду ведення кіберборотьби у воєнних конфліктах сучасності, розкриття існуючих тенденцій та визначення закономірностей її подальшого розвитку. Адже уроки, винесені з передового досвіду, потенційно можуть містити в собі ключі до розуміння як у подальшому вести воєнні дії у кіберпросторі (оперувати в кібердомені) та запобігати загрозам кібербезпеці держави.

1.2. Аналіз та узагальнення передового досвіду ведення кіберборотьби під час першого періоду воєнних у кіберпросторі (2005–2010 рр.)

Перший період є початковим для тієї кіберборотьби, якою її прийнято розглядати сьогодні, він асоціюється з такими воєнними діями у кіберпросторі, як [11; 15–16]:

Titan Rain – кіберрозвідка за державною інформаційною інфраструктурою США та Великої Британії, яку вважають спонсорованою або реалізованою Китаєм. У результаті операції зловмисники, скориставшись вразливістю нульового дня (zero-day exploit), отримали доступ до службової інформації зі сховищ даних таких відомств як: Міністерств оборони та закордонних справ США та Великої Британії, Міністерства енергетики США, NASA

та ін. Ця діяльність була викрита у 2005 році. Є підстави вважати, що кібершпіонаж приховано здійснювався з 2003 року. Titan Rain є першою відомою, але далеко не останньою операцією такого типу, в якій підозрюють Китай та підрозділ його Народно-визвольної армії Unit 61398;

кібервплив на інформаційну інфраструктуру Естонії шляхом нанесення серії кібератак у квітні-травні 2007 року. Спричинена суперечностями між етнічними естонцями та російськомовною (проросійсько налаштованою) діаспорою соціальна нестабільність в той момент досягла свого максимуму. Тогочасна інформаційна інфраструктура Естонії, що швидко розвивалася у напрямі «безпаперового» урядування, ще не мала достатнього рівня кіберзахисту. Скориставшись цим, зловмисники нанесли низку розподілених кібератак на відмову в обслуговуванні (DDoS-атаки) у період з 27 квітня до 18 травня. Отримуючи по 2000 запитів на секунду замість звичайних тисячі в день, офіційні веб-ресурси більшості міністерств держави, двох найбільших банків (протягом декількох днів транзакції були неможливими), декількох політичних партій правого спрямування та урядовий поштовий сервер вийшли з ладу. Незважаючи на заяви офіційних осіб держави щодо причетності до кібератак рф, невдовзі уряд Естонії був змушений визнати, що доказів, які б це підтверджували у ході розслідування виявлено не було. Тому, за офіційною версією відповідальними за заподіяну шкоду є група кіберзлочинців, які використовували ботнети – взламані персональні комп'ютери. Фізично ботнети розташовувалися у таких країнах як Єгипет, рф та США. Відповідно діапазон їх мережевих IP-адрес не був логічно зв'язаним, що значною мірою вплинуло на успішність атаки. Причиною тому, чим естонський досвід є таким важливим та визначним для подальшого розвитку подій є те, що реакцією на зазначені DDoS-атаки стало створення Об'єднаного центру передових технологій з кібероборони НАТО (2008 р.) і написання у 2012 році, за його ініціативи, Таллінського посібника з кібервійни – першого офіційного документу щодо застосування норм міжнародного гуманітарного права до воєнних дій у кіберпросторі;

масований кібервплив напередодні та впродовж російсько-грузинської війни (2008 р.), який є першим в історії випадком ведення державою координованих воєнних дій в кіберпросторі у

