УДК 004.056.5:355.01(477)
DOI: 10.31673/2409-7292.2023.030001

Савченко В. А.

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КІБЕРОБОРОНИ ДЕРЖАВИ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Стаття присвячена проблемі стійкості кібероборони національної безпеки в контексті сучасних збройних конфліктів. У роботі розглядаються ключові аспекти, які становлять загрозу для кібербезпеки держави, включаючи кібератаки, кібершпигунство і кіберсаботаж. Стаття аналізує необхідність розвитку кіберінфраструктури, підготовки кадрів та кризового плану для відновлення після кібератаки. Також розглядається роль державних інституцій у забезпеченні кібербезпеки, включаючи розробку нормативного регулювання і співпрацю з приватним сектором та академічними установами. Крім того, стаття висвітлює міжнародний аспект стійкості кібероборони і важливість співпраці між державами та дотримання міжнародних норм і правил у кіберпросторі. Робота закінчується висновками щодо важливості спільних зусиль національних та міжнародних громадських структур для забезпечення сталої кібербезпеки в умовах збройних конфліктів.

Ключові слова: кібербезпека, кібероборона, стійкість кібероборони, війна, збройний конфлікт.

Вступ

В сучасному світі кібербезпека стала однією з найбільш актуальних та чутливих складових національної безпеки держав. Відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [1]:

«Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії» (рис. 1).

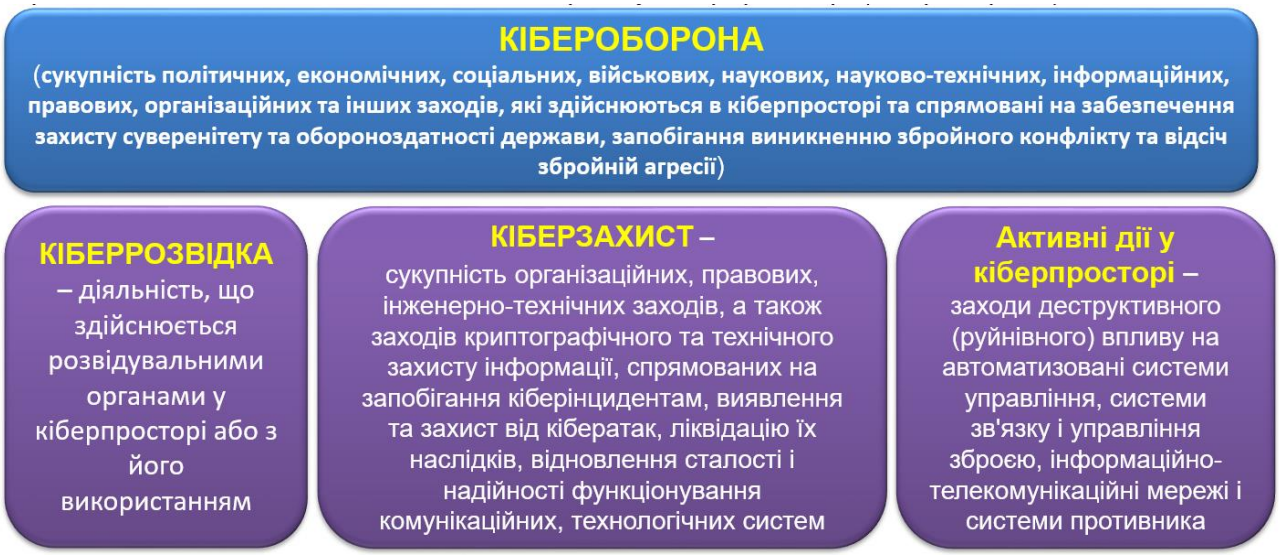

Рис. 1. Сутність кібероборони держави

Також, відповідно до статті 8 цього ж Закону: «Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану».

Постановка проблеми

Збройні конфлікти та геополітичні напруження додають новий рівень складності та серйозності до питань кібероборони. Забезпечення стійкості кібероборони стає важливим завданням, яке вимагає комплексного підходу та систематичної роботи.

