Список використаних джерел

1. Global overview report digital 2024. 31 January 2024. URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата звернення: 3 вересня 2024 р.).

2. Digital 2024: Ukraine. Global overview report digital 2024. 23 february 2024. URL: https://datareportal.com/reports/digital-2024-ukraine (дата звернення: 3 вересня 2024 р.).

3. Словник психологічних термінів. Національний фармацевтичний університет. МОЗ України. 2015. URL: https://nuph.edu.ua/slovnik-psihologichnih-terminiv/ (дата звернення: 3 вересня 2024 р.).

4. Lubenets I., Kulyk O., Kulakova N., Lisnychenko L., Naumova I. The problem of child safety in the digital space // Amazonia Investiga, September 2023. Volume 12. Issue 69. p.281-290 (p.286). DOI: https://doi.org/10.34069/AI/2023.69.09.25 (дата звернення: 3 вересня 2024 р.).

5. Children and parents: media use and attitudes report. Ofcom. 30 March 2022. URL: http://surl.li/urlpiw (дата звернення: 3 вересня 2024 р.).

6. Кадакова К. У Європі зростає попит на українське порно, біженки та їхні діти мають високий ризик сексуальної експлуатації – дослідження // Divoche media. 27.03.2023 р. URL: http://surl.li/gjdno (дата звернення: 4 вересня 2024 р.).7. Музика О. Що відомо про ПВК «Редан»: ця молодіжна субкультура вже дійшла до України. 24 канал. Новини від 01.03.2023 р. URL: http://surl.li/hqvpy (дата звернення: 3 вересня 2024 р.).

8. Кримінальна ситуація в Україні в умовах війни: основні тенденції. 2022 рік: монографія / авт. кол.: М.Г. Вербенський, О.Г. Кулик, І.В. Наумова та ін.; за заг. ред. д-ра юрид. наук, проф. М. Г. Вербенського. Київ: Юрінком Інтер, 2023. 388 с.

Лунгол Ольга
кандидат педагогічних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки
Донецький державний університет внутрішніх справ
ORCID ID: 0000-0001-8128-0072

КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ

Кібербезпека в умовах гібридної війни є ключовим аспектом національної безпеки, враховуючи інтеграцію сучасних військових конфліктів у цифрову площину. Гібридні війни включають не лише традиційні військові дії, але й використання кібероперацій, інформаційного тиску, економічних санкцій та дипломатичних дій, що спрямовані на підрив критичних інфраструктур та дестабілізацію політичної ситуації в державі. У цьому контексті Україна, яка

тривалий час зазнає активної агресії з боку рф, є особливо вразливою до нових видів кіберзагроз, що підвищує значимість та важливість досліджень у цій сфері.

Кіберзагрози негативно впливають на функціонування державних інституцій, фінансових систем, енергетичних мереж та інших критично важливих об'єктів, що становить значний ризик для національної безпеки України. Крім того, інформаційні атаки, спрямовані на дезінформацію, психологічні операції та підрив довіри суспільства, стають невід'ємною складовою гібридної агресії, що посилює її ефективність та складність у протидії.

Таким чином, наукове дослідження викликів кібербезпеки та розробка методів протидії кіберзагрозам у контексті гібридної війни є не лише актуальним, а й необхідним для створення ефективної стратегії захисту нашої держави. Дане дослідження спрямоване на вивчення сучасних загроз, аналіз існуючих підходів до кіберзахисту та визначення шляхів підвищення стійкості національної кіберінфраструктури до кібернетичних атак та інформаційних операцій.

Вітчизняні науковці Дудар В. та Денисенко С. [1] розглядають гібридну війну як багатокомпонентну форму ведення конфлікту, що включає комбінацію традиційних військових дій, кібероперацій, інформаційних кампаній, економічного тиску та використання нерегулярних збройних формувань. Особливу увагу науковці приділяють кібератакам як важливій складовій гібридної війни [1]. Дудар В. та Денисенко С. досліджують конкретні приклади кібератак, спрямовані на критичну інфраструктуру України, урядові та військові об'єкти, а також інформаційні системи.

Дібікова Ю. [2] зазначає, що особливу роль у гібридній війні сьогодні посідають соціальні мережі та відеохостинги: Facebook, Twitter, Instagram, TikTok, YouTube тощо, які перетворюються на платформи для широкомасштабного поширення пропаганди, фейкових новин і дезінформації, координації гібридних операцій, таких як масові протести, дестабілізація ситуації або організація деструктивних дій, здійснення шпигунства та розвідки [2]. Науковиця описує у своїх дослідженнях про створення фальшивих акаунтів та груп, через які розповсюджується спотворена інформація для маніпулювання громадською думкою. Соціальні мережі активно застосовуються у гібридній війні для впливу на громадську думку та настрої через цілеспрямоване поширення певної інформації, наративів і пропаганди, які спрямовані на створення конфліктів, розпалювання національної ворожнечі, підрив стабільності та інших деструктивних процесів.

