Рекомендації та перспективи впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України

Recommendations and prospects for introducing the experience of foreign countries into the system of forming the genesis of the development of cyber technologies in the sphere of security and defense of Ukraine

Олег Семененко [A]
Corresponding author: д. військ. н., професор, начальник відділу, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Сергій Островський [A]
к.в.н., начальник науково-дослідного відділу, e-mail: ostrovserg@ukr.net, ORCID: 0000-0002-4702-9808

Максим Бондаренко [B]
e-mail: whoishitchkok@gmail.com, ORCID: 0009-0005-7902-9440

Ярослав Вовк [B]
e-mail: whoishitchkok@gmail.com, ORCID: 0009-0001-5710-5642

Дмитро Куценко [B]
e-mail: whoishitchkok@gmail.com, ORCID: 0009-0000-5940-9941

Oleh Semenenko [A]
Corresponding author: Dr of military Sciences, Professor, e-mail: aosemenenko@ukr.net, ORCID: 0000-0001-6477-3414

Serhii Ostrovskyi [A]
Candidate of Military Sciences, Head of the Research Department, e-mail: OstrovSerg@ukr.net, ORCID: 0000-0003-2767-0891

Maksym Bondarenko [B]
e-mail: whoishitchkok@gmail.com, ORCID: 0009-0005-7902-9440

Yaroslav Vovk [B]
e-mail: whoishitchkok @gmail.com, ORCID: 0009-0001-5710-5642

Dmutro Kutsenko [B]
e-mail: whoishitchkok@gmail.com, ORCID: 0009-0000-5940-9941

[A] Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна
[B] Міністерство оборони України, м. Київ, Україна

[A] Central Research Institute of the Armed Forces of Ukraine, Kyiv, Ukraine
[B] Ministry of Defence Ukraine, Kyiv, Ukraine

Received: August 10, 2023 | Revised: August 23, 2023 | Accepted: August 31, 2023

DOI: 10.33445/sds.2023.13.4.6

Мета роботи: полягає у розробленні рекомендацій та визначенні перспектив впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України.

Метод дослідження: основними методами досліджень є методи аналізу та синтезу, методи воєнно-економічної теорії, методи оцінювання та співставлення, індукції та дедукції, методи математичної статистики.

Результати дослідження: визначено послідовність формування генезису кібертехнологій у сфері безпеки та оборони України; проведено огляд розвитку кібертехнологій у деяких країнах світу у сфері безпеки та оборони станом на кінець 2021 року в рамках позитивного досвіду для України; розкрито показники фінансування розвитку галузі кібертехнологій оборонної сфери та країни в цілому, які розкривають ставлення цих країн до пріоритетності розвитку кібертехнологій та відношення керівництва держави до цієї галузі; сформовано напрями подальших досліджень за тематикою формування генезису розвитку кібертехнологій у сфері оборони України.

Теоретична цінність дослідження: аналіз теоретичних та практичних аспектів досвіду іноземних держав в системі формування генезису розвитку кібертехнологій у сфері безпеки та оборони України дозволив сформувати загальні рекомендації щодо розвитку кібертехнологій в

Purpose: is to develop recommendations and determine the prospects of introducing the experience of foreign countries into the system of forming the genesis of the development of cyber technologies in the sphere of security and defense of Ukraine.

Method: the main methods of research are methods of analysis and synthesis, methods of military economic theory, methods of evaluation and comparison, induction and deduction, methods of mathematical statistics.

Findings: In the article: the sequence of formation of the genesis of cyber technologies in the sphere of security and defense of Ukraine is defined; a review of the development of cyber technologies in some countries of the world in the field of security and defense was conducted as of the end of 2021 as part of a positive experience for Ukraine; indicators of funding for the development of cyber technologies in the defense sphere and the country as a whole are disclosed, which reveal the attitude of these countries to the priority of the development of cyber technologies and the attitude of the state leadership to this industry; the directions of further research on the topic of the formation of the genesis of the development of cyber technologies in the sphere of defense of Ukraine were formed.

Theoretical implications: the analysis of theoretical and practical aspects of the experience of foreign countries in the system of forming the genesis of the development of cyber technologies in the sphere of security and defense of Ukraine made it possible to formulate general recommendations for the development of cyber

сфері безпеки та оборони Україні, а також визначити шляхи та строки їх практичної реалізації.
Тип статті: теоретичний**,** описовий, практичний, методичний.

technologies in the sphere of security and defense of Ukraine, as well as to determine the ways and terms of their practical implementation.
Paper type: theoretical, descriptive, practical, methodical.

Ключові слова: кібертехнологій, кібербезпека, кіберзброя, кібертероризм, кібершпигунство.

Key words: cyber technologies, cyber security, cyber weapons, cyber terrorism, cyber espionage.

1. Вступ

Актуальність дослідження генезису розвитку кібертехнологій у сфері оборони України є надзвичайно важливою в контексті сучасної геополітичної обстановки та загроз, що стосуються кібербезпеки та національної безпеки загалом [1]–[5]. Дослідження даного питання сьогодні має кілька ключових аспектів, що підкреслюють його актуальність, а саме:

- зростаючі кіберзагрози, тому, що у сучасному світі кіберзагрози стають все більш небезпечними та розповсюдженими [4]–[12]. Держави, у тому числі Україна, стикаються зі зростаючими атаками на інформаційні системи, критичну інфраструктуру та оборонні системи. Розвиток кібертехнологій у сфері оборони є необхідним для відповіді на ці загрози та забезпечення національної безпеки;

- залежність від технологій, тому, що сучасна військова діяльність сильно залежить від інформаційних та комунікаційних технологій. Країни, які володіють передовими кібертехнологіями, мають перевагу у веденні військових операцій, здатність швидко реагувати на загрози та забезпечувати сучасний рівень захисту;

- розвиток військового потенціалу, сьогодні Україна знаходиться в складних геополітичних умовах, де важливо мати сильний військовий потенціал для забезпечення національної територіальної цілісності. Розвиток кібертехнологій може значно підвищити ефективність військових операцій, забезпечити оперативне реагування на загрози та зменшити ризики для військових та цивільних об'єктів;

- дослідження генезису розвитку кібертехнологій у сфері оборони сприяє науковому та технологічному прогресу в країні. Це сприяє залученню талановитої молоді до роботи над сучасними технологіями, створенню інноваційних рішень та підвищенню наукового потенціалу України;

- міжнародне співробітництво, обумовлено тим, що проблеми кібербезпеки та розвитку кібертехнологій є глобальними. Активна участь України в міжнародних ініціативах та співробітництві може сприяти обміну досвідом, найкращими практиками та технологіями у цій сфері.

Отже, дослідження генезису розвитку кібертехнологій у сфері оборони України є актуальним завданням, яке впливає на національну безпеку, воєнний (оборонний) потенціал країни, інноваційний розвиток та міжнародне співробітництво країни [1]–[20].

2. Теоретичні основи дослідження

Аналіз останніх досліджень, публікацій та документів за тематикою статті показує [1]–[19], що сучасний світ переживає епоху стрімкого розвитку кібертехнологій та відчутної залежності від цифрового простору. У цьому контексті, тема кібербезпеки та кіберзахисту в сфері оборони стає однією з найбільш актуальних і нагальних завдань на глобальному та регіональному рівнях. Постійні та швидкозмінні технологічні досягнення, а також зростаюча кількість кібератак на об'єкти оборони вимагають глибокого та постійного аналізу проблематики, а також розробки ефективних заходів захисту національних та глобальних інтересів.

На глобальному рівні, кібертероризм, кібершпигунство та кібератаки стають суттєвими загрозами для міжнародної безпеки, військової стабільності та глобального економічного розвитку. Проведення досліджень у цій галузі допомагає розкрити нові можливості та сценарії

розвитку подій у цифровому просторі та сприяє формуванню стратегій міжнародного співробітництва в галузі кібербезпеки.