Аналіз дотичних робіт

У монографії [2] досліджені теоретичні та практичні аспекти забезпечення національної стійкості в умовах мінливості й невизначеності безпекового середовища. Розроблені рекомендації щодо концептуальних засад та моделі забезпечення національної стійкості в Україні, формування й реалізації комплексної державної політики у сфері національної безпеки та стійкості, удосконалення законодавства Україні у відповідній сфері. У той же час питання кібербезпеки та кібероборони розглянуті авторкою поверхнево і не є ключовими для забезпечення національної стійкості.

У роботі [3] автори дають визначення, мету, завдання та формулюють стратегічні цілі кібероборони держави. Разом з тим, питання стійкості такої кібероборони залишаються поза увагою авторів. Публікація [4] глибоко аналізує суть поняття «Кібероборона», проте, основний акцент публікації зроблено на реалізації організаційних заходів кібероборони та створенні кібервійськ.

У цій статті ми розглянемо, як забезпечити стійкість кібероборони держави в умовах збройного конфлікту. Ми розглянемо загрози, які створюють кібератаки, і визначимо елементи, які допомагають зміцнити кібероборону. Також, ми проаналізуємо роль державних інституцій у забезпеченні кібербезпеки та важливість міжнародного співробітництва у цій сфері. Розуміння цих питань мають вирішальне значення для забезпечення національної безпеки та збереження миру в умовах сучасних геополітичних реалій.

Загрози кібербезпеці в умовах збройного конфлікту

Умови збройного конфлікту суттєво збільшують загрози для кібербезпеки держави. Кібератаки можуть бути використані в якості зброї, яка наносить значну шкоду як військовим, так і цивільним об'єктам. Далі ми розглянемо основні аспекти цих загроз та їх можливі наслідки.

Кібератаки та їх види. Умови збройного конфлікту роблять кібератаки ще більш небезпечними, оскільки їх метою може бути завдання шкоди об’єктам інфраструктури, комунікацій, електронної системи управління тощо. Можна виділити наступні види кібератак, які є найбільш характерними під час збройного конфлікту:

DDoS атаки: Полягають у перевантаженні цільового сервера запитами, що призводить до відмови в обслуговуванні. Умови збройного конфлікту можуть призвести до масштабних DDoS-атак на важливі об'єкти.

Шкідливе програмне забезпечення та віруси: Зловмисний код може використовуватися для руйнування або злому інформаційних систем. У разі збройного конфлікту, це може стати інструментом руйнування інфраструктури.

Фішинг та соціальна інженерія: Шахраї можуть використовувати соціальні мережі та фішингові атаки для отримання доступу до конфіденційної інформації та керівництва держави.

Кібершпигунство: Держави або хакерські групи можуть використовувати кібершпигунство для здобуття важливих розвідувальних даних та секретів.

Ризики для державної безпеки. Умови збройного конфлікту збільшують ризики для державної безпеки через кібератаки. Деякі з найбільш важливих ризиків включають:

Втрата даних: Кібератаки можуть призвести до великих втрат конфіденційної інформації, такої як військові плани, дипломатична пошта, інформація про критичну інфраструктуру тощо.

Відмова систем управління: Кібератаки можуть паралізувати системи управління та комунікації, що суттєво ускладнює прийняття стратегічних рішень та керування військами.

Завдання економічної шкоди: Кібератаки можуть спричинити значну економічну шкоду державі, зокрема, завдати шкоди фінансовим інститутам, енергетичним компаніям та іншим важливим галузям.

Кібератаки на Україну у 2022–2023 р.р. За даними Державної служби спеціального зв'язку та захисту інформації України протягом 2022 року Україна стикнулася з 7 тис. кібератак на інформаційну інфраструктуру. У порівнянні з 2021 роком, загальна кількість атак збільшилась майже втричі.