Когут Ю. [4] наголошує на тому, що робота з протидії проявам гібридної війни нового типу є важливою складовою державного забезпечення національної безпеки з метою формування відповідного захисту держави в міжнародних конфронтаціях. Науковець також стверджує, що глобальною метою гібридної війни є закріплення частини стратегічно важливих ресурсів країни-жертви за агресором [4]. Причому «передавання» таких ресурсів здійснюється елітою «країни-жертви» добровільно, адже сприймається нею не

як захоплення, а як рух шляхом розвитку та зміни ментальності народу, яка внаслідок трансформації втрачає свої основні цілі та духовні цінності, замінюючи їх морально-психологічними ілюзіями та міфами агресора. Гібридна війна включає в себе одночасне використання традиційних військових сил разом з нерегулярними формуваннями, проведенням операцій у кіберпросторі, а також здійсненням інформаційного впливу, економічного (енергетичного, продовольчого) тиску та дипломатичного впливу на супротивника.

Таким чином, сутність гібридної війни полягає в інтеграції різних аспектів протистояння – інформаційного, політичного, економічного, соціального, гуманітарного та воєнного. Характерною особливістю гібридизації війни нового типу є поєднання «жорсткої» військової сили зі стратегією «м'якої» сили, що включає систему дипломатичних, економічних, юридичних, політичних та культурних інструментів ненасильницького впливу на ситуацію в державах, спрямованих на маніпулювання елітами та населенням країни-жертви.

Сучасні підходи до кіберзахисту мають базуватися на таких основних принципах, як превентивність, виявлення, реагування та відновлення. Кожен із цих принципів реалізується через різноманітні технологічні рішення, організаційні заходи та нормативно-правову базу. Так, попередження кіберзагроз включає використання мережевих фаєрволів, антивірусного програмного забезпечення, систем виявлення вторгнень та захисту від розподілених атак на відмову в обслуговуванні. Системи моніторингу та аналізу мережевої активності дозволяють оперативно ідентифікувати підозрілі дії. Використання інструментів аналізу поведінки користувачів та машинного навчання дозволяє підвищити точність виявлення загроз. Великі дані та аналітика з використанням штучного інтелекту вже зараз відіграють ключову роль у виявленні складних, багаторівневих атак.

Для підвищення стійкості національної кіберінфраструктури необхідно впроваджувати комплексні рішення, що враховують як технологічні, так і організаційні аспекти, такі як використання штучного інтелекту для аналізу великих даних та автоматизацію процесів виявлення і реагування на загрози; проведення регулярних навчань та підвищення кваліфікації; зміцнення співпраці між державами у сфері кібербезпеки задля обміну інформацією про нові загрози та найкращі практики кіберзахисту; створення спеціалізованих органів, відповідальних за координацію кіберзахисту на національному рівні тощо.

Наукове дослідження викликів кібербезпеки та методів протидії у контексті гібридної війни є надзвичайно важливим для підвищення стійкості національної інфраструктури до сучасних загроз. Враховуючи глобальні тенденції та специфіку кіберзагроз, необхідно зосередитися на розвитку наукових підходів до захисту та підвищення кіберстійкості державних інституцій та критично важливих об'єктів.

Список використаних джерел

1. Дудар В., Денисенко С. Гібридна війна та кібератаки російської федерації проти України: поняття, стратегії та наслідки. *Український літопис*. 2024. С. 23-30. DOI:https://doi.org/10.31470/2786-8583-2024-3-23-30.
2. Дібікова Ю.С. Інформаційна складова гібридної війни: українські реалії. *Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки.* Том 2, № 25. 2022. С. 25 – 36.
3. Лунгол О.М. Роль кібергігієни у безпеці та розвитку українського суспільства. Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів : матеріали VIII Всеукраїнської науково-практичної конференції, м. Одеса, 30 квітня 2024 року. Одеса : ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2024. С. 268 – 270.
4. Когут Ю.І. Гібридна війна нового типу як загроза політичній безпеці держав. *Національні інтереси України*. № 2 (2). С. 505 – 517. https://doi.org/10.52058/3041-1793-2024-2(2)-505-517.

Майданік Ірина
кандидат соціологічних наук, старший науковий співробітник,
провідний науковий співробітник
Інститут Демографії та проблем якості життя НАН України

ПРИМУСОВА МІГРАЦІЯ НАСЕЛЕННЯ УКРАЇНИ ЯК НАСЛІДОК ПОВНОМАСШТАБНОЇ ВІЙНИ

Військове вторгнення РФ в Україну спричинило масштабні системні зміни у міграційних процесах населення. Гібридна фаза війни, пов’язана з окупацією Криму та частини Донецької та Луганської областей, призвела до виникнення помітних потоків внутрішнього переміщення населення, проте суттєво не порушила колишніх усталених форм трудової, освітньої, маятникової міграції на підконтрольних уряду територіях. Повномасштабна агресія підняла до максимуму військові ризики та небезпеки, розширила їх ареал на територію всієї України (особливо сильно це стало відчуватися після запровадження країною-агресором масованих обстрілів цивільної інфраструктури). В таких умовах на порядку денному почали домінувати вимушені міграції населення.

Поряд з феноменом вимушеної міграції наукова література виділяє поняття примусової міграції [1, с. 46]. Зазначені поняття схожі за значенням, оскільки описують переміщення недобровільного характеру. Проте їхні причини та механізми можуть відрізнятися. Примусові міграції описують ситуації, коли рішення про зміну місця проживання або перебування приймає за людину держава або інша силова структура. Окремі джерела пов’язують її з рішенням судових органів щодо виселення за межі країни [2]. Натомість вимушена міграція передбачає наявність бодай мінімального вибору щодо