На регіональному рівні, кожна країна стикається з унікальними викликами у сфері кібербезпеки, які залежать від її геополітичного положення, технологічного розвитку та оборонної інфраструктури. Дослідження щодо кіберзагроз та можливостей розвитку кіберзбройних сил стають критичними для формування національних стратегій безпеки та захисту важливої інформації.

Аналіз досліджень та публікацій за тематикою статті [3]–[19] показує, що в іноземних державах ця галузь отримує значний обсяг уваги та інвестицій. Іноземний досвід показує, що успішне формування кібертехнологій у сфері безпеки та оборони базується на сильних наукових дослідженнях, тісній співпраці між університетами, дослідницькими центрами та приватним сектором, а також ефективному впровадженні результатів цих досліджень у практику. Важливим аспектом є також розвиток кадрового потенціалу в цій галузі, зокрема підготовка фахівців з високим рівнем компетенцій технічного напряму та безпосередньо кібербезпеки. Нижче наведено результати аналізу основних іноземних та вітчизняних джерел за тематикою статті, а також розкрито основний зміст дослідження за кожним джерелом:

[4] Singer P.W. and Allan Friedman (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. P. 336. Ця книга розглядає проблеми кібербезпеки та кібервійни, а також їх вплив на сучасний світ. Автори аналізують технічні, політичні та економічні аспекти цих питань;

[5] Alexander Klimburg (2017). The Darkening Web: The War for Cyberspace. Penguin Books. P. 448. Книга досліджує зростання конфліктів у кіберпросторі та їх вплив на міжнародні відносини. Автор досліджує ролі держав, хакерських груп та інших акторів у кібербезпеці;

[6] Дергачов О. (2018). Кібербезпека: загрози та захист. Національний університет "Львівська політехніка". С. 312. Книга присвячена аналізу загроз кібербезпеці та можливостям їх запобігання та захисту. Автор детально розглядає технічні та організаційні аспекти кіберзаходів;

[7] Тищенко О. (2016). Інформаційна безпека держави: кібераспекти. Національна академія державного управління при Президентові України. С. 232. Автор розглядає роль кібертехнологій у забезпеченні інформаційної безпеки держави, виокремлюючи основні виклики та шляхи їх подолання;

[8] David E. Sanger. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown. P. 384. Книга розглядає розвиток кіберзброї, кібершпигунства та їх вплив на міжнародну політику та геополітичні відносини між країнами та світу в цілому;

[9] Richard A. Clarke and Robert K. Knake (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco. P. 320. Автори обговорюють загрози кібервійни для національної безпеки та пропонують стратегії для захисту від цих загроз;

[10] Гіль О. (2019). Кібербезпека держави: інструменти, методи, практика. Видавничий дім "Ін Юре". P. 400. Книга присвячена розгляду питань кібербезпеки держави, включаючи правові, технічні та організаційні аспекти;

[11] Бортнік С., Скасницький О. (2016). Кібербезпека: загрози та виклики. Національний технічний університет України "Київський політехнічний інститут". P. 268. Автори аналізують сучасні загрози кібербезпеці, їхні впливи на суспільство та можливі шляхи подолання цих викликів;

[12] Lester Evans. (2020). Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners. Independently published. P. 240. Книга надає загальний огляд кібербезпеки, включаючи аспекти соціального інжинірингу, Інтернету речей та етичного хакінгу;

[13] Singer P.W. and Allan Friedman. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. С. 336. Ця книга розглядає проблеми кібербезпеки та кібервійни, а також їх вплив на сучасний світ. Автори аналізують технічні, політичні та економічні аспекти цих питань;

[14] Губарєв В. (2020). Кібербезпека та захист інформації. Національний університет "Львівська політехніка". С. 272. Книга присвячена аспектам кібербезпеки та захисту інформації, включаючи технічні, правові та соціальні аспекти;

[15] Гарань О. (2019). Кібербезпека України: стан, пріоритети, ризики. Інститут світової політики. С. 120. Автор аналізує стан кібербезпеки в Україні, виділяючи основні пріоритети та ризики в цій сфері;

[16] P.W. Singer and August Cole. (2015). Ghost Fleet: A Novel of the Next World War. Eamon Dolan/Mariner Books. P. 416. Це науково-фантастичний роман, що розглядає можливий сценарій майбутньої війни, де кібертехнології та військова техніка відіграють ключову роль;

[17] Richard A. Clarke and Robert K. Knake. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press. P. 320. Автори обговорюють важливість кібербезпеки як п'ятої сфери (після землі, води, повітря та космосу) та розглядають підходи до захисту від кіберзагроз;

[18] Мішечкіна Л. (2020). Кібербезпека в системі національної безпеки України. Видавничий дім "Ін Юре". С. 400. Книга розглядає взаємозв'язок кібербезпеки з національною безпекою України, а також важливість кіберзахисту для забезпечення суверенітету держави;

[19] Сокірко В. (2017). Кібербезпека: проблеми, загрози та виклики. Видавництво: Центр учбової літератури. С. 336. Автор розглядає основні питання кібербезпеки, включаючи її проблеми, загрози та виклики для сучасного суспільства.

Проведений аналіз наведених джерел показує, що впровадження подібного досвіду в Україні стикається зі своїми викликами. Сьогодні в Україні необхідно створити ефективну систему підтримки наукових досліджень у цій галузі, сприяти партнерству між академічною спільнотою та промисловістю, а також створити сприятливе середовище для інновацій та підприємництва в кібербезпеці. Забезпечення кібербезпеки в сфері оборони також вимагає розробки високотехнологічних рішень та впровадження передових практик. Отже, аналіз показує, що інтеграція закордонного досвіду в галузі кібертехнологій у сфері безпеки та оборони є важливим кроком для забезпечення національної кібербезпеки та підвищення ефективності оборонної галузі в Україні.

3. Постановка проблеми

Триваюча російсько-українська війна демонструє, що сучасні конфлікти можуть включати не лише фізичні бойові дії, а й використання кіберзброї, яка може завдати непередбачувану шкоду важливим інфраструктурним об'єктам та економіці країни, а саме:

по-перше, кібератаки можуть призвести до порушення функціонування критичних інфраструктур, таких як енергетичні системи, транспорт, фінансові установи тощо, що може призвести до значних економічних втрат та дестабілізації суспільства;

по-друге, інформаційні операції в кіберпросторі можуть використовуватися для маніпулювання громадською думкою, дезінформації та дестабілізації соціально-політичної ситуації, що може вплинути на масову психологію населення та зруйнувати довіру до власних інституцій;

по-третє, забезпечення кібербезпеки є важливим аспектом захисту державних та військових секретів. Зламання кіберзахисту може призвести до витоку конфіденційної інформації, яка може бути використана проти національних інтересів держави.

У зв'язку з цим, розвиток кібертехнологій у сфері оборони стає пріоритетом для України, а формування генезису розвитку кібертехнологій у сфері оборони України є нагальним завданням сьогодення. Ефективна кібероборона може суттєво підвищити стійкість країни до сучасних загроз і забезпечити національну безпеку в умовах активної кібервійни. Для цього необхідно інвестувати в розробку та здійснювати впровадження передових кіберзахисних технологій, підвищувати кваліфікацію фахівців у цій галузі, сприяти активному співробітництву з міжнародними партнерами. Отже, у звітному періоді російсько-української війни актуальність розвитку кібертехнологій у сфері оборони України визначається потребою забезпечити стійкість суспільства до нових, складних викликів у кіберпросторі, зберегти національну безпеку та суверенітет.