Крім того, з 24 лютого і до кінця 2022 року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA опрацювала 2194 кіберінциденти. З них 120 стосувалися фінансового сектору, 156 – комерційних організацій та 92 – сектору телекомунікацій і розробки програмного забезпечення [5].

У 2023 році команда CERT-UA лише у першому кварталі зафіксувала 700 потужних атак, 88.8% з яких становлять саме DDoS-атаки. Головними об'єктами DDoS-атак у першому півріччі 2023 року в Україні стали: держава, фінансова сфера, медіа, IT, телеком та логістика.

Умови збройного конфлікту зумовлюють потребу вдосконалення заходів кібербезпеки та прийняття ефективних заходів для захисту державних інтересів в кіберпросторі. Далі у статті ми розглянемо елементи забезпечення стійкості кібероборони, ролі державних інституцій та міжнародний аспект цього питання.

Елементи забезпечення стійкості кібероборони

Забезпечення стійкості кібероборони є критично важливим завданням для будь-якої сучасної держави, особливо в умовах збройного конфлікту. Ефективна кібероборона передбачає розвиток комплексної стратегії, яка включає в себе численні елементи, спрямовані на попередження, виявлення та реагування на кібератаки. Тому, далі ми розглянемо основні складові забезпечення стійкості кібероборони.

Розвиток кіберінфраструктури. *Системи захисту мереж та інформації* включають у себе антивіруси, брандмауери, системи виявлення вторгнень, шифрування даних та інші технології. Вони призначені для виявлення та усунення загроз в реальному часі. Розвиток та постійне оновлення цих систем є важливим для підтримки кібербезпеки.

Захист критично важливих об'єктів: Критично важливі об'єкти, такі як енергетичні системи, транспорт, банківські установи та зв'язок, потребують особливого захисту. Вони можуть бути метою спроб руйнування або розкриття конфіденційної інформації. Важливим є посилення захисту цих об'єктів та використання резервних систем.

Підготовка персоналу. Ефективна кібероборона вимагає надійної підготовки персоналу. Регулярні навчання та тренування щодо кібербезпеки допомагають розповсюджувати навички та свідомість серед співробітників та державних службовців. Навчання повинно включати в себе розпізнавання загроз, процедури реагування та попередження соціальної інженерії.

Залучення експертів: У разі збройного конфлікту важливо мати доступ до експертів з кібербезпеки. Це може бути як внутрішній резерв, так і зовнішні консультанти, які можуть надавати професійну експертизу щодо кіберзагроз та допомагати в розслідуванні інцидентів.

Створення кризових планів та стратегій. *Відновлення після кібератаки*: Важливо мати плани відновлення після кібератаки, які включають в себе процедури відновлення інфраструктури та даних, а також роботу з громадськістю та відшкодування збитків. Це допомагає скоротити час відновлення після інциденту.

Співпраця з іншими державами: Умови збройного конфлікту вимагають співпраці з іншими державами щодо обміну інформацією про кіберзагрози та спільних заходів для їх попередження. Міжнародна співпраця є важливим елементом стійкості кібероборони.

Співпраця з приватним сектором: Приватні компанії, які володіють критично важливою інфраструктурою, також мають бути включені до планів стійкості кібероборони. Співпраця з приватним сектором може допомогти виявляти та реагувати на загрози швидше та ефективніше.

Захист важливої інформації: Важлива інформація повинна бути захищена від доступу несанкціонованих осіб. Це може включати в себе шифрування, контроль доступу та резервне зберігання.

Планування для надзвичайних ситуацій: Крім відновлення після кібератаки, важливо мати плани для надзвичайних ситуацій, таких як евакуація персоналу, комунікація в умовах відсутності інтернету чи електроенергії, інші та інші заходи для забезпечення безпеки та стійкості.

Роль державних інституцій у забезпеченні кібероборони

Роль державних інституцій у забезпеченні кібероборони досить важлива, оскільки вони визначають та реалізують політику та стратегію держави щодо кібербезпеки. Ці інституції мають на меті розробку та впровадження заходів, спрямованих на запобігання кібератак, виявлення загроз та ефективне реагування на них.