синхронізації з кінетичним протиборством на морі, у повітрі та на суходолі. Щонайменше за три тижні до початку активної фази конфлікту інформаційна інстраструктура Грузії почала піддаватися кібератакам, інтенсивність яких досягла максимуму з її початком. Веб-ресурси 54-ох організацій держави за напрямами урядування, фінансів та комунікацій були недоступними на момент початку війни завдяки атаці на відмову в обслуговуванні. Основна мета цих кібератак – не дати уряду висвітлювати події для цивілізованого світу та отримати його реакцію, у короткі терміни провівши наземну операцію, а також підсилити настрої зневіри та паніки серед населення. Ще одним виміром впливу був інформаційно-психологічний, прикладом чому є атака на викривлення контенту (вмісту) веб-сайту президента Грузії та зображення Михайла Саакашвілі в образі Гітлера. Серед особливостей можна вказати те, що перед враженням веб-ресурсів офіційних установ DDoS-атака була також направлена на популярний кіберзлочинний форум, для недопущення протидії грузинських хакерів. Останнім все ж вдалося дещо контратакувати, наприклад, на деякий час вивести з ладу веб-сайт інформаційного агентства «РІА Новини», однак це не спричинило якогось ефекту на хід війни. У цій ситуації спонсорування кібератак рф сумнівів не викликало, а безпосереднє їх виконання, на основі аналізу інтернет-трафіку, приписують APT Russian Business Network;

Agent.btz – кіберрозвідка за допомогою ШПЗ (комп'ютерного хробака), що розповсюдився військовими мережами США зі скомпрометованого флеш-накопичувача після його фізичного під'єднання до одного з комп'ютерів Центрального командування Збройних сил США. Виявивши у 2008 році, що за допомогою Agent.btz було отримано доступ як до не таємної, так і до інформації з обмеженим доступом, Пентагон витратив 14 місяців на повне очищення від нього своїх мереж та систем у межах оборонної кібероперації «Operation Buckshot Yankee». Базовою реакцією на витік конфіденційних даних стала заборона на використання сторонніх накопичувачів усіх типів на американських військових об'єктах, а стратегічною та визначною – утворення 21 травня 2010 року Кіберкомандування США, а згодом і кіберкомандування видів збройних сил. Agent.btz пов'язують із APT, відомим

як Turla, Uroborus, Snake, Venomous Bear, Krypton, а його, відповідно, з ФСБ рф;

кібервплив на інформаційну інфраструктуру США та Південної Кореї шляхом проведення циклу DDoS-атак. Кібератаки відбувалися у 3 хвилі, перша з яких розпочалася 04 липня 2009 року. Серед об'єктів, які піддалися атакам на відмову в обслуговуванні можна відмітити офіційні веб-ресурси Білого Дому, Пентагону, президента Південної Кореї та її оборонного і безпекового відомств, газети «The Washington Post», однієї з американських бірж та ін. Ці атаки одразу ж почали асоціювати із Північною Кореєю через їхній початок саме в день випробувань нею балістичних ракет малої дальності. Пізніше, у результаті аналізу декількох інших кібератак, дослідники дійшли висновку, що зазначені події 2009 року дійсно є результатом діяльності спонсорованого урядом КНДР APT Lazarus Group;

кібератаки на М'янму, що розпочалися 25 жовтня 2010 року з метою скомпрометувати проведення виборів до парламенту держави, які до цього не здійснювалися з 1990 року через режим військової диктатури. Кібератаки оцінюються як «значно потужніші» за ті, що відбулися в Естонії та Грузії у попередніх роках. Їхніми цілями стали сервери головного інтернет-провайдера країни, а також веб-ресурси міністерства зв'язку та телекомунікацій. Тодішня мережева організація М'янми дозволяла приймати та передавати інтернет-трафік обсягом до 45 МБіт/с, в той час як DDoS-атака забезпечила надсилання запитів зі швидкістю 10 – 15 ГБіт/с, триваючи більше восьми годин кожного дня. Атаку пов'язують із військовою диктатурою, яка не бажала передавати владу в країні демократам.

Підсумовуючи досвід ведення кіберборотьби першого періоду можна зробити такі висновки:

1. Основним типом об'єктів кібервпливу були об'єкти інформаційної інфраструктури (веб-ресурси, файлові та поштові сервери, сховища конфіденційних даних та ін.).

2. Для нанесення кібервпливу найчастіше застосовувалися DDoS-атаки, а також атаки на викривлення (зміну) контенту веб-ресурсів (defacement attack), ШПЗ було призначеним переважно для кіберрозвідки.

3. Кількісного значення кібервпливу тогочасних кібератак напряму залежало від кількості хостів (ботнетів), задіяних у DDoS-атаці та їх розподіленості у глобальній мережі Інтернет.