Невід'ємною складовою актуальності питання формування генезису розвитку кібертехнологій у сфері оборони України є постійний характер кіберзагроз з боку Росії та інших потенційних противників [1]–[6]. У контексті тривалої російсько-української війни, Кремль активно використовує кібератаки та інформаційні операції для підриву національної безпеки України. Це включає в себе спроби дезорганізації військового управління, блокування критичних інфраструктурних об'єктів, поширення фейкової інформації, та навіть спроби втручання у виборчі процеси. Зростаюча складність та суворість кіберзагроз вимагають від країни активної реакції та глибокого вивчення цього феномену. Важливо враховувати, що кіберзагрози не обмежуються лише військовою сферою, а також поширюються на економічний, політичний та інформаційний розвиток країни. Недостатня кібербезпека може серйозно підірвати інвестиційний клімат, призвести до втрати довіри міжнародних партнерів, а також до зростання загроз для громадянського суспільства та демократичних інститутів [7]–[12]. Україна має потенціал та ресурси для активного розвитку кібертехнологій в сфері оборони. Створення інноваційних кіберзахисних рішень, розробка захищених комунікаційних систем для військових та керівництва, а також навчання фахівців з кібербезпеки – все це сприятиме підвищенню національної стійкості до кіберзагроз. Також важливо зміцнювати міжнародне співробітництво в цій галузі, обмінюючись досвідом та інформацією з іншими країнами, щоб в сукупності протистояти глобальним кібервикликам. У підсумку, умови тривалої російсько-української війни наголошують на необхідності активного формування генезису розвитку кібертехнологій у сфері оборони України, бо це стає важливим кроком для забезпечення національної безпеки, ефективного використання інформаційних ресурсів та збереження суверенітету країни.

Отже, метою статті є розроблення рекомендацій та визначення перспектив щодо впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України.

4. Результати

Генезис розвитку кібертехнологій у сфері оборони відноситься до процесу появи, еволюції і розвитку цифрових технологій та інформаційних систем, які використовуються для забезпечення безпеки, ведення військових операцій та вирішення завдань національної оборони. Цей процес охоплює створення нових програмних і апаратних засобів, кіберзброї, аналітичних систем, а також вдосконалення методів захисту від кіберзагроз та забезпечення кібербезпеки.

Генезис в цьому контексті відображає послідовність подій та етапів, що призвели до створення та розвитку кібертехнологій у військовій галузі. Він охоплює такі аспекти, як наукові дослідження, винайдення нових методів атаки та захисту, розвиток відповідних кадрових ресурсів, а також взаємодію з цивільним сектором для перенесення цифрових інновацій з громадської сфери в сферу безпеки та оборони.

Генезис розвитку кібертехнологій у сфері оборони є складною та динамічною областю, яка постійно вдосконалюється для відповіді на зростаючі кіберзагрози та виклики військової безпеки. Генезис розвитку кібертехнологій у сфері оборони охоплює багатоаспектний процес становлення, розвитку та впровадження цифрових технологій та інформаційних систем з метою забезпечення національної безпеки та оборони. Цей процес має велике значення для сучасних військових структур та організацій, оскільки кібертехнології відіграють важливу роль у всіх аспектах військової діяльності, починаючи від розвідки та закінчуючи керуванням військовими операціями. У сучасному цифровому світі, де технології є невід'ємною частиною нашого повсякденного життя, поняття кібертехнологій займає центральне місце. Кібертехнології відіграють критичну роль у функціонуванні суспільства, економіки, а також в сферах оборони і безпеки. Вони охоплюють широкий спектр технічних, програмних та організаційних засобів, які дозволяють здійснювати операції, обмін і зберігання інформації в електронній формі. Кібертехнології, з одного боку, сприяють зручності та швидкості взаємодії, а з іншого – вони відкривають двері до нових видів загроз, пов'язаних із кібербезпекою. У контексті оборони, кібертехнології грають важливу роль у підтримці національної безпеки та оборони від сучасних загроз, які можуть виникнути у кіберпросторі. Кібертехнології оборонної сфери включають в себе широкий спектр засобів і стратегій, спрямованих на захист інфраструктури, важливих державних систем та конфіденційної інформації, що включає в себе розробку криптографічних методів, систем виявлення та аналізу кібератак, а також створення кіберзброї для дефенсивних і офензивних цілей. У контексті тривалої російсько-української війни, роль кібертехнологій стає надзвичайно важливою. Цифрові атаки можуть використовуватися для розкриття вразливостей в інфраструктурі, збору розвідувальної інформації, а також дестабілізації внутрішньої ситуації. Розвиток кібертехнологій в сфері оборони стає необхідністю для забезпечення національної безпеки та здатності протистояти сучасним викликам. У цьому контексті, розкриття понять із сфери кібертехнологій оборонної сфери (табл. 1) має особливе значення, оскільки це відкриває можливість глибокого розуміння сутності та важливості цих понять та термінів у контексті сучасної геополітичної обстановки.

Наведені у табл. 1 поняття відображають широкий спектр аспектів, пов'язаних з кібертехнологіями та їх роллю в сфері оборони і безпеки. Ці терміни і поняття спільно формують основу для розуміння кібертехнологій та їх ролі в оборонній та безпековій сферах.

Протягом останніх десятиліть сучасні технології виробництва, зв'язку та обробки інформації стрімко перетворюють сприйняття світу. Суттєвий вплив цих змін зачіпає й сферу національної безпеки та оборони. Україна, як країна, що активно розвивається, не могла залишитись осторонь цього процесу. Розвиток генезису кібертехнологій у сфері безпеки та оборони також має свої етапи, які допомагають краще зрозуміти та адаптуватись до нових викликів. На рис. 1 наведено підхід до формування основних етапів послідовності розвитку генезису кібертехнологій у сфері безпеки та оборони України, із наведеного видно, як ці етапи прогресували, та які особливості були притаманні кожному з них. Важливо зазначити, що це узагальнена модель розвитку, і реальний процес формування генезису кібертехнологій у сфері безпеки та оборони України залежить від багатьох факторів, таких як політичні, економічні та технологічні. Треба розуміти, що реальний процес розвитку може змінюватися в залежності від багатьох факторів, тому ця модель є загальною ілюстрацією можливого напрямку розвитку кібертехнологій у сфері оборони України. Загалом, впровадження кібертехнологій у сферу оборони України потребує комплексного підходу, який враховує технологічні, організаційні, навчальні та стратегічні аспекти. Україна має можливість відповідно реагувати на кіберзагрози та розвивати свої кібероборонні здібності, використовуючи досвід інших держав та власні потенціали.

Сьогоднішні реалії міжнародної арени характеризуються стрімким та постійним розвитком кібертехнологій, особливо в сфері оборони. Іноземні держави активно

вдосконалюють свої кіберсистеми, впроваджують нові методи та технології для забезпечення національної безпеки та ведення кібервійни. У зв'язку з цим, для України надзвичайно важливим є аналіз досвіду розвитку кібертехнологій в оборонній сфері інших країн.