Нормативне регулювання кібербезпеки

Законодавство та політика: Державні інституції відповідають за створення законодавства та політичних документів, які регулюють кібербезпеку. Це включає в себе прийняття законів, які криміналізують кіберзлочини та встановлюють відповідальність за порушення кібербезпеки.

Створення стандартів та регуляторних актів: Держави можуть розробляти стандарти та регулятиви для галузей, які важливі для національної безпеки, такі як енергетика, фінанси, транспорт та зв'язок. Ці стандарти визначають вимоги до кібербезпеки та регулюють заходи, які повинні бути вжиті для захисту критично важливих об'єктів.

Роль військових та правоохоронних структур

Військові структури відіграють ключову роль у забезпеченні кібероборони держави (рис. 2). Вони відповідають за виявлення, відсіювання та захист військових мереж і інформації. Військова кіберборона також включає в себе розробку кіберстратегій та військових доктрин.

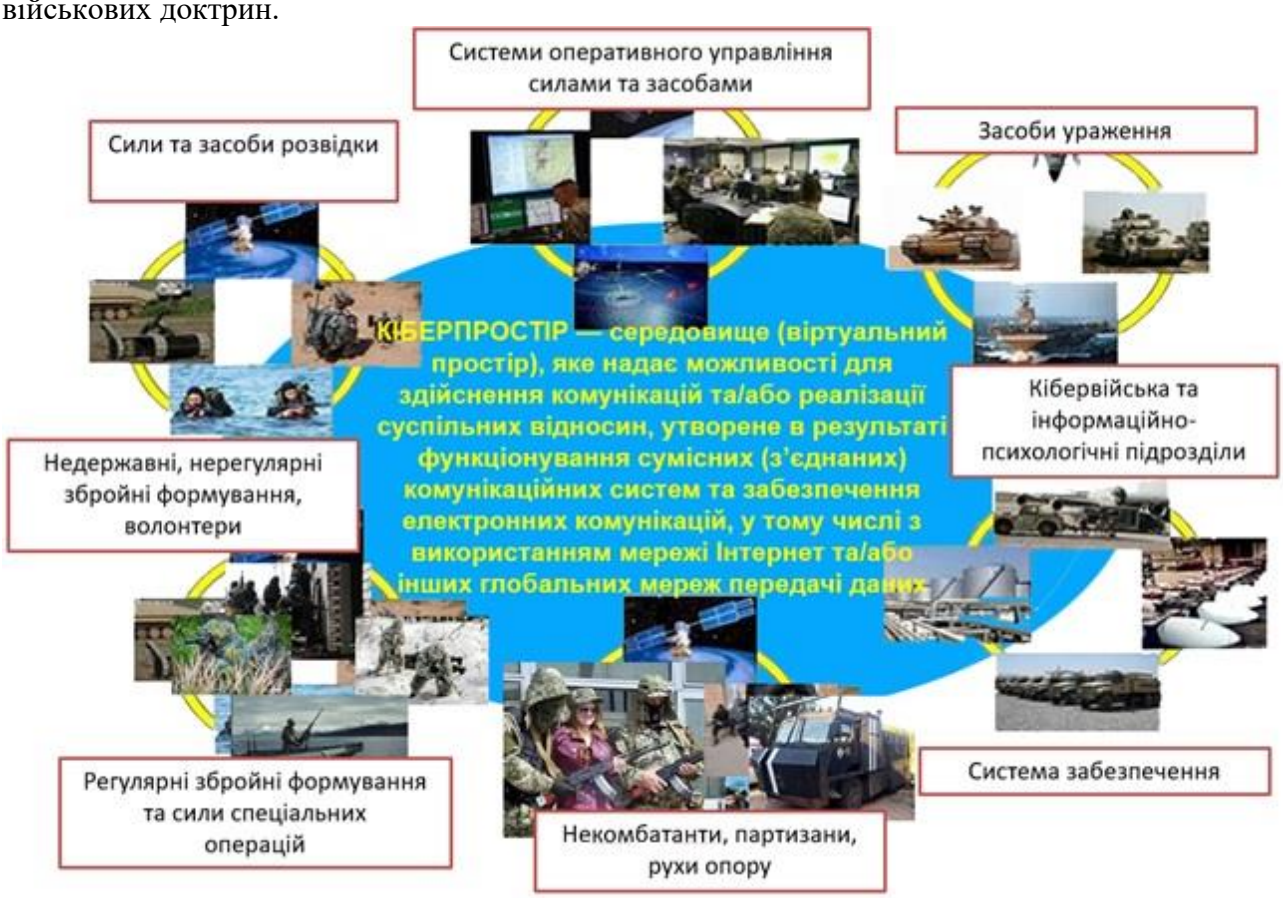

Рис. 2. Військова компонента кібероборони

Правоохоронні органи здійснюють розслідування кіберзлочинів та переслідують винних осіб. Вони також відповідають за виявлення та розслідування загроз для національної безпеки у кіберпросторі.

Співпраця з приватним сектором та академічними установами

Приватний сектор: Велика частина критично важливої інфраструктури перебуває у власності та управлінні приватних компаній. Державні інституції співпрацюють з приватним сектором для розробки та впровадження заходів кібербезпеки. Ця співпраця включає в себе обмін інформацією про загрози та спільні ініціативи.

Академічні установи: Академічні установи грають важливу роль у дослідженні кібербезпеки та розробці нових технологій для захисту інформації та інфраструктури. Державні інституції можуть співпрацювати з академічними установами для проведення досліджень та навчання.

Фінансування та ресурси

Бюджети та фінансування: Для забезпечення ефективної кібероборони держави повинні виділяти достатні кошти на розвиток та підтримку кіберінфраструктури та кадрів.

