Зміст

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. В низки держав, як-от України, спеціальні підрозділи для ведення протиборства у кіберпросторі (кіберборотьби) перебувають на етапі формування та набуття спроможностей, в деяких (наприклад, США) такі військові формування існують та досить результативно застосовуються за призначенням вже тривалий час. Технології та засоби кіберзахисту, кіберрозвідки та кібервпливу удосконалюються в унісон з розвитком інформаційних технологій. Форми і способи протиборства у кіберпросторі постійно видозмінюються для досягнення поставлених воєнних цілей. 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.

В умовах відбиття Україною повномасштабної асиметричної збройної агресії, яка ведеться зокрема й у кіберпросторі, питання кіберстійкості інформаційно-комунікаційних систем оборонного та безпекового призначення є актуальним як ніколи. Цифрова трансформація українського суспільства призвела до критичної залежності безпеки громадян, національної та воєнної безпеки від стійкого рівня функціонування об'єктів критичної інформаційної інфраструктури держави. З огляду на це, вкрай важливою є можливість прогнозування динаміки функціонування інформаційно-комунікаційних систем оборонного та безпекового призначення в умовах постійного кібервпливу противника з метою оцінювання рівня їх кіберстійкості.

Розділ 1

ПРАКТИКА ФУНКЦІОНУВАННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ОБОРОННОГО ТА БЕЗПЕКОВОГО ПРИЗНАЧЕННЯ В УМОВАХ КІБЕРВПЛИВУ ПРОТИВНИКА

Функціонування захищених інформаційно-комунікаційних систем (ІКС) оборонного та безпекового призначення та кіберстійкість такого функціонування залежить від ефективності кібервпливу противника, достатнього кіберзахисту власної кіберінфраструктури та оперативності кіберрозвідки обох сторін кіберборотьби, яка є комплексом заходів з кіберзахисту, кіберрозвідки й кібервпливу.

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 Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (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 Advanced persistent threat (APT), як Sandworm та FancyBear. Більш ніж ймовірно, ці групи діють під егідою Головне розвідувальне управління Генерального штабу Збройних Сил російської федерації (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