Таблиця 1 – Основні терміни та поняття із сфери кібертехнологій

№ з/п	Терміни	Визначення та його коротка характеристика
1	Кібертехнології	це сукупність технічних засобів, методів та процесів, спрямованих на використання і управління інформацією, даними та системами в електронному середовищі. Кібертехнології охоплюють широкий спектр діяльності, включаючи комп'ютерні науки, інформаційну безпеку, мережеві технології, штучний інтелект, аналіз даних та інше.
2	Кібертехнології оборонної сфери	це спеціалізовані кібертехнологічні рішення та методи, призначені для захисту та забезпечення безпеки важливих інформаційних інфраструктур, систем та даних, що використовуються в оборонній сфері. Ці технології включають в себе заходи проти кібератак, розробку кіберзаходів для реагування на загрози та відновлення після інцидентів.
3	Інформаційна безпека	це стан захищеності інформаційних ресурсів (даних, систем, мереж тощо) від незаконного доступу, змін, руйнування або втрати, забезпечуючи їх конфіденційність, цілісність та доступність.
4	Кібербезпека	це сукупність заходів, процедур і технологій, спрямованих на захист інформаційних систем від кібератак, зловмисних дій та небажаних подій.
5	Кібератака	це незаконна діяльність, спрямована на порушення цілісності, конфіденційності чи доступності інформаційної системи. Це може бути внесення змін у дані, блокування доступу до системи або її компрометація з різних мотивів.
6	Кіберзахист	це процес розробки та впровадження технічних і організаційних заходів для запобігання кібератакам і забезпечення безпеки інформаційних систем.
7	Шпигунство в кіберпросторі	це діяльність організацій або осіб, спрямована на отримання конфіденційної інформації шляхом несанкціонованого доступу до інформаційних систем.
8	Кібервійна	це конфлікт між державами або групами, де кібератаки використовуються як засіб для досягнення військово-політичних цілей.
9	Кіберзброя	це програми, коди або технічні засоби, призначені для завдання шкоди або спричинення збоїв у комп'ютерних системах, мережах або інфраструктурі.
10	Кіберінцидент	це небажана або аномальна подія, яка відбувається в інформаційній системі та може свідчити про можливу кібератаку або порушення безпеки.
11	Кіберспільнота	це група експертів, дослідників і фахівців, які працюють у сфері кібербезпеки та спільно діляться знаннями, дослідженнями та інформацією для запобігання кіберзагрозам.
12	Кібераналітика	це процес збору, аналізу та інтерпретації даних, щоб виявити загрози та вразливості в інформаційних системах та мережах.
13	Кібервразливість	це слабка точка або недолік в інформаційній системі, яка може бути використана для здійснення кібератаки або злому.
14	Кіберрезерв	це група фахівців із кібербезпеки, готових швидко реагувати на кібератаки та інші кіберзагрози, а також відновлювати пошкоджені системи.
15	Кібердетеренція	це стратегічні заходи, спрямовані на запобігання кібератакам через введення відсічної відповіді або покарання в разі виявлення ворожих дій.
16	Кіберімунітет	це здатність інформаційних систем та мереж стійко відновлюватися після кібератаки, а також вчасно виявляти і реагувати на нові загрози.

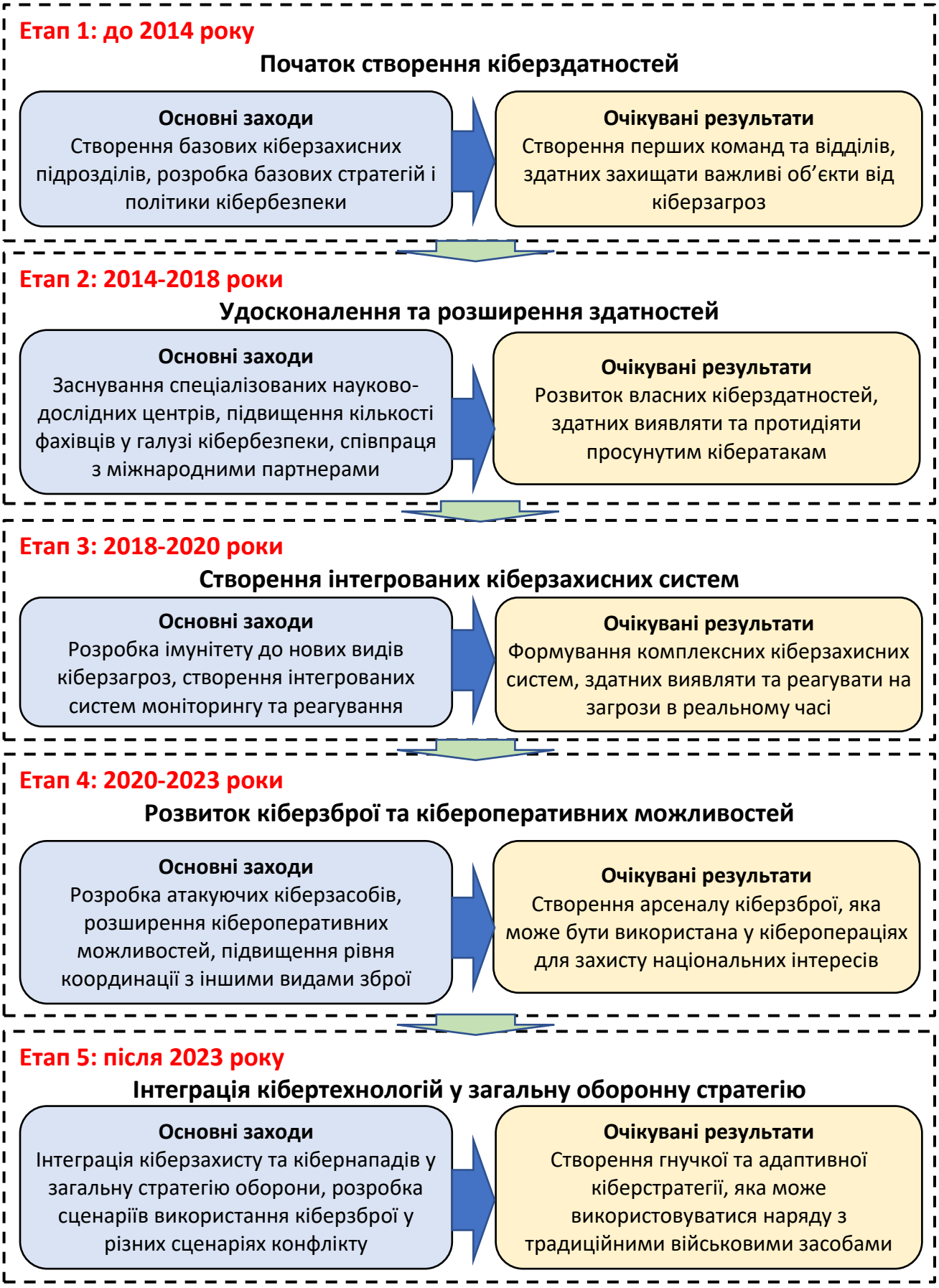

Рисунок 1 – Послідовність розвитку генезису кібертехнологій у сфері безпеки та оборони України

Однією з найактуальніших причин вивчення іноземного досвіду є посилення загроз кібербезпеці та кіберагресій. Зловмисники та державні актори все частіше використовують кібератаки для здійснення різноманітних дестабілізуючих дій, від крадіжок конфіденційної інформації до впливу на виборчі процеси та інфраструктуру країн. Набуття знань щодо практик інших країн у цьому контексті допоможе Україні адаптувати свою кіберстратегію та підвищити рівень захищеності від можливих загроз.

Крім того, аналіз досвіду розвитку кібертехнологій в іноземних державах може надати Україні ідеї та рекомендації щодо покращення власних оборонних зусиль. Це може стосуватися розробки нових кіберзбройових систем, вдосконалення методів виявлення та аналізу кіберзагроз, підвищення кіберосвіти військовослужбовців тощо.

Також важливо відзначити, що співпраця та обмін досвідом з іншими країнами можуть сприяти створенню єдиної міжнародної платформи для боротьби з кіберзагрозами. Спільні стандарти та підходи до кібербезпеки можуть допомогти зменшити ризик конфліктів у кіберпросторі та підвищити стійкість всіх країн до кібератак.

З огляду на це, аналіз досвіду розвитку кібертехнологій у сфері оборони в іноземних державах є невід'ємною складовою стратегічних зусиль України на шляху до підвищення кібербезпеки, національної обороноздатності та створення стійкого кіберсуверенітету.

Загальний огляд розвитку кібертехнологій у деяких країнах світу у сфері безпеки та оборони станом на кінець 2021 року наведено у табл. 2.

Наведені в табл. 2 приклади показують, що різні країни вдосконалюють свої кібервійськові можливості та кіберзахист на основі власних потреб та стратегічних цілей. Україна може вивчати підходи цих країн та адаптувати їх до своєї ситуації з метою підвищення національної кібербезпеки та оборони.