Людські ресурси: Державні інституції також повинні забезпечувати кваліфікований персонал для здійснення кібербезпеки. Це охоплює військових, правоохоронців, аналітиків, інженерів і спеціалістів з кібербезпеки.

Забезпечення стійкості кібероборони вимагає скоординованих зусиль державних інституцій, приватного сектору та академічних установ. Ефективне законодавство, міцні військові та правоохоронні структури, співпраця з приватним сектором та академічними установами, а також належне фінансування дозволяють країні забезпечити високий рівень кібербезпеки в умовах збройного конфлікту. Далі ми розглянемо міжнародний аспект стійкості кібероборони.

Забезпечення стійкості кібероборони – це процес, що постійно еволюціонує та вимагає надійної стратегії та систематичного підходу. Постійна оцінка загроз, підготовка персоналу, співпраця з іншими державами та розвиток кіберінфраструктури є важливими компонентами успішного забезпечення кібербезпеки в умовах збройного конфлікту. Далі ми розглянемо роль державних інституцій та міжнародний аспект стійкості кібероборони.

Міжнародний аспект стійкості кібероборони

У світі, де кібератаки можуть бути виконані з будь-якого кутка глобусу, міжнародний аспект стійкості кібероборони набуває вирішального значення. Співпраця між державами, створення міжнародних стандартів та регулятивів, а також участь у міжнародних ініціативах грають ключову роль у забезпеченні кібербезпеки та відповіді на кіберзагрози. Далі ми розглянемо міжнародний аспект стійкості кібероборони.

Міжнародне право та норми

Міжнародне право: Міжнародне право грає важливу роль у регулюванні кібербезпеки. Кібероперації, здійснювані державами, повинні відповідати основним принципам міжнародного права, включаючи принципи невтручання в суверенітет і недоторканість держав, що закріплені в Уставі Організації Об'єднаних Націй.

Кібернорми та довірливі відносини: Міжнародні кібернорми та довірливі відносини сприяють створенню правил гри в кіберпросторі. Наприклад, Робоча група ООН з питань інформаційної безпеки розробила низку рекомендацій щодо кібернорм та прозорості в кіберпросторі.