Важливо зазначити, що в розвитку кібертехнологій для оборони кожна країна спирається на свої внутрішні потреби та власний стратегічний підхід. Україна може вивчати позитивні практики і технології з різних країн, адаптувати їх до власних потреб та розвивати відповідні кібервійськові здібності для забезпечення національної безпеки. Враховуючи досвід і практики розвитку кібертехнологій у цих країнах, Україна може підвищити свої оборонні кіберздібності, використовуючи позитивні елементи з кожної з них. Важливо розробити власний стратегічний підхід, який відповідатиме національним потребам та загрозам. Загалом, Україна може взяти на озброєння позитивні практики та технології з інших країн для розвитку власних кібертехнологічних здібностей у сфері безпеки та оборони.

Загальний огляд показників фінансування розвитку галузі кібертехнологій оборонної сфери та країни в цілому (рис. 2 та рис. 3), розкриває ставлення цих країн до пріоритетності розвитку кібертехнологій та відношення керівництва держави до цієї галузі.

Розкриємо деякі особливості розвитку кібертехнологій в деяких провідних країнах, а саме:

США: США вважаються однією з провідних країн у розробці кібертехнологій в обороні. Вони мають великий бюджет на ці цілі та активно ведуть роботу над кіберзброєю, кіберзахистом та кіберспостереженням.

Китай: Китай також зростає у сфері кібертехнологій в обороні. Вони інвестують у розробку власної кіберзброї та засобів кіберзахисту, і ця галузь стала однією з пріоритетних.

росія: Росія відома своїми кіберспробами та активною участю у кібервійнах. Вони також розвивають свою кіберзброю та засоби кіберзахисту.

Європейські країни: Декілька країн Європи, такі як Німеччина, Франція та Велика Британія, також активно працюють над розвитком кібертехнологій в обороні. Вони можуть спрямовувати свої зусилля на покращення кіберзахисту та кіберспостереження.

Україна: Україна також веде роботу над розвитком кібертехнологій у сфері оборони, особливо після подій, пов'язаних з анексією Криму та конфліктом на сході країни. Україна активно залучає фахівців до цієї галузі та співпрацює з партнерами з інших країн.

Витрати на розвиток кібертехнологій у сфері оборони можуть варіюватися від року до року і від країни до країни. Це залежить від багатьох факторів, таких як геополітична ситуація, наявність загроз кібербезпеці, стратегічні плани країни тощо.

Розвиток кібертехнологій у сфері оборони є актуальним завданням для багатьох країн, оскільки ці технології стають все важливішим компонентом сучасної військової стратегії. Основні способи розвитку кібертехнологій у сфері безпеки і оборони за досвідом іноземних держав наведені в табл. 3.

Таблиця 2 – Огляд розвитку кібертехнологій у деяких країнах світу у сфері безпеки та оборони станом на кінець 2021 року (досвід для України)

№ з/п	Основні характеристики розвитку кібертехнологій	Позитивні аспекти переймання досвіду Україною
США		
1	США є лідером у розробці кібертехнологій для військових потреб. У них існують спеціальні військові команди, такі як Кіберкоманда США, які спеціалізуються на кібербезпеці та кібервійськових операціях. США також активно інвестують у дослідження та розробки кіберзброї, включаючи атаки на комп'ютерні системи противника, відновлення даних, розвідку тощо.	Розвиток військових кіберкоманд і командувань для кібербезпеки. Інвестування у дослідження та розробки кіберзброї та кібервійськових операцій. Розробка планів відновлення після кібератак та підвищення кіберстійкості важливих інфраструктур.
Російська Федерація		
2	Росія активно використовує кіберзброю як засіб ведення інформаційної війни та спостереження за іншими країнами. Вони відомі своєю здатністю до здійснення складних кібератак, включаючи напади на критичну інфраструктуру.	Розвиток дієвої кіберзброї для відповіді на можливі кіберзагрози. Покращення кіберзахисту критичних об'єктів і інфраструктури.
Китай		
3	Китай також активно розвиває кібертехнології для оборонних цілей. Вони фокусуються на розробці кіберзброї, великих даних, штучного інтелекту та кіберрозвідці.	Розвиток кібертехнологій для аналізу та прогнозування оборонних ситуацій. Використання штучного інтелекту для оптимізації оборонних процесів та стратегій.
Ізраїль		
4	Ізраїль відомий своїми інноваціями в кібертехнологіях, особливо в області кібербезпеки. Вони володіють ефективними методами виявлення та протидії кіберзагрозам.	Співпраця з ізраїльськими компаніями та експертами у сфері кібербезпеки. Впровадження ефективних методів виявлення та реагування на кіберзагрози.
Велика Британія		
5	Велика Британія також активно працює над розвитком кібербезпеки та кібервійськових можливостей. У них існують спеціальні військові підрозділи, такі як Національний центр кібербезпеки (NCSC), які займаються забезпеченням кібербезпеки в країні.	Розвиток національного центру кібербезпеки та координація зусиль зі збереження кібербезпеки в країні. Співпраця з британськими експертами у сфері кібербезпеки та обмін досвідом.

№ з/п	Основні характеристики розвитку кібертехнологій	Позитивні аспекти переймання досвіду Україною
	Індія	
6	Індія також звертає увагу на розвиток кібертехнологій у сфері оборони. Вони активно розвивають власні кібервійськові здібності та працюють над захистом своїх критичних інфраструктур.	Розвиток кібервійськових підрозділів для захисту важливих інфраструктур. Розробка стратегій кібербезпеки для державних інституцій та підприємств.
	Південна Корея	
7	Південна Корея визначається своїми передовими технологіями, включаючи кібертехнології. Вони інвестують у розвиток кіберзахисту та кібервійськових здібностей для захисту від загроз північної сусідньої КНДР.	Можливі позитивні аспекти для України: Використання передових технологій для розвитку кіберзахисту та кібервійськових здібностей. Зосередження на захисті від можливих кібератак зі сусідніх держав.
	Швеція	
8	Швеція відома своїми дослідженнями в галузі кіберзахисту та кібербезпеки. Вони активно співпрацюють з іншими європейськими країнами для розробки спільних кіберзахисних стратегій.	Розвиток міжнародної співпраці у сфері кібербезпеки та обмін досвідом з іншими країнами. Розробка спільних стратегій кіберзахисту разом з партнерами.
	Німеччина	
9	Німеччина також активно працює над розвитком кібертехнологій для оборони. Вони зосереджуються на використанні штучного інтелекту та аналізу великих даних для забезпечення кібербезпеки.	Використання штучного інтелекту та аналізу даних для прогнозування кіберзагроз та виявлення вразливостей. Розвиток кібертехнологій для обробки та аналізу великих обсягів інформації.
	Франція	
10	Франція також вкладає зусилля у розвиток кібервійськових можливостей. Вони активно розробляють кіберзброю та здійснюють кібервійськові операції для захисту національних інтересів.	Розробка ефективної кіберзброї та реалізація кібервійськових операцій для захисту від можливих загроз. Використання кіберзброї як ефективного засобу ведення військової операцій.
	Японія	
11	Японія розробляє кібервійськові здібності для захисту важливих національних інфраструктур. Вони також активно вивчають використання штучного інтелекту та кіберзахисту для військових цілей.	Використання штучного інтелекту для автоматизації кіберзахисту та виявлення незвичних або підозрілих дій. Застосування кібертехнологій для захисту критичних інфраструктур, таких як енергетика та транспорт.
	Італія	
12	Італія також звертає увагу на розвиток кібервійськових здібностей та кібербезпеки. Вони активно співпрацюють з іншими країнами Європейського Союзу для створення спільних стандартів та стратегій.	Розвиток міжнародної співпраці в рамках об'єднаних зусиль для забезпечення кібербезпеки. Розробка спільних стратегій кіберзахисту разом з іншими країнами, які мають подібний досвід.
	Польща	
13	Польща також активно інвестує в розвиток кібервійськових можливостей. Вони зосереджуються на розробці кіберзахисту та кібербезпеки в армії.	Розвиток кібервійськових здібностей в армії для забезпечення кібербезпеки та відповіді на можливі кібератаки. Розробка кіберзахисту на рівні військових структур та об'єктів.

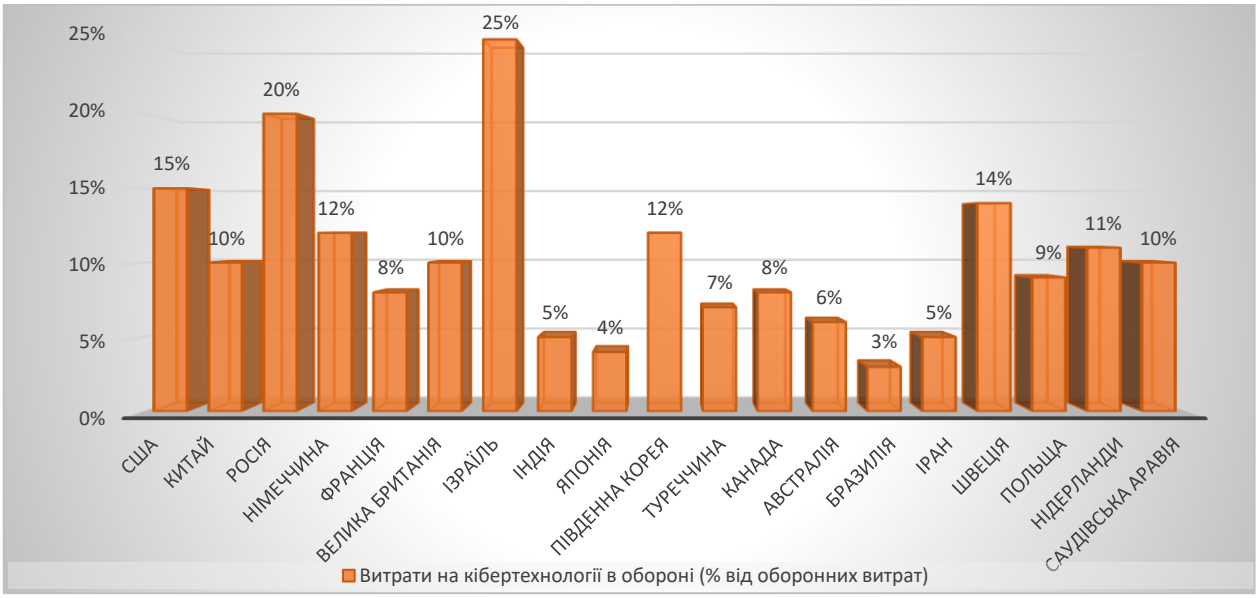

Рисунок 2 – Середній показник частки витрат на кібертехнології в оборонному бюджеті деяких країн світу (2018-2023 роки)

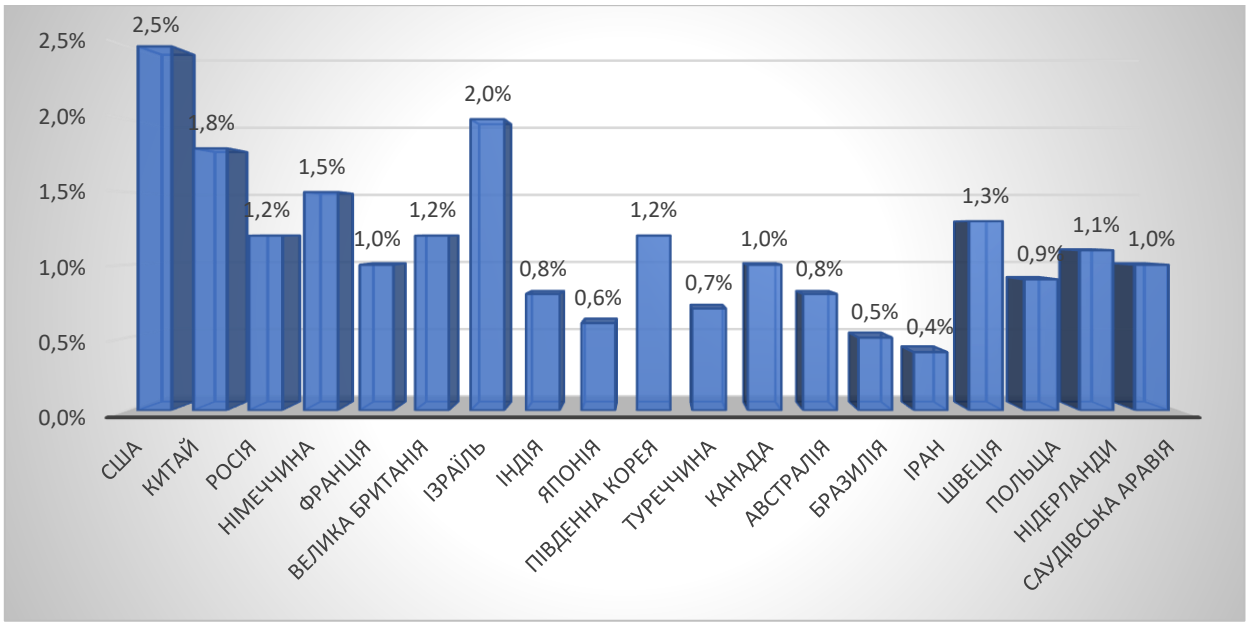

Рисунок 3 – Середній показник частки витрат на кібертехнології від ВВП деяких країн (2018-2023 роки)

Важливо зауважити, що ефективність кожного способу може залежати від багатьох факторів, включаючи технічну підготовку, рівень інвестицій, політичну волю та геополітичну ситуацію. Більшість країн поєднують декілька з цих підходів у своїй стратегії розвитку кібертехнологій у сфері оборони.

Отже, здійснюючи аналіз генезису розвитку кібертехнологій у сфері безпеки та оборони іноземних держав, можна зробити важливий висновок. Іноземні держави активно використовують кібертехнології як важливий інструмент для забезпечення національної безпеки та оборони. Цей досвід свідчить про успішність такого підходу, адже кіберзагрози стають все складнішими та впливовішими. Україна має потенціал для впровадження подібних практик у власній сфері безпеки та оборони.

Впровадження кібертехнологій може значно підвищити ефективність захисту від сучасних загроз, забезпечуючи оперативну реакцію на атаки та злочинні дії в кіберпросторі.

Таблиця 3 – Основні способи розвитку кібертехнологій у сфері безпеки і оборони за досвідом іноземних держав

№ з/п	Спосіб	Характеристика	Характеристика ефективності	Країни, які використовують
1	Розробка кіберзброї	Деякі країни активно інвестують у розробку спеціальних кіберзасобів, які можуть використовуватися для здійснення кібератак на ворожі інфраструктури, системи зв'язку, енергетичі об'єкти тощо. Це може включати створення вірусів, троянських програм, руткітів тощо.	Ефективність цього способу залежить від технічного рівня розроблених засобів та вміння ефективно впроваджувати їх у реальних умовах.	Такий підхід є характерним для країн із розвиненою кіберінфраструктурою, таких як США, Росія, Китай.
2	Створення кіберзахисту	Інші держави зосереджуються на розробці ефективних систем кіберзахисту для захисту своїх військових та цивільних інфраструктур від кібератак. Це може включати розробку антивірусів, систем виявлення вторгнень, аналізу трафіку тощо.	Ефективність полягає у здатності вчасно виявляти та відвертати кіберзагрози.	Такий підхід популярний серед країн Європи, які акцентують на кібербезпеці.
3	Створення кіберкоманд	Деякі країни формують спеціальні військові чи цивільні кіберкоманди, які спеціалізуються на веденні кібероперацій та взаємодії з іншими збройними силами. Це дозволяє цільово використовувати кібертехнології в рамках загальної військової стратегії.	Ефективність залежить від професіоналізму та координації команд.	Такий підхід актуальний для багатьох розвинених країн, що мають розвинуті військові структури.
4	Міжнародна співпраця та нормативне регулювання	Деякі держави намагаються створити міжнародні коаліції або договори для обміну інформацією про кіберзагрози, встановлення стандартів кібербезпеки та вироблення правил поведінки в кіберпросторі. Це може сприяти зменшенню ризику конфліктів у кіберпросторі.	Ефективність залежить від готовності країн дотримуватись встановлених норм та співпраці.	Цей підхід характерний для багатьох країн Європи та Північної Америки.