Міжнародні спільні ініціативи

Міжнародні угоди та конвенції: Деякі держави укладають міжнародні угоди та конвенції, спрямовані на забезпечення кібербезпеки. Наприклад, Будапештська конвенція про кіберзлочинність та Кібернормандія, розроблена Європейським Союзом, об'єднують держави в питаннях боротьби з кіберзлочинністю та регулювання кіберпростору.

© Савченко, В. А. (2023). Забезпечення стійкості кібероборони держави в умовах збройного конфлікту. Сучасний захист інформації, 3(55), 6–11. https://doi.org/10.31673/2409-7292.2023.030001.

Міжнародні ініціативи та форуми: Міжнародні ініціативи, такі як Глобальний інтернет-форум, форум з питань інформаційної безпеки в Мюнхені, та інші, створюють можливості для обміну ідеями та досвідом між державами щодо кібербезпеки.

Міжнародна співпраця

Спільні дії в разі кібератак: умови збройного конфлікту можуть вимагати спільних дій декількох держав для відповіді на масштабні кібератаки. Спільні дії можуть включати в себе обмін інформацією, координацію заходів та підтримку від інших держав.

Технічна співпраця: Держави можуть співпрацювати у сфері кібербезпеки, обмінюючи технічною інформацією та ресурсами для виявлення та реагування на кіберзагрози.

Розбудова міжнародних партнерств: Держави можуть розбудовувати міжнародні партнерства для спільного вирішення питань кібербезпеки. Такі партнерства можуть включати в себе обмін досвідом, технологіями та навчанням.

Міжнародний аспект стійкості кібероборони важливий для забезпечення безпеки та захисту в умовах збройного конфлікту. Співпраця між державами та дотримання міжнародних норм і правил в кіберпросторі сприяють стійкості та безпеці. Далі буде розглянуто важливість публічної свідомості та освіти в галузі кібербезпеки.

Висновки

Забезпечення стійкості кібероборони держави в умовах збройного конфлікту є важливим завданням, яке вимагає комплексного підходу та співпраці на національному та міжнародному рівнях. Приклади кібератак на Україну показують, що кіберзагрози можуть бути використані для досягнення політичних та стратегічних цілей в умовах збройного конфлікту.

Для забезпечення стійкості кібероборони держави в умовах збройного конфлікту важливо розвивати кіберінфраструктуру, підготовку персоналу та кризові плани для відновлення після кібератаки. Роль державних інституцій включає в себе розробку нормативного регулювання, розвиток кібервійськових та правоохоронних структур, а також співпрацю з приватним сектором та академічними установами. Міжнародний аспект стійкості кібероборони передбачає дотримання міжнародного права та норм, участь у міжнародних угодах та ініціативах, а також співпрацю з іншими державами у вирішенні спільних проблем кібербезпеки. Співпраця та довірливі міроприйняття в кіберпросторі є ключовими для забезпечення стійкості.

Забезпечення стійкості кібероборони – це складне завдання, яке вимагає постійного вдосконалення та співпраці. Тільки шляхом спільних зусиль національних та міжнародних громадських структур можна забезпечити надійний захист у кіберпросторі.

Перелік посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19.
2. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. – Київ : НІСД, 2022. – 456 с.
3. Даник Ю.Г. Основи кібербезпеки та кібероборони / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.
4. Всеохоплююча оборона України: стан, проблеми та заходи щодо зміцнення кібероборони держави і створення кібервійськ. URL : https://opk.com.ua/
5. Кібератаки на Україну. URL : https://uworld.news/news/kiberataky-rosii-na-ukrainu-ie-1002005.html
6. Buchan, J., Carr, M., & Hancock, C. (2018). Cyber Resilience: A Review of Critical National Infrastructure in the UK. International Journal of Disaster Risk Reduction, 27, 145-152.

Надійшла 08.07.2023 Рецензент: д.т.н., професор Вишнівський В.В.