Забезпечення національної кібербезпеки вимагатиме широкого спектра заходів: від створення відповідної правової бази та підтримки наукових досліджень до розвитку власних кадрових потенціалів та співпраці з партнерами на міжнародній арені.

Таким чином, здійснення перспективного впровадження кібертехнологій у сферу безпеки та оборони України на основі іноземного досвіду може стати ключовим фактором у підвищенні здатності країни захищати свої національні інтереси в умовах зростаючих кіберзагроз.

Впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері оборони та безпеки України може мати кілька перспективних напрямків, основні з них наведені у табл. 4.

Таблиця 4 – Перспективні напрями подальших досліджень щодо впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері оборони та безпеки України

№ з/п	Напрям досліджень	Характеристика напряму	Очікуваний результат
1	Технологічний обмін і партнерства	Україна може встановлювати технологічні партнерства та обмін з іншими країнами, які мають високорозвинені кібертехнологічні сектори.	Це дозволить обмінюватися передовими технологіями, навичками та знаннями у сфері кібербезпеки та кібероборони.
2	Навчання та підготовка	Впровадження досвіду іноземних держав може включати організацію спільних навчальних програм, семінарів, тренінгів та майстер-класів для українських фахівців з кібербезпеки	Це допоможе підвищити кваліфікацію та компетентність в цій сфері.
3	Захист критично важливих інфраструктур	Україна може вивчати досвід інших країн у сфері захисту критично важливих інфраструктур від кібератак.	Це стосується енергетики, транспорту, фінансових систем та інших стратегічних секторів.
4	Створення міжнародних спільнот	Україна може активно долучатися до міжнародних спільнот та організацій, що займаються кібербезпекою, таких як Європейський союз, НАТО, Ініціатива з кібербезпеки G7 тощо.	Це дозволить спільно працювати над розробкою стандартів та норм у цій сфері.
5	Дослідження та розвиток	Вивчення досвіду інших країн може надихнути українських дослідників та інженерів на створення нових інноваційних рішень у галузі кібербезпеки та кібероборони.	Це сприяє розвитку української науки у галузі кібербезпеки та кібероборони.
6	Міжнародні проєкти	Україна може приєднуватися до міжнародних проектів, спрямованих на спільне розроблення та впровадження кібертехнологій у сфері оборони.	Це може включати спільні дослідницькі проекти, створення спільних центрів розробки, а також обмін інженерами та фахівцями.
7	Адаптація найкращих практик	Вивчення досвіду інших країн, пошук передових практик адаптації розвитку кібертехнологій в Україні до умов ЄС та НАТО.	Це може допомогти ідентифікувати найкращі практики в сфері кібербезпеки та кібероборони і адаптувати їх до умов України.

Важливо зазначити, що впровадження досвіду іноземних держав повинно бути адаптовано до конкретних потреб та викликів, з якими стикається Україна, і враховувати національні інтереси та стратегічні цілі.

Проведення досліджень у напрямку формування рекомендацій щодо розвитку кібертехнологій в сфері безпеки та оборони обумовлені рядом ключових факторів та трендів, що визначають сучасну міжнародну ситуацію. До основних із них можна віднести те, що:

- з кожним роком кіберзагрози стають більш складними і небезпечними. Хакерські атаки можуть впливати на роботу урядових систем, критичну інфраструктуру та військові

системи. Однак застосування високих технологій у військовій сфері також надає можливостей для захисту та здійснення кібероперацій;

- конкуренція в галузі кібертехнологій, обумовлена тим, що військові і цивільні організації у всьому світі змагаються за доступ до передових кібертехнологій. Розвиток власних кіберздібностей стає пріоритетом для багатьох країн;

- кібертехнології можуть значно підвищити ефективність військової оборони та забезпечити нові можливості для протидії загрозам. Вони можуть використовуватися для виявлення та відстеження ворожих атак, захисту важливих інформаційних ресурсів і підвищення загального рівня безпеки;

- кіберзагрози та розвиток кібертехнологій мають глобальний характер. Співробітництво між країнами у цій галузі може сприяти спільній боротьбі з загрозами та забезпечити мир та стабільність;

- розвиток кібертехнологій також має велике економічне значення. Він створює нові ринки та можливості для інновацій, що сприяє економічному зростанню та забезпечує конкурентоспроможність країни.

З урахуванням цих факторів, проведення досліджень та формування рекомендацій щодо розвитку кібертехнологій в сфері безпеки та оборони стає необхідністю. Це допоможе забезпечити ефективний захист від кіберзагроз, підвищити обороноздатність країни і сприяти мирному співіснуванню в умовах глобальної кіберізоляції.

Аналіз теоретичних та практичних аспектів досвіду іноземних держав в системі формування генезису розвитку кібертехнологій у сфері безпеки та оборони України дозволив сформувати основні загальні рекомендації щодо розвитку кібертехнологій в сфері безпеки та оборони (табл. 5).

Наведені у табл. 5 рекомендації є загальними і можуть варіюватися залежно від конкретної ситуації та потреб України в оборонній кіберсфері, а також рекомендації можуть слугувати загальним орієнтирами для розвитку кібертехнологій у сфері безепки та оборони України в цілому.

Таблиця 4 – Загальні рекомендації щодо розвитку кібертехнологій в сфері безпеки та оборони

№ з/п	Напрям рекомендацій	Зміст рекомендацій	Термін реалізації	Основні заходи для реалізації	Очікуваний результат
1	Створення національної кіберстратегії	Розробити комплексний план, що охоплює різні аспекти кібербезпеки та розвитку кібертехнологій в оборонній сфері.	1 рік	Створення робочої групи з представників галузевих експертів для аналізу потреб, визначення пріоритетів та формулювання стратегії.	Чіткий напрямок розвитку кібертехнологій, забезпечення координації зусиль та визначення показників успішності.
2	Розвиток кібервійськових здібностей	Розробка та впровадження кібервійськових підрозділів для захисту та атак на кіберпростір противника.	2-3 роки	Набір та підготовка спеціалістів, розробка сценаріїв кібератак та відповідей на них, створення інфраструктури для аналізу кіберзагроз.	Здатність реагувати на кіберзагрози та здійснювати ефективні кібератаки при необхідності.
3	Розробка кіберзахисних технологій	Розробка та впровадження систем для виявлення, аналізу та нейтралізації кіберзагроз.	1-2 роки	Дослідження нових методів виявлення загроз, створення аналітичних інструментів, навчання персоналу.	Забезпечення високого рівня кібербезпеки, зниження ризику успішних кібератак.
4	Партнерство з приватним сектором	Співпраця з кібербезпековими компаніями для обміну	Постійно	Підписання угод про співпрацю, організація	Зростання якості експертизи та швидкості інновацій у кібербезпеці.

№ з/п	Напрям рекомендацій	Зміст рекомендацій	Термін реалізації	Основні заходи для реалізації	Очікуваний результат
		знаннями, технологіями та ресурсами.		спільних досліджень та тренінгів.	
5	Формування кадрового потенціалу	Розвиток освітніх програм та тренінгів з кібербезпеки для підготовки кваліфікованих фахівців.	3-5 років	Створення спеціалізованих навчальних програм, набір і підготовка викладачів.	Забезпечення постійного доступу до висококваліфікованих спеціалістів у галузі кібербезпеки.
6	Створення інноваційних дослідницьких центрів	Створення спеціалізованих центрів для досліджень у сфері кібербезпеки та розвитку передових кібертехнологій.	2-4 роки	Виділення фінансування для створення інфраструктури, привернення вчених та експертів, організація співпраці з університетами та промисловими партнерами.	Здійснення передових досліджень та створення інноваційних кібертехнологій для оборонної сфери.
7	Створення національних кіберзагонів	Розробка та впровадження програм навчання для молоді з акцентом на кібербезпеку та кібертехнології.	1-3 роки	Організація конкурсів, хакатонів, лекцій та майстер-класів для підвищення інтересу молоді до кібербезпеки.	Залучення молоді до сфери кібертехнологій, підготовка нового покоління фахівців.
8	Забезпечення кібербезпеки критично важливої інфраструктури	Впровадження систем для захисту критично важливих об'єктів від кібератак.	2-5 років.	Аналіз загроз, розробка систем виявлення та запобігання атакам, проведення регулярних аудитів.	Забезпечення надійності та стабільності роботи критично важливих систем у разі кіберзагроз.
9	Посилення міжнародної співпраці	Активізація співпраці з іншими країнами та міжнародними організаціями у сфері кібербезпеки та кібертехнологій.	Постійно	Участь у міжнародних конференціях, обмін інформацією про загрози та рішення, спільні практики.	Очікуваний результат: Здатність діяти разом у разі глобальних кіберзагроз та обмін досвідом.

5. Висновки

Впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України є важливим кроком для підвищення ефективності та конкурентоспроможності країни в цій сфері. Основними висновками за результатами статті можна визначити те, що:

- впровадження досвіду інших країн дозволить українським спеціалістам з кібербезпеки та оборони здобути нові знання та навички, які можна використовувати для розвитку і вдосконалення власних технологій та підходів;

- використання іноземного досвіду дозволить зміцнити кібербезпеку та оборону України, оскільки інші країни можуть мати більше досвіду в роботі з кіберзагрозами і створенням високотехнологічних оборонних систем;

- впровадження іноземного досвіду також допоможе знизити залежність від імпорту кібертехнологій та програмного забезпечення, що може створити більшу автономію в галузі кібербезпеки та оборони;

- взаємодія з іноземними партнерами у сфері кібербезпеки та оборони може сприяти створенню спільних проектів і програм, що підсилить партнерство України з іншими країнами.

- за допомогою впровадження іноземного досвіду, Україна може розширити свої можливості у розробці нових кібертехнологій та створенні інноваційних рішень у галузі безпеки та оборони.

Україна знаходиться в складному геополітичному контексті, і впровадження іноземного досвіду в галузі кібербезпеки і оборони може позитивно вплинути на зміцнення національної безпеки країни та забезпечення обороноздатності.

Узагальнюючи можна сказати, що впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України має великий потенціал для поліпшення стану безпеки та підвищення технологічної конкурентоспроможності країни.

6. Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

7. Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Російсько-українська війна (з 2014). URL: https://uk.wikipedia.org/wiki.
2. Російсько-українська війна: історичний контекст. URL: https://uinp.gov.ua/informaciyni-materialy/rosiysko-ukrayinska-viyna-istorychnyy-kontekst.
3. Cyber digest. Огляд подій в сфері кібербезпеки, грудень 2022. Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України». Національний координаційний центр кібер безпеки. 2022. С. 44.
4. Singer P.W. and Allan Friedman (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. P. 336.
5. Alexander Klimburg (2017). The Darkening Web: The War for Cyberspace. Penguin Books. P. 448.
6. Дергачов О. (2018). Кібербезпека: загрози та захист. Національний університет "Львівська політехніка". С. 312.
7. Тищенко О. (2016). Інформаційна безпека держави: кібераспекти. Національна академія державного управління при Президентові України. С. 232. Автор розглядає роль кібертехнологій у забезпеченні інформаційної безпеки держави, виокремлюючи основні виклики та шляхи їх подолання.

References

1. Russian-Ukrainian war (since 2014). Available from : https://uk.wikipedia.org/wiki.
2. Russian-Ukrainian war: historical context. Available from : https://uinp.gov.ua/informaciyni-materialy/rosiysko-ukrayinska-viyna-istorychnyy-kontekst.
3. Cyber digest. Overview of events in the field of cyber security, December 2022. Prepared with the support of the USAID Project "Cyber security of critical infrastructure of Ukraine". National Cyber Security Coordination Center. 2022. P. 44.
4. Singer, P.W. and Allan Friedman (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. P. 336.
5. Alexander, Klimburg (2017). The Darkening Web: The War for Cyberspace. Penguin Books. P. 448.
6. Dergachev, O. (2018). Cyber security: threats and protection. Lviv Polytechnic National University. C. 312.
7. Tyshchenko, O. (2016). State information security: cyber aspects. National Academy of Public Administration under the President of Ukraine. C. 232. The author considers the role of cyber technologies in ensuring the information security of the state, highlighting the main challenges and ways to overcome them.
8. David, E. Sanger. (2018). The Perfect Weapon:

8. David E. Sanger. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown. P. 384.
9. Richard A. Clarke and Robert K. Knake (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco. P. 320.
10. Гіль О. (2019). Кібербезпека держави: інструменти, методи, практика. Видавничий дім "Ін Юре". Р. 400.
11 Бортнік С., Скасницький О. (2016). Кібербезпека: загрози та виклики. Національний технічний університет України "Київський політехнічний інститут". Р. 268.
12. Lester Evans. (2020). Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners. Independently published. P. 240.
13. Singer P.W. and Allan Friedman. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. С. 336.
14. Губарєв В. (2020). Кібербезпека та захист інформації. Національний університет "Львівська політехніка". С. 272.
15. Гарань О. (2019). Кібербезпека України: стан, пріоритети, ризики. Інститут світової політики. С. 120.
16. P.W. Singer and August Cole. (2015). Ghost Fleet: A Novel of the Next World War. Eamon Dolan/Mariner Books. P. 416.
17. Richard A. Clarke and Robert K. Knake. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press. P. 320.
18. Мішечкіна Л. (2020). Кібербезпека в системі національної безпеки України. Видавничий дім "Ін Юре". С. 400.
19. Сокірко В. (2017). Кібербезпека: проблеми, загрози та виклики. Видавництво: Центр учбової літератури. С. 336.

8. David E. Sanger. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown. P. 384.
9. Richard, A. Clarke and Robert K. Knake (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco. P. 320.
10. Gil, O. (2019). Cyber security of the state: tools, methods, practice. "In Yure" Publishing House. P. 400.
11 Bortnik S., Skasnytskyi O. (2016). Cyber security: threats and challenges. National Technical University of Ukraine "Kyiv Polytechnic Institute". P. 268.
12. Lester Evans. (2020). Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners. Independently published. P. 240.
13. Singer P.W. and Allan Friedman. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. C. 336.
14. Gubarev V. (2020). Cyber security and information protection. Lviv Polytechnic National University. C. 272.
15. Garan O. (2019). Cybersecurity of Ukraine: state, priorities, risks. Institute of World Politics. C. 120.
16. P.W. Singer and August Cole. (2015). Ghost Fleet: A Novel of the Next World War. Eamon Dolan/Mariner Books. P. 416.
17. Richard A. Clarke and Robert K. Knake. (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press. P. 320.
18. Mishechkina L. (2020). Cyber security in the national security system of Ukraine. "In Yure" Publishing House. C. 400.
19. Sokirko, V. (2017). Cyber Security: Issues, Threats and Challenges. Publisher: Center for Educational Literature. C. 336.